INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE
E ADMINISTRAÇÃO DE LISBOA

O PAPEL DA AUDITORIA INTERNA NO REGIME GERAL DE PROTEÇÃO DE DADOS ENQUANTO TERCEIRA LINHA DE DEFESA

Sandra Alonso Diogo

Lisboa, março de 2021

INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DE LISBOA

O PAPEL DA AUDITORIA INTERNA NO REGIME GERAL DE PROTEÇÃO DE DADOS ENQUANTO TERCEIRA LINHA DE DEFESA

Sandra Alonso Diogo

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre no Mestrado em Auditoria, realizada sob a orientação científica de Maria da Luz Vilela Miranda, Mestre Especialista em Auditoria Interna.

Constituição do Júri:
Prof. Especialista Gabriel Alves - Presidente
Prof ª Especialista Maria Albertina Rodrigues - Arguente
Prof ª Especialista Maria da Luz Miranda - Vogal

Lisboa, março de 2021

Declaro ser a autora desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido (no seu todo ou qualquer das suas partes) a outra instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas. Mais acrescento que tenho consciência de que o plágio – a utilização de elementos alheios sem referência ao seu autor – constitui uma grave falta de ética, que poderá resultar na anulação da presente Dissertação.

Dedicatória

Dedico este trabalho com todo o Amor, porque sem eles nada seria igual,

à minha avó materna, Odete Augusto com 91 anos, meu exemplo de coragem, generosidade, pelo seu sorriso ímpar de quem abraça com os olhos

e ama incondicionalmente, por tudo o que sou.

À minha mãe Edite Augusto, por tudo em que se tornou.

Ao meu pai Eugénio Alonso, a título póstumo, por tudo o que será sempre.

Ao meu marido, José Diogo, meu companheiro de uma vida.

À minha filha Mariana Diogo, meu coração fora do peito.

Agradecimento

Agradeço, ao Instituto Superior de Contabilidade e Administração de Lisboa, em especial à minha Orientadora, Professora e Mestre Especialista, Maria da Luz Miranda e ao Professor Coordenador deste Mestrado em Auditoria, Mestre Especialista Gabriel Alves, assim como ao restante Corpo Docente, por tudo o que me ensinaram.

À ANA – Aeroportos de Portugal, empresa da qual visto inteiramente a camisola e em especial à minha Diretora, Dra. Helena Girão, pela confiança e motivação que sempre me transmitiu.

Aos meus familiares, em especial ao meu marido e filha, pela compreensão, apoio e carinho, pelo incentivo e inspiração nos momentos mais desgastantes.

Aos colegas que conheci e com quem privei, tanto da turma 2 como da turma 1, pelo companheirismo e espírito de entreajuda. Em especial à Andreia Cortes, Fabiana Nunes, Mariuska Rufilo, Miguel Limão, Raquel Dolores e Margarida Costa.

A todos quantos, direta ou indiretamente contribuíram de alguma forma para a realização desta Dissertação, que desenvolvi com toda a entrega.

O meu sincero agradecimento!

Resumo

Segundo o Modelo das Três Linha de Defesa, publicado em 21 de setembro de 2010 pelas FERMA e ECIIA no *Guidance on the 8th EU Company law*, cabe à Auditoria Interna, enquanto organismo independente, uma avaliação objetiva e isenta da gestão do risco, controlo e governação da organização.

Em maio de 2018, tornou-se aplicável em toda a União Europeia o Regime Geral de Proteção de Dados (RGPD) e mais, recentemente em agosto de 2019, foi promulgada a Lei nº 58/2019 que se traduziu numa mudança de abordagem no que respeita às questões relativas à privacidade e segurança de dados pessoais, impondo-se como um novo desafio para as Organizações, trazendo novos riscos para a Gestão, nomeadamente ao nível da Auditoria Interna.

Decorrente desta nova regulamentação/Legislação de Proteção de dados, surgiu o Risco de incumprimento do RGPD, um risco de conformidade, que se veio a verificar ser para as Organizações, da maior relevância, designadamente a nível reputacional, com impacto significativo no mercado.

Estes novos riscos vêm implicar profundas alterações no Sistema de Controlo Interno das Organizações, veja-se o previsto no Regulamento, Artº 24º «Responsabilidade do responsável pelo tratamento» nº 1, que determina que,

> [...] o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

Tal deliberação imputa ao responsável pelo tratamento de dados a aplicação das medidas técnicas e organizativas que permitam não só mitigar os riscos como comprovar que as medidas mitigadoras estão em conformidade, são revistas e atualizadas, pressupondo para tal que exista monitorização e consequentes ações de melhoria.

Cabe, neste sentido, à Auditoria Interna enquanto terceira linha de defesa (também ao nível do RGPD) realizar as auditorias, de modo a garantir uma validação independente e

objetiva, suportada em evidências, da conformidade face aos requisitos do regulamento e legislação, mas, igualmente apurar, se os controlos existentes são efetivos e suficientes para a mitigação dos riscos e quais as melhorias a implementar.

No entanto, na alínea a), do Art.º 11º, da Lei 58/2019 são, ainda, definidas como «Funções do Encarregado da Proteção de Dados», para além das previstas nos Art.ºs 37 e 39.º do RGPD,

> [a]ssegurar a realização de auditorias, quer periódicas, quer não programadas.

Levando a que se coloque a seguinte questão: Como diferenciar o papel da Auditoria Interna das atribuições do Encarregado da proteção de dados, em matéria de Auditorias ao RGPD?

Ora, na visão do auditor interno, tal não parece significar que a execução destas auditorias, caiba ao EPD ou que esteja ao seu nível de atuação fazê-lo. Tendo como referência o modelo das três linhas de defesa, pode-se constatar que as funções do EPD/DPO, se enquadram no âmbito da segunda linha e não da terceira linha, esta última, correspondendo à Auditoria Interna.

Perseguindo este entendimento, desenvolveu-se nesta Dissertação, uma investigação sobre o papel da Auditoria Interna no Regime Geral de Proteção de Dados, enquanto terceira linha de Defesa, por contraponto com as funções a assegurar pelo Encarregado de Proteção de dados, no que respeita à realização das auditorias neste âmbito, no sentido da sua clarificação, tendo-se concluido que a distinção entre estes papeis, não é totalmente clara.

Palavras-Chave: Auditoria Interna; Regime Geral de Proteção de Dados (RGPD); Modelo das Três linhas de Defesa; Terceira Linha de Defesa; Encarregado de Proteção de Dados.

Abstract

According to the Three Line of Defense Model, published on September 21, 2010 by FERMA and ECIIA in the Guidance on the 8th EU Company law, Internal Audit, as an independent area, is responsible for an objective and exempt assessment of risk management, control and governance of the organization.

In May of 2018, the General Data Protection Regulation (GDPR) became applicable throughout the European Union and more recently in August 2019, Law 58/2019 was enacted, which translated in a change of approach with regard to issues related to privacy and security of personal data, imposing itself as a new challenge for Organizations, it brought new Risks for Management, namely in terms of Internal Audit.

As a result of this new regulation/Data Protection Legislation, The GDPR non-compliance risk arose, a compliance risk, which proved to be of the utmost relevance for Organizations, namely at reputational level, with a significant impact on the Market.

These new risks imply profound changes in the Organizations' Internal Control System, according with the Regulation, Art. 24 «Responsibility of the controller» nr.1, determines that,

> [...] the controller shall implement appropriate technical and organizational to ensure and be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Such a decision imputes to the data controller the application of technical and organizational measures that allow not only to mitigate risks, but also to prove that the mitigating measures are in conformity, are reviewed and updated, assuming that there is monitoring and consequent improvement actions.

In this sense, it is up to the Internal Audit as the third line of defense (also at the level of the GDPR) to carry out the audits, in order to guarantee an independent and objective validation, supported by evidence, of the compliance with the requirements of the regulation and legislation, but, also to ascertain, whether the existing controls are effective and sufficient to mitigate risks and what improvement actions should be implemented.

However, in Article 11 (a), of Law 58/2019, they are also defined as “Data Protection Officer Functions”, in addition to those provided for in Articles 37 and 39 of the GDPR,

> [e]nsure the performance of audits, whether periodic or unscheduled.

Leading to the following question: How to differentiate the role of Internal Audit from the duties of the Data Protection Officer, in terms of Audits to the GDPR?

Although, in the view of the internal auditor, this does not seem to mean that the execution of these audits is the responsibility of the EPD or that it is at its level of performance to do so. Having as reference the model of the three lines of defense, it can be seen, that the functions of the EPD / DPO, fall within the scope of the second line and not the third line, the latter, corresponding to the Internal Audit.

Pursuing this understanding, this dissertation developed an investigation into the role of Internal Audit in the General Data Protection Regime, as the third line of defense, in contrast to the functions to be performed by the Data Protection Officer, with regard to the carrying out audits in this area, in order to clarify them, having concluded that the distinction between these roles is not entirely clear.

Key Words: Internal Audit; General Data Protection Regime (GDPR); Three lines of defense model; Third Line of Defense; Data Protection Officer.

Índice

Índice de Tabelas

Índice de Gráficos

Índice de Figuras

Lista de Abreviaturas

AIPD – Avaliação de Impacto sobre Proteção de Dados

DPIA – *Data Protection Impact Assessment*

DPO – *Data Protection Officer*

ECIIA – *European Confederation of Institutes of Internal Auditing*

EPD – Encarregado de Proteção de Dados

ERM – *Enterprise Risk Management*

FERMA – *Federation of European Risk Management Associations*

FIP – *Fair Information Practices*

IIA- *Institute of Internal Auditors*

IPAI- Instituto Português de Auditoria Interna

PIA –*Privacy Impact Assessment*

RGPD – Regime Geral de Proteção de Dados

1 Introdução

A presente Dissertação enquadra-se no âmbito do Mestrado em Auditoria do Instituto Superior de Contabilidade e Administração de Lisboa (ISCAL) e tem como tema:

«**O Papel da Auditaria Interna no Regime Geral de Proteção de Dados, enquanto terceira linha de Defesa».**

O tema foi abordado por contraponto com as funções a assegurar pelo Encarregado de Proteção de Dados quanto às auditorias a realizar neste âmbito, de modo a clarificar o papel dos Auditores Internos e o papel que cabe aos Encarregados da Proteção de dados, não numa lógica disruptiva, mas antes numa perspetiva holística e de melhoria contínua, de modo a salvaguardar e acrescentar valor às Organizações e incrementar os níveis de confiança no mercado.

1.1 Relevância do Tema Abordado

O Regulamento Geral de Proteção de Dados (RGPD) é uma realidade incontornável que vem a acontecer mais efetivamente desde maio de 2018, no panorama jurídico da União Europeia, trazendo uma preocupação atual, transversal e generalizada às Organizações, sejam estas entidades privadas ou publicas, todas procuram da melhor forma adaptar-se às novas obrigações legais impostas por este Regulamento e aos novos riscos que daí decorrem e por consequência das alterações profundas que implicam no sistema de controlo interno das mesmas, assim como os novos desafios que trazem à Auditoria Interna.

O Risco de incumprimento do RGPD, é o risco que mais diretamente resulta da entrada em vigor do novo regulamento e da Lei nacional 58/2019, que consoante a atividade da empresa, assim se pode apresentar como um risco com impacto potencial de maior ou menor significância, não só ao nível financeiro como reputacional e por consequência com reflexo na confiança do mercado.

Às empresas que passaram a fase inicial de adaptação e implementação de práticas que acautelem o cumprimento dos requisitos do RGPD e controlos para mitigar os riscos decorrentes deste quadro regulamentar, coloca-se agora um novo desafio, o de avaliar se

as medidas implementadas permitem efetivamente corresponder aos objetivos e se as mesmas são as mais adequadas à realidade atual e à dinâmica própria de cada empresa, cabendo à Auditoria Interna no âmbito das suas funções e enquanto terceira linha de defesa, pela sua objetividade e independência dar o seu melhor contributo, para a melhoria contínua.

Mas qual o papel da Auditoria Interna na aplicação e observância dos requisitos do RGPD? E qual o seu nível de intervenção? São algumas das questões que se colocam às Organizações.

Tanto mais, que a Lei 58/2019 (de 08 de Agosto) determina, no seu Art.º 11º «Funções do Encarregado de Proteção de Dados» na alínea a) que este deve «[a]ssegurar a realização de auditorias, quer periódicas, quer não programadas.»

Pondo-se desde logo às Organizações a questão de como distinguir no respeitante às Auditorias ao RGPD, em que se consubstancia o assegurar das auditorias e qual efetivamente o papel do Encarregado de Proteção de dados (EPD) e o papel da Auditoria Interna?

A clarificação das atribuições de cada um, será determinante para que não se perca a objetividade e independência e haja ganhos efetivos de eficiência dos processos e da Organização.

Acresce que também o Modelo das três linhas de Defesa, aqui considerado como referencial e como base para o estabelecimento do Sistema de Gestão de Risco e Controlo Interno e um dos Modelos de Gestão de Risco com maior expressão a nível organizacional mundial, ter sido repensado, num projeto liderado pelo IIA com a participação de vários especialistas, resultando na sua revisão.

1.2 Objeto e objetivo

Esta Dissertação teve como objeto a análise do Papel da Auditoria Interna aplicada ao RGPD, pelos novos desafios e riscos trazidos pelo Regulamento, assim como das exigências que decorrem da Lei 58/2019, ao nível de Auditoria Interna, face às responsabilidades atribuídas ao Encarregado de Proteção de dados em matéria de

Auditoria, tendo presente o Modelo das três linhas de Defesa, enquanto referencial para o estabelecimento do Sistema de Gestão de Risco e Controlo Interno nas Organizações.

Neste sentido, foi definido como objetivo do presente trabalho clarificar o papel da Auditoria Interna enquanto terceira linha de defesa, por contraponto com o papel recentemente determinado pelo Regulamento Geral da Proteção de Dados e pela Lei 58/2019, que atribui como função do Encarregado da Proteção de Dados (EPD), entre outras, o de assegurar a realização de auditorias.

Por forma a corresponder a este objetivo foram levantadas as seguintes hipóteses:

Hipótese 1 - Existe relação entre o nível de clareza com que é entendido o papel da Auditoria Interna no RGPD e a observância na Organização do Modelo das três linhas de defesa.

Hipótese 2 - O nível de preparação da Auditoria Interna para corresponder aos novos desafios trazidos pelo RGPD, relaciona-se com a proteção de dados ser uma prioridade na gestão da informação nas Organizações.

Hipótese 3 - Existe relação entre o grau de maturidade (anos) na função de auditor e o entendimento das funções atribuídas no âmbito do RGPD ao EPD/DPO quanto às auditorias a assegurar neste âmbito.

Hipótese 4 – O grau de preparação tecnológica das Organizações para o cumprimento do RGPD está relacionado com existência de um EPD/DPO ou entidade externa responsável pela proteção de dados na Organização.

Hipótese 5 - A existência nas Organizações de um Encarregado da proteção de dados ou entidade externa com esta responsabilidade relaciona-se com os procedimentos vigentes na Organização darem resposta aos requisitos do RGPD.

Hipótese 6 –Existe relação entre o estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD e a preparação da Auditoria Interna para responder aos novos desafios que este novo enquadramento traz.

1.3 Metodologia e Estrutura da Dissertação

A presente Dissertação integra as fases referentes ao método de investigação científica que se pretende seguir para o desenvolvimento da mesma, com vista à obtenção de resultados objetivos e seguros, tendo-se estruturado em três grandes fases.

Numa primeira fase e tendo em conta o objetivo definido, foi aprofundada a exploração teórica e revisão da literatura no que respeita ao tema e conceitos, designadamente, sobre a Auditoria Interna, o Modelo das Três Linhas de Defesa (incluindo a sua evolução), assim como do RGPD e das implicações da nova Lei 58/2019, que veio trazer novos riscos e definir novos papeis, o que implica da parte das Organizações um esforço de clarificação, designadamente no que respeita ao papel da Auditoria Interna, face às funções atribuídas ao Encarregado de Proteção de dados em matéria de auditorias a assegurar ao RGPD. Correspondendo ao capítulo 2 da Dissertação.

Na fase seguinte, (capítulo 3) com a realização de um questionário informático, pretendeu-se obter respostas que permitissem concluir sobre o que pensam os auditores internos a exercer funções em Portugal (população alvo), sobre o papel da Auditoria Interna no RGPD enquanto terceira linha de defesa. Tendo contado com o apoio do IPAI para a divulgação do questionário.

Numa terceira e última fase, de generalização, retiraram-se as conclusões decorrentes da análise estatística das respostas obtidas ao questionário, para assim se apresentarem de forma fundamentada os resultados da investigação, no capítulo 4 da Dissertação.

2 Enquadramento Teórico e Revisão da Literatura

Neste capítulo pretendeu-se efetuar um enquadramento teórico dos principais conceitos associados ao tema, resultantes da recolha de informação realizada, a qual se baseou em legislação e regulamentação, monografias, documentos digitais, livros, entre outros.

2.1 A Auditoria Interna – Conceito e evolução

Há registos históricos que apontam no sentido de os primórdios de auditoria remontarem ao Egipto e à Babilónia, em que as auditorias eram realizadas por fiscais que controlavam as atividades desenvolvidas nas grandes construções, assim como na fiscalização da cobrança de impostos e das movimentações de bens nos armazéns dos faraós.

De igual forma, estes registos referem que os imperadores Romanos tinham ao seu serviço altos funcionários nomeados para inspecionar as contas das diversas províncias do império.

Numa fase mais avançada da história de Portugal, no século XIV, no Brasil colonial, existia a figura do juiz colonial, pessoa destacada pela coroa Portuguesa, cuja principal função seria a de assegurar a correta cobrança dos tributos do tesouro português, e o apuramento com exatidão dos registos e a salvaguarda dos bens.

O conceito de auditaria às empresas, mais próximo da realidade atual, terá tido origem em Inglaterra nos séculos XVIII, XIX e surge como consequência da revolução industrial e dos novos modelos de gestão, em que quem gere o negócio não é necessariamente quem investe o capital.

Com a crise económica de 1929, surgiu a necessidade de se estabelecerem regras para as empresas cotadas em bolsa, tornando-se obrigatória a existência de auditorias independentes, às contas dessas empresas, auditorias contabilísticas e financeiras.

As empresas começam a recorrer aos serviços de outras empresas para a realização de auditorias externas, independentes e assim assegurar aos seus acionistas e investidores, que o reporte das contas (balanços) apresentado pelos gestores como resultante da

atividade empresarial (industrial/comercial) refletia fielmente a situação financeira das suas empresas.

Os auditores externos enquanto profissionais que avaliavam as contas das empresas necessitavam de ter acesso a documentação, às transações realizadas e às respetivas contas. Para efeito de apresentação das contas, documentos e comunicação com os profissionais externos, eram nomeados colaboradores das próprias empresas, que pela sua interação com os auditores externos, foram adquirindo experiência e conhecimentos sobre o trabalho que estes profissionais desenvolviam.

As empresas não tardaram a perceber que ao potenciarem o desenvolvimento desses conhecimentos adquiridos por esses colaboradores, poderiam eles próprios realizarem, se não todo, parte dos serviços que eram assegurados pelos auditores externos, contribuindo para reduzir custos e simultaneamente melhorar o controlo das contas das empresas.

Por outro lado, com o alargamento dos mercados internacionais e a dispersão dos processos produtivos os gestores das empresas perceberam que as avaliações anuais realizadas pela auditoria externa não eram suficientes.

De igual forma, a impossibilidade de supervisionar todas as atividades veio realçar a necessidade de as empresas implementarem normas e procedimentos internos no sentido de ser assegurado o desempenho e a fiabilidade contabilística, que de nada serviriam se não houvesse ao nível interno um acompanhamento e verificação sobre a sua aplicação prática por parte dos colaboradores da empresa.

Pode dizer-se que nascia assim a função de auditor interno, em que um grupo de colaboradores da confiança da gestão, por serem colaboradores da própria empresa a exercer funções anteriormente realizadas pelos auditores externos, foram denominados auditores internos.

Os auditores internos, inicialmente auxiliares de verificação, apoiavam e preparavam a documentação destinada à apresentação aos auditores externos, mas asseguravam igualmente a verificação da documentação e da contabilização relativa às transações realizadas assim como a conferência de valores.

Nas empresas de maior dimensão e dispersas geograficamente, os auditores realizavam deslocações às suas filiais, quer a nível nacional quer internacional, no sentido de verificar também aí, se as operações realizadas cumpriam com as normas e procedimentos estabelecidos pela empresa.

Com a evolução do mundo empresarial e o crescimento/desenvolvimento das empresas, os auditores internos passaram a abarcar um mais alargado e transversal leque de áreas de análise e as suas funções e competências ultrapassaram em muito, a conferência de valores e de documentos contabilísticos.

O conceito de Auditoria Interna como hoje é conhecido, "Auditoria Interna moderna" surge por volta de 1940 nos Estados Unidos da América. Este novo conceito resultou de um conjunto de modificações sucessivas que foram ocorrendo, consequência também da sua relevância para o mundo empresarial.

Surge como algo mais abrangente que não se resume à salvaguarda dos ativos ou à deteção da fraude. Os auditores internos deixaram de ser meros conferentes e/ou inspetores, no início, em regra subordinados à área da contabilidade, passando a desempenhar funções, de controlo administrativo, cujo objetivo consistia em medir e avaliar a eficácia dos fluxos operacionais e aferir sobre a efetiva aplicação dos controlos internos em geral, conquistando um papel de assessoria e apoio à gestão das organizações e contribuindo assim para uma maior credibilização da função e a acrescentar valor.

São várias as definições de Auditoria Interna, vejam-se algumas seguindo como fio condutor a sua ordem cronológica:

O IIA – *Institute of Internal Auditors*, começa por definir em 1978, a Auditoria Interna como:

> [u]ma actividade de avaliação independente estabelecida dentro da organização como um serviço à organização. É um controle que funciona examinando e avaliando a adequação e a efetividade de outros controles. […]

De acordo com Uhl e Fernandes (1981: 17) a Auditoria Interna define-se como:

> [ta]refa designada a avaliar de forma independente, dentro de uma organização, as operações contábeis, financeiras e de outros tipos, no sentido de prestar um serviço

> à administração. É um controle administrativo, cuja função é medir e avaliar a eficácia de outros controles.

Attie (1986: 6) por seu turno, considera que:

> [a] Auditoria Interna pode auxiliar uma organização na melhoria dos seus negócios através da identificação de áreas que estejam mais expostas ao risco e da sugestão de melhorias.

Já, Sawyer (2003: 10), a quem foi atribuído o título de pai da Auditoria Interna moderna, vem defini-la como:

> [u]ma avaliação sistemática e objectiva realizada por auditores internos das diversas operações e controlos de uma organização, para determinar se (1) a informação financeira e operacional é precisa e confiável; (2) os riscos da organização são identificados e posteriormente minimizados; (3) os regulamentos e as políticas internas e procedimentos são seguidos; (4) os critérios de funcionamento são seguidos; (5) os recursos são usados de forma eficiente e económica; e (6) os objectivos da organização são efectivamente alcançados.

Pickett (2005: 125) vem referir que a Auditoria Interna, é

> [u]ma actividade de garantia e de consultoria na medida em que avalia a capacidade dos controlos implementados evidenciando se a organização consegue gerir bem o risco.
>
> A Auditoria Interna melhora as operações de uma organização numa perspectiva de melhoria contínua. […]

Segundo a perspetiva reformulada do IIA - *The Institute of Internal Auditors* e de acordo com o IPAI – Instituto Português de Auditoria Interna(2013:5) a Auditoria Interna é por definição:

> [u]ma actividade independente, de garantia e de consultoria, destinada a acrescentar valor e a melhorar as operações de uma organização. Ajuda a organização a alcançar os seus objectivos, através de uma abordagem sistemática e disciplinada, na avaliação e melhoria da eficácia dos processos de gestão de risco, de controlo e de governação.

Para Martins e Morais (2013: 91)

> [a] auditoria é uma função contínua, completa e independente, desenvolvida na entidade, por pessoal desta ou não, baseada na avaliação do risco, que verifica a existência, o cumprimento, a eficácia e a otimização dos controlos internos e dos processos de *Governance*, ajudando-a no cumprimento dos seus objectivos.

De acordo com Pinheiro (2014: 55),

> [a] Auditoria Interna é o controlo dos controlos, instituído numa empresa ou organização e visa contribuir para a promoção da economia, eficácia e eficiência das operações desenvolvidas. […]

Pese embora as diferentes definições, salienta-se como aspeto fundamental e consensual a necessária independência, da Auditoria Interna, enquanto condição essencial para o cumprimento do seu propósito maior, acrescentar valor às Organizações, trazer confiança à gestão através das suas análises imparciais, isentas, suportadas em factos/evidencias, verificáveis/rastreáveis, contribuindo assim para a otimização dos processos e sua transparência, pela objetividade de critérios em que baseia os seus julgamentos.

2.1.1. O Futuro da Auditoria Interna é já hoje

Não é de hoje que os auditores internos consideram no âmbito dos seus trabalhos e preocupações os riscos associados às novas tecnologias de informação e informáticos. A crescente utilização do correio eletrónico e das redes sociais como meio preferencial de comunicação e de desenvolvimento do negócio, nomeadamente os negócios on-line, veio potenciar os riscos relacionados com a segurança da informação e com a proteção dos dados, razão pela qual os auditores internos viram uma vez mais a necessidade de se prepararem para os novos desafios e munir-se de competências e ferramentas que lhes permitissem dar resposta e se possível antecipar-se às novas necessidades deste mundo cada vez mais informatizado, dominado pelo digital e de tecnologias avançadas, em que a robótica e/ou a inteligência artificial já não são obra da ficção cientifica, mas uma realidade atual e em franca expansão.

De acordo com um recente artigo de opinião da PWC, Auditoria Interna| Artigo de opinião | hits| PwC Portugal (15/01/2020) os auditores internos vêm-se cada vez mais pressionados para criarem valor para as Organizações e vêm igualmente as valências e competências necessárias ao desempenho das funções a aumentar e a diversificarem-se.

Segundo José Miguel Teixeira, Manager da PwC:

> Os diferentes desafios na interação com reguladores, gestores operacionais, com a gestão de risco, e com a gestão de topo das organizações criam uma necessidade de flexibilidade da função de Auditoria Interna.

No sentido de potenciar a criação de valor para as Organizações, a Auditoria Interna e os seus responsáveis devem atuar, de modo a:

- Desenvolver competências sólidas e orientadas para as necessidades do negócio e evolução do mercado;
- Coordenar-se com as funções de gestão de risco corporativo (*Enterprise risk management* (ERM));
- Ter em consideração os riscos potenciais, emergentes nas atividades de Auditoria Interna;
- Prestar um serviço distinto da auditoria de conformidade (associada apenas à verificação).

Nesse pressuposto, foram recentemente identificados oito atributos, como sendo os que mais poderão contribuir para o desenvolvimento efetivo da Auditoria Interna e para a criação de valor para as organizações, seja qual for a sua dimensão e/ou âmbito do trabalho. Veja-se a Figura 2.1:

Figura 2.1 - Atributos da Atual Auditoria Interna para a criação de valor

Fonte: https://www.pwc.pt/pt/hits/artigos-opiniao/jose-teixeira.html

Assim, a Auditoria Interna tem de estar preparada, cada vez mais, para realizar auditorias de ampla diversidade e complexidade pondo à prova a sua capacidade de adaptação a novas e inesperadas circunstâncias. Veja-se o caso da atual pandemia por Covid-19, um acontecimento à escala global, que veio desafiar ainda mais as Organizações que de um dia para o outro viram expostas a nu as suas fragilidades, mas também novas oportunidades para se reinventarem, assim como aos seus negócios.

Apesar das contingências o mundo continuou a girar e as Organizações adaptaram-se à nova realidade da melhor forma que conseguiram, em grande parte graças às novas tecnologias. Realidade que teve também impacto na função de Auditoria Interna e que implicou de algum modo a sua reorganização e mudança, designadamente dos métodos de trabalho, o recurso ao teletrabalho tornou-se essencial, o reforço da utilização de ferramentas de data analytics assim como a utilização de plataformas digitais (Teams, Zoom, entre outras) que passaram a substituir as tradicionais salas de reunião, de formação e/ou fóruns, permitiram aos auditores prosseguir com a sua atividade e contínuar a criar valor para as Organizações.

O XV Fórum do IPAI sobre o tema "Auditoria Interna em Ambiente de Pandemia" veio demonstrar que a proteção de dados, neste contexto, acentuou-se enquanto preocupação das Organizações, enquadrando-se no *top ten* dos principais riscos, apenas ultrapassado pelo risco de fraude e pelo risco de segurança informática/cibersegurança, no topo deste ranking. O que vem reafirmar a atualidade e a pertinência do tema, assim como a relevância do papel que cabe à Auditoria Interna enquanto terceira linha de defesa, mas também de parceiro estratégico da gestão para a criação de valor e na mitigação dos riscos emergentes.

O presente é o futuro e o futuro é já hoje, para as Organizações e para a Auditoria Interna.

2.2 O Modelo das Três Linhas de Defesa

Figura 2.2 - Modelo das Três Linhas de Defesa

Fonte: IIA (*Institute of Internal Auditors*); FERMA (*Federation of European Risk Management Associations)*

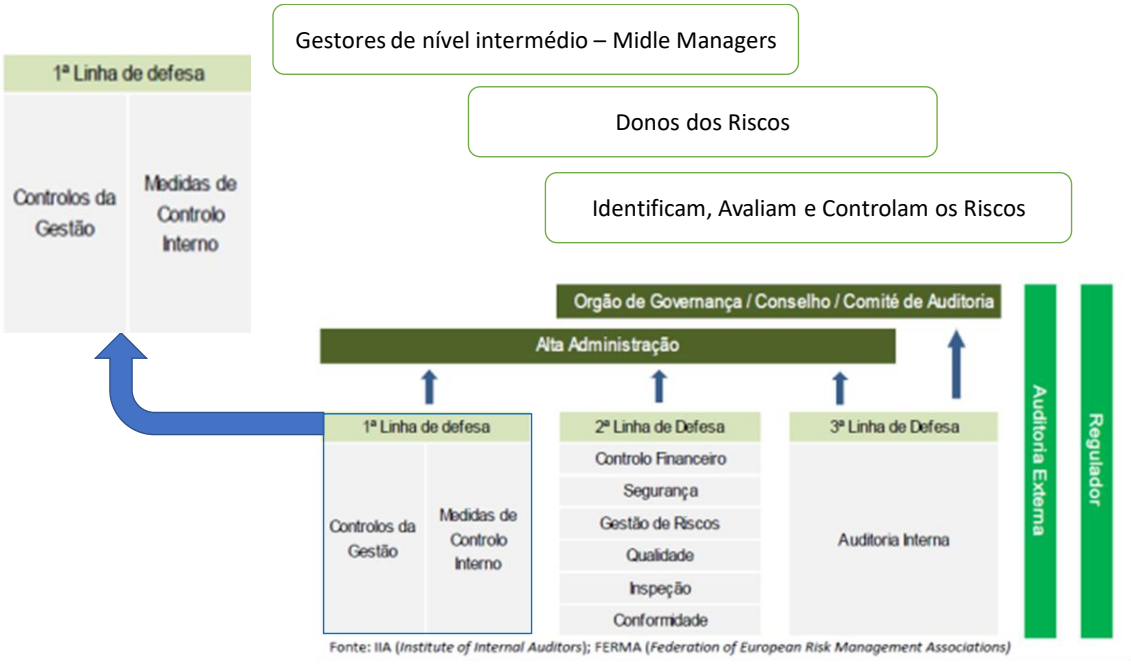
O Modelo das três linhas de defesa surgiu com a publicação em 21 de setembro de 2010, pelas FERMA (*Federation of European Risk Management Associations*) e ECIIA (*European Conference of Institute of Internal Auditors*) na *8th Company Law Directive* e foi desde então recomendado pelo IIA (*The Internal Institute of Auditors).*

Este modelo de gestão de risco foi o referenciado pelo IIA e um dos melhor acolhidos nas Organizações, por ser considerado um modelo que de forma simples e eficaz contribui para melhorar a comunicação da gestão de riscos e controlo, destacando-se como fator chave a sua transparência, relativa às responsabilidades atribuídas a cada uma das partes interessadas na condução dos negócios e operação da Organização, algo que se revela essencial para evitar lacunas, interpretações desajustadas e/ou situações de indefinição.

Neste modelo, a terceira linha de Defesa é assegurada pela Auditoria Interna, pelo seu papel nas Organizações, de independência e objetividade, o que lhe permite fazer julgamentos mais fidedignos e isentos sobre a eficácia da governação, relativamente à gestão do risco e do controlo interno.

2.2.1 A primeira linha de defesa - Controlo da Gestão e Medidas de Controlo Interno

Figura 2.3 - Primeira Linha de Defesa



Fonte: Elaboração própria com base na Declaração de Posicionamento do IIA «As Três Linhas de Defesa do Gerenciamento Eficaz de Riscos e Controles, 2013»

A primeira linha de defesa está focada na gestão operacional. Os gestores operacionais gerem o risco e têm responsabilidade sobre eles, o que na prática significa que, para cada risco identificado na empresa com impacto na gestão operacional, deva ser possível atribuir um responsável pela sua gestão.

A gestão dos riscos consiste na identificação, avaliação, controlo e mitigação dos riscos. A gestão também procura garantir que as atividades estejam de acordo com as metas e os objetivos estabelecidos pela organização e, no caso de se verificarem ineficiências no controlo, a implementação de ações corretivas.

A gestão operacional, no seu papel de primeira linha de defesa, deve desenvolver e implementar controlos e a supervisão, dos mesmos, por parte dos seus funcionários, atribuindo-lhes uma ordem hierárquica de responsabilidades.

2.2.2 A segunda linha de defesa – Funções de Gestão de Riscos e Conformidade

Figura 2.4 - Segunda Linha de Defesa

Fonte: Elaboração própria com base na Declaração de Posicionamento do IIA «As Três Linhas de Defesa do Gerenciamento Eficaz de Riscos e Controles, 2013»

A segunda linha de defesa pretende reforçar o controlo das atividades da primeira linha de defesa e auxiliar na sua monitorização e desenvolvimento. Esta é estabelecida com o objetivo de garantir que as funções de primeira linha sejam, adequadamente executadas e se concretizem em conformidade, assegurando a *compliance*.

A estrutura da segunda linha de defesa pode variar de acordo com o modelo hierárquico das empresas, mas, tipicamente, as funções desta linha incluem:

- Uma função (e/ou comité) de gestão de riscos que facilite e monitorize a implementação de práticas eficazes de gestão de riscos por parte da gestão operacional e auxilie os "donos" dos riscos a definir a meta de exposição ao risco e a reportar adequadamente informações relacionadas a riscos em toda a organização.
- Uma função de conformidade que monitorize diversos riscos específicos, tais como não conformidades face a leis e regulamentos aplicáveis. Neste aspeto, a

função reporta separada e diretamente à alta administração e, em alguns setores do negócio, diretamente ao órgão de governação. Podem ser múltiplas as funções de conformidade existentes numa mesma organização, com responsabilidade por diversos tipos e específicos de monitorização da *compliance,* designadamente em áreas como, as da saúde e segurança no trabalho, ambiental e qualidade.

- Uma função de controlo que monitorize os riscos financeiros e questões de reporte financeiro.

As funções desempenhadas pela segunda linha de defesa, são independentes em relação à primeira linha, porém ainda têm subjacentes funções de gestão.

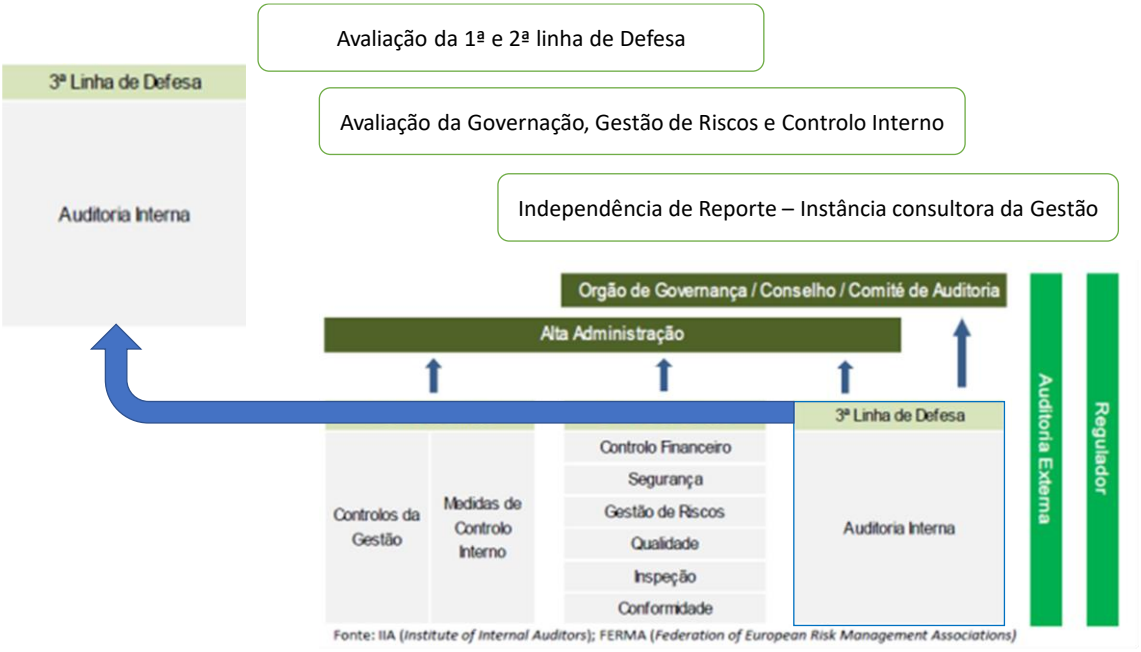
Assim sendo, a segunda linha pode influenciar e desenvolver o controlo interno e o sistema de riscos, assumindo-se por esse motivo, como uma linha importante, mas ainda sem garantir análises efetivamente independentes, aos órgãos de governação acerca da gestão de risco e do controlo interno.

As responsabilidades atribuídas a uma segunda linha de defesa podem incluir:

- Apoiar as políticas de gestão, definir papéis e responsabilidades e estabelecer metas para implementação;
- Fornecer estruturas de gestão de riscos;
- Identificar questões atuais e emergentes;
- Identificar mudanças no apetite ao risco implícito da organização;
- Auxiliar a gestão a desenvolver processos e controles para gerir os riscos;
- Dar orientações e formação sobre processos de gestão de riscos;
- Facilitar e monitorizar a implementação de práticas eficazes de gestão de riscos por parte da gestão operacional.
- Alertar a gestão operacional para questões emergentes e para as mudanças no cenário regulatório e de riscos.
- Monitorizar a adequação e a eficácia do controlo interno, a precisão e a integridade do reporte, a conformidade com leis e regulamentos e a resolução oportuna de deficiências.

2.2.3 A Terceira Linha de Defesa – Auditoria Interna

Figura 2.5 - Terceira Linha de Defesa



Fonte: Elaboração própria com base na Declaração de Posicionamento do IIA «As Três Linhas de Defesa do Gerenciamento Eficaz de Riscos e Controles, 2013»

A Auditoria Interna tem um nível de independência, de objetividade e um conhecimento transversal da Organização, o que lhe permite oferecer informações mais rigorosas e fidedignas, dada a sua isenção e integridade, sobre a eficácia da governação, nomeadamente no que respeita à gestão de risco e do controlo interno.

A Auditoria Interna, enquanto terceira linha de defesa, presta avaliação e aconselhamento independente à gestão.

O âmbito da avaliação, que é facultada à Administração e ao órgão de gestão é transversal e caracteriza-se, em regra pelo seguinte:

- Dar resposta sobre a eficiência e a eficácia das operações;
- A salvaguarda de ativos;
- A fiabilidade e a integridade dos processos de reporte;
- A conformidade com leis, regulamentos, políticas, procedimentos e contratos.

Inclui todos os elementos da estrutura de gestão de riscos e controlo interno:

- O ambiente geral de controlo interno;
- Todos os elementos da estrutura de gestão de riscos da organização (i.e. identificação de riscos, avaliação de riscos e resposta);
- Informação e comunicação;
- e monitorização.

Abrange a empresa como um todo, divisões, subsidiárias, unidades de operação e funções - incluindo os processos do negócio, como vendas, produção, marketing, segurança, funções orientadas para o cliente e operações - assim como funções de suporte (por exemplo, contabilização de receitas e despesas, recursos humanos, compras, gestão de infraestruturas e ativos, inventário e tecnologias de informação).

Assim, pode dizer-se que a Auditoria Interna tem um papel de grande importância, funcionando como uma alavanca para a melhoria contínua das Organizações, independentemente da dimensão das mesmas, pelo contributo que pode dar, designadamente em ambientes complexos, para garantir a eficácia e eficiência dos seus processos de governação e da gestão de riscos no sentido de acrescentar valor e ser uma mais valia.

Para que tal se concretize, a função de Auditoria Interna deverá ser independente, com uma equipa adequada, orientada para os objetivos estratégicos da Organização e dotada de recursos com competências multidisciplinares, que permita:

- Atuar de acordo com as normas internacionais reconhecidas para a prática de Auditoria Interna;
- Reportar a um comité de auditoria e/ou órgão não executivo do Conselho de Administração (por exemplo ao Presidente do Conselho), de modo a cumprir com as suas responsabilidades de forma, efetivamente independente;
- Ter uma linha de reporte ativa e eficaz ao órgão de governação.

2.2.4 Críticas ao Modelo das Três Linhas de Defesa

Pese embora, o Modelo das Três linhas de Defesa não tenha sido uma criação do IIA, este Instituto foi um forte impulsionador deste Modelo, tendo em 2013 publicado uma declaração de posicionamento de apoio ao mesmo, que se julga motivado em grande parte pelo forte reconhecimento de um papel crucial à Auditoria Interna, enquanto terceira linha de Defesa e enquanto prestador de avaliação independente e objetiva, às Organizações.

Este modelo que veio a ganhar ampla aceitação e popularidade ao longo de vários anos, tendo sido adotado por inúmeras Organizações, atraídas pela sua simplicidade e clareza na definição de responsabilidades ao nível da gestão e controlo de riscos, segmentadas em três linhas distintas de defesa, veio nos últimos anos a ser alvo de algumas críticas e vozes dissonantes, referindo por um lado que as suas linhas fixas, o tornam inflexível face aos atuais desafios, à dinâmica que as constantes mudanças dos mercados exigem da gestão e por outro lado, que o seu foco sobre a defesa limita a sua eficácia.

A questão essencial é que não deve existir uma abordagem única, dado que cada Organização enfrenta riscos, desafios e oportunidades distintos que agregam variabilidade aos seus desafios. Sendo de toda a relevância encontrar a combinação certa de normas, práticas, controlos, estruturas e processos que apoiem a boa gestão, de modo a potenciar o sucesso das Organizações.

De igual forma, os cenários de risco cada vez mais complexos e em constante evolução, os rápidos avanços tecnológicos, podem constituir tanto uma ameaça quanto uma oportunidade. Além do mais, conforme as Organizações desenvolvam novas abordagens para gerir e controlar os seus riscos, as linhas do modelo podem tornar-se menos definidas, menos segmentadas, podendo levar em alguns casos à existência de responsabilidades partilhadas, da qual resulta a expressão «linhas difusas».

A par da eventual necessidade do modelo evoluir para linhas de defesa mais flexíveis «linhas difusas», está o facto deste modelo ter o seu foco em «proteger valor» sem dar a devida relevância à necessidade de ir mais além e se constituir como um fator determinante para melhorar o valor, isto é, de acordo com a mais recente abordagem do IIA a Auditoria Interna «deve ser reconhecida como fundamental para melhorar e proteger o valor organizacional». Para o efeito a Auditoria Interna deverá ser

reconhecida como mais do que uma terceira linha de proteção de valor, mas um valor em si mesmo.

Com o apoio de especialistas em gestão dos setores público e privado, académicos, reguladores e representantes das quatro grandes empresas de Auditoria a nível internacional, o IIA lançou um projeto para atualizar este modelo.

De acordo com o Presidente do Conselho do IIA, Naohiro Mouri, no comunicado que anunciou à imprensa o ambicioso projeto, que o:

> [N]osso objetivo não é substituir as Três Linhas de Defesa ou inventar um novo modelo, mas garantir que ele possa acomodar as nuances e dinâmicas que vemos em diferentes organizações, para que elas possam alavancar e aprender umas com as outras de forma mais eficaz e estratégica.

Naohiro Mouri, refere ainda, que:

> [T]ambém devemos adotar o conceito de que o risco vai além da defesa. A incerteza cria riscos e cria oportunidades. Deve-se considerar ambos os lados na tomada de decisões e no planejamento em todos os níveis. As organizações devem decidir a maneira mais apropriada de alocar e estruturar os recursos e as responsabilidades dentro de suas organizações, usando as Três Linhas de Defesa a seu favor.

O objetivo do IIA foi então, o de encontrar a melhor forma de atualizar o modelo das Três Linhas de Defesa por forma a refletir as mudanças na gestão de riscos e governação modernos, e simultaneamente preservar a sua abordagem direta e clara. Isto é, tornar o modelo mais flexível, adequado a todos os setores e compatível com os desafios e oportunidades que os riscos acarretam.

Este projeto foi liderado por uma equipa de trabalho formado por especialistas em *governance* e contou com a vasta experiência de um grupo consultivo adicional, composto por 30 membros. Incluiu uma revisão abrangente das abordagens de governação a nível mundial, incorporando comentários públicos por meio de um processo formal de exposição, que resultou numa nova declaração de posicionamento do IIA, emitida em junho de 2019.

Nesta declaração de posicionamento o IIA veio reforçar o entendimento de que não se pretendia uma revisão integral do modelo, mas antes aumentar e melhorar os seus

pontos fortes, de modo a corresponder às diversas e atuais necessidades organizacionais, no sentido de potenciar e criar valor.

Na tabela seguinte apresentam-se os pontos fortes e as oportunidades de melhoria, identificadas na declaração de posicionamento do IIA em junho de 2019:

Tabela 2.1 - Pontos fortes vs Oportunidades de Melhoria do Modelo das Três Linhas

Pontos Fortes	Oportunidades de Melhoria
É simples, fácil de entender e fácil de comunicar.	
Foca-se na importância de uma gestão eficaz de riscos e controlos.	Contextualizar a gestão de riscos e controlo como parte da governação, e de apoio ao sucesso organizacional e à criação de valor.
Apoia os esforços da organização para responder a oportunidades e ameaças.	Encorajar uma abordagem proativa e reativa ao alcance das metas da organização.
Consiste numa base para a clareza e eficiência na organização de atividades e recursos de gestão de riscos e controlo.	Enfatizar a importância da coordenação e colaboração, em alinhamento com as prioridades estratégicas e necessidades operacionais.
Descreve papeis desempenhados por cada uma das principais funções e *stakeholders* externos que são relevantes para a gestão de riscos e controlo.	Facultar a clareza adicional aos papeis e responsabilidades das funções individuais e à sua contribuição conjunta para a governação, sucesso organizacional e criação de valor.
Descreve uma forma/meio de estruturar funções principais	Destacar as oportunidades para uma adoção mais flexível e ágil do modelo.
Tem sido amplamente adotado, especialmente por organizações e reguladores de serviços financeiros.	Considerar as diferenças organizacionais, principalmente quanto à dimensão, setor e maturidade; demonstrar a importância e permitir a pronta adoção por qualquer organização.

Pontos Fortes	Oportunidades de Melhoria
Reconhece o papel dos auditores externos e reguladores na gestão de riscos e controlo	Considerar outros *stakeholders* externos e o seu potencial contributo para a governação, o sucesso organizacional e a criação de valor.
Permite a pronta explicação do papel da Auditoria Interna como «terceira linha de defesa».	Expandir esse papel, reconhecendo a função de Auditoria Interna como parceira estratégica e consultora de confiança.
Fornece um *framework* útil para discussões sobre independência, objetividade e avaliação.	Considerar e explicar as «linhas difusas» e descrever as salvaguardas apropriadas.
É ilustrado por um gráfico conhecido e simples	Aprimorar a representação gráfica, fazendo refletir a evolução e a melhoria do modelo.

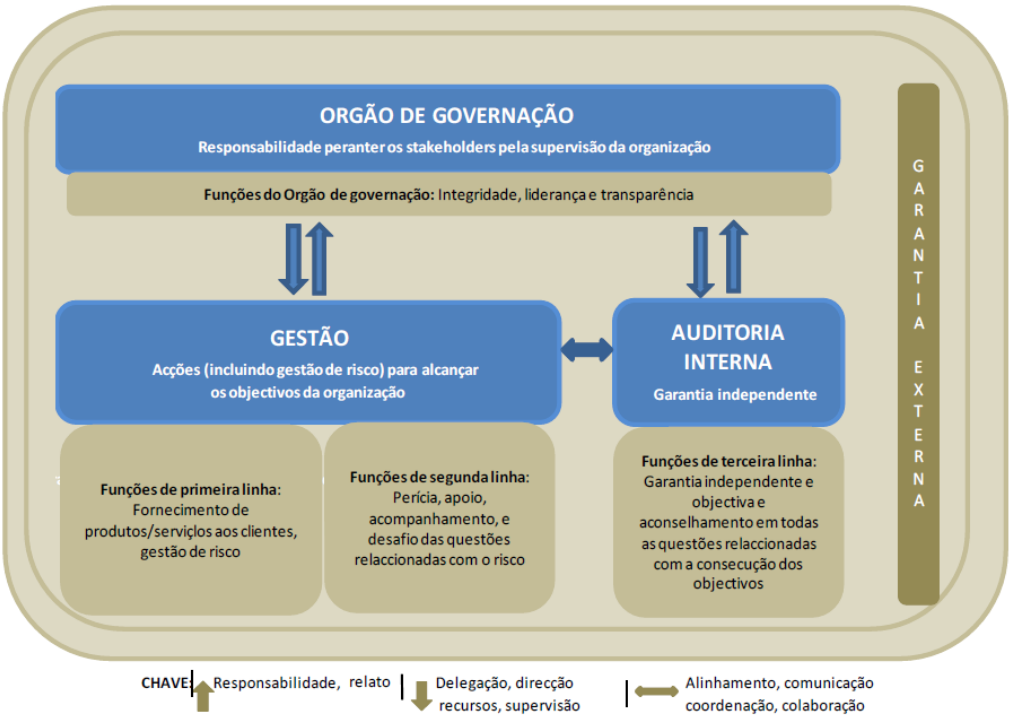
Fonte: Elaboração própria com base no «IIA Documento de Exposição Três Linhas de Defesa» Junho 2019

As melhorias apontadas pela equipa de especialistas, refletem assim, a preocupação quanto à governação e de que forma pode esta função, através da evolução do Modelo das Três Linhas, contribuir ativamente para promover o sucesso organizacional e a criação de valor, constituindo-se ela própria como uma mais valia para as Organizações.

2.2.5 Atualização das Três Linhas de Defesa e Evolução do Modelo

A 12 de Agosto de 2020, o IPAI publica a edição do Modelo das três Linhas do IIA, com a atualização das Três Linhas de Defesa, que traz uma nova visão e "promete" mudar a forma como as Organizações percecionam os riscos, os controlos, a comunicação, a prestação de contas e a avaliação/monitorização, mudança que apesar de ser uma evolução natural do anterior Modelo, se traduz em alterações relevantes. Como se pode constatar na figura seguinte (Figura 2.6):

Figura 2.6 - Atualização do Modelo das Três Linhas



Destaca-se como uma das grandes mudanças, o maior envolvimento do órgão de governação. No novo Modelo estão, claramente delineadas as funções e responsabilidades do órgão de governação, bem como da gestão e da Auditoria Interna, sem, contudo, que essas funções se limitem à gestão de riscos.

O foco na governação global/transversal das Organizações, veio reforçar a proteção e incrementar a criação de valor para as Organizações, passando de uma abordagem essencialmente defensiva/detetiva, para uma abordagem preditiva e de antecipação dos riscos, respondendo assim, a uma das principais críticas ao anterior Modelo, cuja abordagem defensiva assentava sobretudo na proteção e não tanto na criação de valor.

Salienta-se, no entanto, como a maior mudança, a identificação dos seguintes seis princípios base, nos quais o novo Modelo, assenta:

- Princípio 1 – Governação

A governação de uma Organização requer estruturas e processos adequados, que possibilitem:

- A responsabilização do órgão de governação, face aos *stakeholders*, pela supervisão da Organização com integridade, transparência e liderança.
- O desempenho de ações pela gestão (inclusive a gestão de risco) através de um processo de decisão baseado no risco e utilização dos recursos, no sentido do cumprimento dos objetivos estabelecidos.
- A garantia de fiabilidade e aconselhamento a assegurar por uma função de Auditoria Interna independente, de modo a trazer clareza e confiança e promover a melhoria contínua, suportada numa indagação rigorosa e comunicação perspicaz.

- Princípio 2 - O papel do Órgão de Governação

O Órgão de Governação deve assegurar que:

- Existem e estão em funcionamento estruturas e processos adequados a uma governação eficaz;
- Os objetivos e as atividades da organização estão alinhados com as prioridades definidas pelos *stakeholders*.
- Delega responsabilidades e disponibiliza recursos à gestão necessários à consecução dos objetivos da organização e, simultaneamente, assegura que são cumpridas as exigências legais, regulamentares e éticas;
- Estabelece e supervisiona uma função de Auditoria Interna independente, objetiva e competente, que deverá, por seu turno, garantir clareza e confiança nos progressos na consecução dos objetivos.

- Princípio 3 - A Gestão e funções de primeira e segunda linha

- A responsabilidade da gestão na consecução dos objetivos da organização inclui ambas as funções de primeira e segunda linha.
- As funções de primeira linha estão diretamente alinhadas com a entrega de produtos e/ou serviços a clientes da organização, incluindo as funções auxiliares.
- As funções de segunda linha apoiam a gestão de risco.

De acordo com o novo Modelo as funções de primeira e segunda linha podem misturar-se ou podem exercer-se, separadamente. Algumas funções de segunda linha podem ser atribuídas a especialistas, que fornecem o seu conhecimento, apoiam, monitorizam e incentivam os que desempenham funções de primeira linha.

As funções de segunda linha podem ainda, centrar-se em objetivos específicos da gestão de risco, tais como, conformidade com a legislação e regulamentos, e comportamento eticamente aceitável; controlo interno; segurança da informação e tecnologias; sustentabilidade; e garantia de qualidade.

Por outro lado, as funções de segunda linha podem assumir uma responsabilidade mais ampla, mais abrangente pela gestão de risco, tal como a gestão de risco empresarial (*Enterprise Risk Management*). No entanto, a responsabilidade pela gestão de risco permanece como parte integrante das funções de primeira linha e no âmbito da gestão.

De notar, que os termos «primeira linha», «segunda linha» e «terceira linha» são adotados do modelo original dado que as «linhas» não pretendem destacar elementos da estrutura, mas uma distinção útil entre funções. Por outro lado, o papel do órgão de governação constitui igualmente uma «linha», mas não terá sido adotado este conceito para evitar equívocos. De igual forma, a numeração (primeira, segunda, terceira) não implica operações sequenciais, muito pelo contrário, dado que todas as funções operam em paralelo.

- Princípio 4 - As funções de terceira linha

A Auditoria Interna é garante de independência e objetividade e presta serviços de consultoria destinados a melhorar a adequação e eficácia da governação e da gestão de risco, através de uma abordagem competente, sistemática e disciplinada, perícia e conhecimento. Ao reportar os seus resultados à gestão e ao órgão de governação, contribui para alavancar a melhoria contínua e consequentemente, reforçar a garantia de fiabilidade de outros contributos internos e externos.

De notar, que em algumas Organizações podem ser consideradas como de terceira linha outras funções, tais como funções de supervisão, inspeção, investigação, avaliação e melhoria, que tanto podem pertencer à função de Auditoria Interna, como existir separadamente.

- Princípio 5 - A independência da terceira linha

A independência da Auditoria Interna, das responsabilidades da gestão é fundamental para que seja assegurada a necessária objetividade, autoridade e credibilidade desta função. Tal é alcançado, pela responsabilidade que tem, perante o órgão de governação, associado ao facto de ter acesso sem restrições ao pessoal, recursos e aos dados necessários para completar o seu trabalho e a liberdade contra o enviesamento e interferência, no planeamento e prestação de serviços de auditoria.

- Princípio 6 - Criar e proteger o valor

Todas as funções ao trabalharem em conjunto, contribuem para a criação e proteção de valor, ao estarem alinhadas umas com as outras, e todas, com as prioridades dos *stakeholders*. O alinhamento das atividades é alcançado com comunicação, cooperação e colaboração. Isto garante a confiança, coerência e transparência da informação necessária à tomada de decisão baseada no risco.

Norman Marks, enquanto membro integrante do grupo consultivo de especialistas para a atualização do Modelo das três linhas de defesa, sobre o novo modelo - Modelo das três linhas - destaca que:

> [A] independência da Auditoria Interna em relação à gestão garante que ela esteja livre de obstáculos e preconceitos no planejamento e execução de seu trabalho, com acesso irrestrito às pessoas, recursos e informações de que necessita. É responsável perante o corpo diretivo. No entanto independência não implica isolamento. […]

Salientando ainda, como melhorias do Modelo, o seguinte:

- Não se trata apenas da defesa, trata-se de atingir os objetivos o que requere criação e proteção de valor.
- Reitera a mensagem consistente do IIA e torna-a ainda mais clara, no que respeita à responsabilidade da gestão, por atingir os objetivos e o sucesso da organização, com supervisão do corpo diretivo (o Conselho). Tal inclui compreender e abordar o que pode acontecer, o «risco».

- Ajuda as organizações a compreender as responsabilidades e os relacionamentos entre o conselho, administração, a Auditoria Interna e outros.
- Baseia-se em princípios sólidos e úteis.
- Reconhece que a designada segunda linha[1] é realmente parte da gestão, sendo agora um desafio, integrando funções como a jurídica, de conformidade, de segurança da informação, de gestão da qualidade e assim é abordada, reconhecendo que há alguma fluidez entre a primeira e a segunda linha.
- Enfatiza a necessidade de colaboração, a essência do GRC[2] que integra a capacidade de atingir objetivos (governança) de maneira confiável, simultaneamente aporta a incerteza (gestão de risco) e age com integridade (conformidade).
- Confirma igualmente que a gestão do risco contribui "para a concretização de objetivos e criação de valor, bem como para as questões de "defesa" e proteção de valor".
- A versão final do diagrama apresenta-se simples, sem necessidade de discutir se há três ou mais linhas.
- É menos sobre "linhas" do que sobre responsabilidades atribuídas "quem faz o quê e como colaboram" entre si, para o sucesso empresarial, embora continue a usar o conceito de "linhas".

---

[1] Alguma literatura considera que as funções de apoio (tal com RH, administrativa e manutenção instalações) são de segunda linha. Convirá esclarecer que o Modelo das Três Linhas considera que nas funções de primeira linha estão incluídas ambas as atividades de "front of house" e"back office", e nas funções de segunda linha atividades complementares focadas nas questões relativas ao risco. https://global.theiia.org/knowledge/chambers-portuguese/Pages/Novo-Modelo-das-Tres-Linhas-do-IIA-Oferece-Evolucao-Tempestiva-de-uma-Ferramenta-Confiavel.aspx

[2] No último relatório OCEG, Michael Rasmussen cita a definição oficial e atual do OCEG de GRC: «GRC é a capacidade de atingir objetivos [governança] de maneira confiável, ao mesmo tempo em que aborda a incerteza [gestão de risco] e age com integridade [conformidade].» (https://normanmarks.wordpress.com/2020/07/08/dysfunctional-grc/)

2.2.5.1 Funções Chave do Modelo das Três Linhas

Pese embora, as diferenças que possam existir nas Organizações ao nível da distribuição de responsabilidades, de acordo com o novo Modelo das Três Linhas são consideradas como funções chave, funções de alto nível que contribuem para fortalecer os princípios deste novo Modelo, as explicitadas, na Tabela seguinte:

Tabela 2.2 - Funções Chave do Modelo das Três Linhas

Órgão de Governação	**Funções Chave**
	Assumir perante os *stakeholders*, o compromisso pela supervisão da Organização, a monitorização dos seus interesses e a comunicação de forma transparente da prossecução dos objetivos estabelecidos.
	Promover a adoção de uma cultura de comportamento ético e responsável.
	Criar estruturas e processos de governação, incluindo comités auxiliares se necessário.
	Delegar responsabilidades e atribuir recursos à gestão de modo a atingirem os objetivos definidos pela Organização.
	Determinar o apetite ao risco da Organização e supervisionar a gestão de risco (incluindo o controlo interno)
	Manter a supervisão quanto à conformidade face às exigências legais, regulamentares e éticas.
	Estabelecer e supervisionar uma função de Auditoria Interna independente, objetiva e competente.

Gestão	**Funções Chave - De Primeira Linha**
	Liderar e orientar ações (incluindo a gestão de risco) assim como a aplicação dos recursos destinados ao alcance dos objetivos da Organização
	Manter uma permanente comunicação com o órgão de governação e reportar os resultados, reais e previsionais, face ao planeado, tendo em conta os objetivos da Organização e o risco.
	Estabelecer e manter estruturas e processos adequados à gestão das operações e risco (incluindo o contro interno).
	Garantir a conformidade face às exigências legais, regulamentares e éticas.
	Funções Chave – de Segunda Linha
	Agilizar e prestar apoio, monitorizar e impulsionar a gestão de risco, incluindo: - O desenvolvimento, concretização e melhoria contínua nas práticas de gestão de risco (inclusive o controlo interno) ao nível da entidade, processos e sistemas. - A concretização dos objetivos da gestão de risco, nomeadamente ao nível da conformidade com as leis, regulamentos e comportamentos eticos aceitáveis; controlo interno; segurança da informação e tecnologia; sustentabilidade; e de qualidade.
	Facultar análises e relatos no que respeita à adequação e eficácia de gestão de risco (incluindo o controlo interno)

Auditoria Interna	**Funções Chave**
	Manter a responsabilidade principal perante o órgão de governação e simultaneamente a independência das responsabilidades da gestão.
	Aportar garantia de fiabilidade independência e objetividade e prestar aconselhamento à gestão e ao órgão de governação quanto à adequação e eficácia do governo e da gestão de risco (incluindo o controlo interno) no apoio à concretização dos objetivos.
	Reportar faltas de independência e objetividade aos órgãos de governação e inclusão de salvaguardas quando necessário.
Prestadores Externos de Garantia de Fiabilidade	**Funções Chave**
	Fornecer uma garantia de fiabilidade adicional de forma a: - Responder às exigências legais e regulamentares no sentido de salvaguardar os interesses dos *stakeholders*; - Corresponder às solicitações da gestão e do Órgão de Governação de modo a complementar as fontes internas de garantia de fiabilidade.

Fonte: Elaboração própria com base no documento «O Modelo das Três Linhas do IIA» de 12/08/2020

Caberá agora às Organizações, avaliar na prática, se este novo Modelo responde à realidade empresarial atual e às suas cada vez maiores e mais diversas necessidades, o que apenas será apreciável no futuro.

2.3 Proteção de Dados – Conceito e evolução

Ao contrário do que se possa pensar as preocupações com a reserva da informação, não são algo novo. Ao longo da história universal, Imperadores, Reis e Rainhas, Nobres e Clérigos (os únicos que sabiam ler e escrever) trocavam correspondência escrita codificada para salvaguarda de informação de cariz pessoal a bem dos interesses políticos e socioeconómicos das nações.

Terá sido, no entanto, em meados do século XX (1950), após a II Guerra mundial, que se começou a escrever a história moderna da proteção de dados. Um conjunto de 10 países formando o Conselho da Europa, com o objetivo de promover o estado de direito, democracia e os direitos humanos abraçou a convenção Europeia dos Direitos do Homem tendo sido estabelecido no seu Art.º 8º que:

> [Q]ualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

Em Portugal, é em 1976, que a nova Constituição Portuguesa, no seu Artº 35º, atribui a

> […] todos os cidadãos o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização.

Em 1980 a Organização para a Cooperação e Desenvolvimento Económico (OCDE) tendo como objetivo criar um sistema de Proteção de dados em toda a Europa, publica as «Recomendações do Conselho relativas às Diretrizes sobre a proteção de privacidade e dos fluxos transfronteiriços de dados pessoais», no entanto estas recomendações não tinham caráter obrigatório e as diretrizes de privacidade variavam consoante o país, contrariando assim o propósito inicial.

Surgiu então, ainda no mesmo ano (1980), pelo *Council of the European Union* a proposta de criação de uma nova Diretiva a nível Europeu para a Proteção de dados, a Diretiva 95/46/EC, mantendo-se o propósito de uniformizar as leis dos diferentes países membros. No entanto e tratando-se de uma Diretiva, ainda havia espaço para cada país fazer a sua interpretação, em termos práticos sem grande acolhimento pelos países.

Em 1991, é aprovada em Portugal a Lei da Proteção de dados Pessoais face à informática - Lei nº 10/91, de 9 de abril – que estabelece como princípio geral, que

> [o] uso da informática deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada e familiar e pelos direitos, liberdades e garantias fundamentais dos cidadãos.

Tendo sido criada a Comissão Nacional de Proteção de Dados Pessoais Informatizados (CNPDPI) autoridade portuguesa de controlo, atualmente designada Comissão Nacional de Proteção de Dados (CNPD).

Em 1995 a UE aprovou a Diretiva 95/46/CE de Proteção de dados, do Parlamento Europeu e do Conselho, respeitante à Proteção das pessoas singulares quanto ao tratamento de dados pessoais e à livre circulação desses dados e em 1998 Portugal aprova a Lei 67/98 de 26 de outubro – Lei da Proteção de dados, que faria a transposição para a ordem jurídica portuguesa da Diretiva 95/46/CE.

Em 2001 o Regulamento 45/2001 veio estabelecer normas para a proteção de pessoas singulares quanto ao tratamento dos seus dados pessoais pelas instituições comunitárias. E em 18 de agosto de 2004, a Lei n.º 43/2004 é promulgada com o propósito de regular a organização e funcionamento da CNPD.

Em 2016, 27 de abril, é aprovado o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que viria a revogar a Diretiva 95/46/CE e a constituir o ponto de viragem nesta matéria.

2.3.1 Regulamento Geral de Proteção de Dados – RGPD

O Regulamento Geral de Proteção de Dados (RGPD) entrou em vigor a 25 de maio de 2018 e mais, recentemente, foi publicada a Lei nº 58/2019, a 08 agosto de 2019, que tem como objeto assegurar a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho de 27 de Abril de 2016 – Regulamento Geral de Proteção de Dados (RGPD) – Relativo à proteção das pessoas singulares no que respeita ao tratamento de dados pessoais e à livre circulação desses dados.

Para além de revogar a anterior lei de proteção de dados (Lei nº 67/98, de 26 de outubro) a nova lei fixa, regras específicas em matérias sobre as quais o RGPD tinha expressamente previsto que os estados membros pudessem ter alguma margem para adequar o regulamento à sua realidade, o que implica um esforço adicional de adaptação a esta realidade nova e em constante mudança e à qual as Organizações não poderão ser alheias.

Contudo, a nova lei, cuja entrada em vigor ocorreu a 09 de agosto de 2019, não deve ser interpretada, sem que seja tido em conta o previsto no RGPD, que a seguir se sintetiza, abordando os principais conceitos.

Nos termos do artigo 3.º do RGPD, o regulamento aplica-se ao tratamento de dados pessoais efetuado por entidades situadas na UE que procedam ao tratamento de dados de pessoas singulares e a qualquer entidade fora da UE que ofereça bens ou serviços a pessoas singulares na UE.

De acordo com o n.º 1 do artigo 4.º do RGPD, podem-se definir dados pessoais como sendo,

> [i]nformação relativa a uma pessoa singular identificada ou identificável […] como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social.

É no Artigo 6.º, que o Regulamento estabelece um dos princípios essenciais deste Regulamento, «Licitude do tratamento» definindo no seu n.º 1 que o tratamento de dados pessoais apenas «é licito se e na medida em que se verifique pelo menos uma […] das situações» previstas e contempladas nas suas alíneas, de a) a f).

Também conforme previsto no artigo 7.º do RGPD, a recolha de dados pessoais apenas pode ser feita com base no consentimento dos titulares dos dados. Este consentimento tem de ser dado por declaração escrita com linguagem clara e simples e deve ser fácil retirar o mesmo, caso o titular dos dados assim o entenda.

Outro aspeto fundamental é que, sempre que haja violação de dados, as entidades responsáveis pelo tratamento dos dados têm de notificar a autoridade de controlo até 72 horas após terem tomado conhecimento do mesmo e, caso implique um elevado risco

para os titulares dos dados, as entidades deverão imediatamente notificá-los, conforme previsto nos artigos 33.º e 34.º do RGPD.

Pelo incumprimento dos requisistos do RGPD podem ser aplicadas coimas, conforme disposto no artigo 83.º deste regulamento e mais, explicitamente previsto na Lei nacional artigo 37.º n.º 2, que estabelece para as contraordenações muito graves, identificadas no n.º 1 do mesmo artigo, que as mesmas serão punidas com coimas, diferenciando, no entanto, se se trata de uma grande empresa, uma PME (Pequena Média Empresa) ou de uma pessoa singular.

Estabelecendo que, no limite e caso se trate de uma grande empresa, as coimas a aplicar podem variar entre os 5 mil e os 20 milhões de Euros, ou 4% do volume de negócios global anual, a nível mundial, aplicando-se o que for mais elevado.

Já, se se tratar de uma PME a coima a aplicar pode variar entre os 2 mil e os 2 milhões de Euros, ou 4% do volume de negócios anual, a nível mundial, conforme o que seja mais elevado.

No caso de pessoas singulares também foram previstas coimas, que podem ir de mil a 500 mil Euros.

Este é sem dúvida um novo paradigma na segurança e proteção dos dados pessoais, levando as Organizações a pensar seriamente nos custos de não cumprimento com o legislado *«the cost of non-compliance»* e o seu impacto quer ao nível financeiro quer reputacional, na continuidade do negócio e na confiança do mercado.

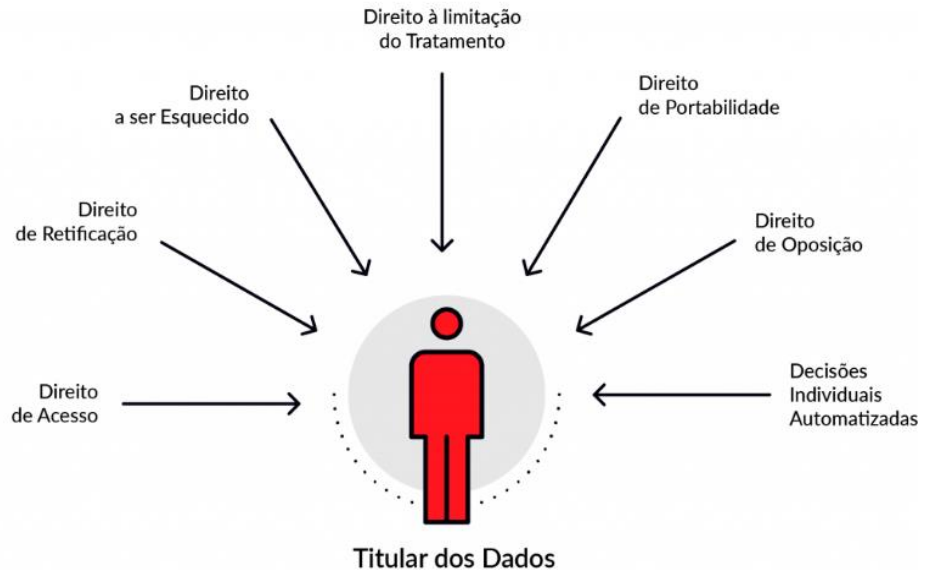
Em Portugal são já conhecidas algumas situações que resultaram em elevadas coimas, sendo o caso mais mediático, o do Hospital do Barreiro, multado em cerca de 400 mil Euros pela Comissão Nacional de Proteção de Dados (CNPD) por acesso indevido aos processos clínicos dos doentes, dados pessoais sensíveis, tendo sido identificadas três infrações muito graves:

- Incumprimento do princípio da integridade e confidencialidade, referente aos acessos e gestão dos utilizadores (*users*),
- Violação do princípio da minimização de dados *«need to know basis»* que deveria restringir o acesso indiscriminado a dados clínicos de doentes

- Incapacidade do responsável pelo tratamento dos dados em assegurar a confidencialidade dos dados pessoais e sensíveis, não existindo diferenciação ou controlo sobre os perfis de acesso atribuídos aos colaboradores, permitindo assim, indevidamente a todos, terem acesso a toda e qualquer informação existente nos sistemas.

Veja-se na figura abaixo (Figura 2.7) os Direitos previstos no âmbito do RGPD, no que respeita ao titular dos dados pessoais.

Figura 2.7 - Direitos do Titular dos Dados Pessoais



Fonte: https://rgpd.help/?gclid=EAIaIQobChMImZrfpta54gIVibbtCh3wLAK0EAAYASAAEgJHAPD_BwE

Estes Direitos têm obrigatoriamente de estar salvaguardados pelas Organizações, implicando que a gestão implemente mecanismos, processos que lhes garantam por um lado o cumprimento dos requisitos do regulamento, mitigando o Risco de incumprimento do RGPD, designadamente no que respeita ao previsto no Artº 24º «Responsabilidade do responsável pelo tratamento», que refere o seguinte:

> [T]endo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e

> poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

O que implica que as Organizações, para além de implementarem medidas que permitam cumprir o estabelecido no RGPD, tenham que evidenciar que essas medidas são monitorizadas e auditadas, pressupondo a respetiva revisão em função das reais necessidades e melhoria contínua dos processos.

2.3.2 O novo quadro do RGPD e o seu impacto nas Organizações

Pode dizer-se, que o novo quadro do RGPD resultou da necessidade de uniformização das leis de proteção de dados, existentes nos diferentes estados membros da União Europeia, que visa simultaneamente uma maior exigência e maior responsabilização das Entidades públicas ou privadas, que tratam dados pessoais. Mas porquê agora?

Este novo quadro regulamentar e legal de proteção de dados, pretende salvaguardar os direitos e garantias dos titulares dos dados, num contexto atual, altamente tecnológico e de modelos de negócios, maioritariamente assentes em informação, estabelecendo regras de atuação, no sentido de proteger a qualidade, legitimidade e segurança dos dados, face às crescentes ameaças à privacidade, resultantes deste mundo digital, mas sobretudo pelo reconhecimento desta natureza de dados, como um ativo da máxima relevância para as Organizações.

A tomada de consciência de que a informação obtida através do tratamento dos dados pessoais é um bem, com um forte poder e consequências a nível económico e reputacional, e que a privacidade, numa sociedade digital, facilmente se encontra ameaçada se não forem avaliados os riscos e tomadas medidas para a sua mitigação, assim como a necessária validação da efetividade dos controlos existentes, veio trazer aos auditores internos uma nova área de atuação, com novos desafios e novas oportunidades de proteger e criar valor para as Organizações, sempre numa lógica de desenvolvimento e de melhoria contínua.

Nesse sentido, há que perceber o impacto do novo enquadramento do RGPD nas Organizações, designadamente ao nível da dinâmica de relacionamento com os clientes, colaboradores e na relação com outros parceiros (subcontratados), sendo essencial consciencializar a gestão de topo, sobre a sua transversalidade, assim como da

necessidade de adotar novas práticas e métricas de *compliance,* conforme se demonstra na figura seguinte:

Figura 2.8 - RGPD Impacto na Dinâmica Organizacional

Fonte: IPAI - Marques, B. M & Mendes, F.F (2020) Auditoria RGPD – Gestão da Privacidade Visão e o Papel do Auditor, Lisboa.

Será necessário elaborar um plano de comunicação interno e externo, face à abrangência desta regulamentação/legislação. Sendo que o plano interno deverá focar-se no esclarecimento e sensibilização dos colaboradores para os procedimentos a adotar para o cumprimento do RGPD. Enquanto que o plano de comunicação externa deverá ter como principal objetivo, gerar confiança nos clientes quanto à utilização adequada dos seus dados.

É essencial avaliar a necessidade de designar um Encarregado da Proteção de Dados(EPD), sendo que não é obrigatório para todas as empresas. Nessa medida, é importante confirmar se a Organização se enquadra nessa obrigatoriedade, de acordo com o previsto no Artº 37º do RGPD e Artigos 12º e 13º da Lei 58/2019 . Nos casos em que seja obrigatória a nomeação de um EPD/DPO (*Data Protection Officer*), será necessário conhecer bem as atribuições inerentes à função, por forma a selecionar o perfil mais adequado.

De igual forma, será essencial proceder ao levantamento das necessidades de adaptação dos processos aos requisitos do RGPD e idealmente promover a realização de Auditoria Interna no sentido de avaliar o impacto operacional do RGPD em cada área da Organização.

Outra necessidade, será a de estruturar um plano de implementação das ações de melhoria e a respetiva operacionalização nas diferentes áreas da Organização, de modo a acautelar a conformidade com os requisitos do regulamento.

Outro aspeto essencial a garantir será a formação sobre a segurança e privacidade de dados pessoais a todos os colaboradores que têm contacto com esta natureza de dados.

Será, igualmente necessária a atualização das políticas de segurança e privacidade e de utilização de cookies, assim como a revisão de procedimentos, de contratos e outros documentos por forma a cumprir aos requisitos do RGPD.

A adaptação do processo de recolha e tratamento de dados com a implementação dos conceitos de *"privacy by design"* e *"privacy by default"* também é algo a acautelar. Conceitos que remetem para a obrigatoriedade de obtenção de consentimento prévio para a utilização dos dados.

A inventariação e catalogação de dados pessoais recolhidos e guardados pela Organização, de modo a identificar os dados pessoais existentes, o tipo de dados, a finalidade do tratamento, o local onde se encontram guardados, o período de utilização, pessoa/entidade que os facultou, quem tem acesso aos dados.

Será igualmente necessário listar procedimentos de recolha e tratamento de dados pessoais, identificando as formas de recolha e de tratamento dos dados, assim como o fundamento legal, base de licitude para o seu tratamento. Documentando esta informação, de modo a que esta seja, facilmente evidenciável.

Implementar ou rever medidas técnicas e organizativas de proteção e privacidade dos dados, como seja a cifragem, pseudonimização ou anonimização dos dados, ou simplesmente a adoção da política de secretária limpa.

Garantir a existência de processos que permitam detetar incidentes de violação de dados pessoais, assim como a respetiva comunicação à entidade reguladora e aos titulares dos dados (se aplicável).

Preparar o *workflow* de resposta aos direitos dos titulares, nomeadamente o direito à informação e o direito ao esquecimento, entre outros.

Validar se as aplicações informáticas existentes na Organização para o processamento de dados se encontram em cumprimento com os requisitos do RGPD e, caso não estejam, providenciar a respetiva atualização em conformidade.

Simultaneamente, será essencial acautelar a conformidade por parte das entidades subcontratadas para a realização de atividades em que interajam com dados pessoais, sendo crucial assegurar que os termos e condições dessa relação, incluindo as indicações sobre a forma de tratamento de dados, estejam, expressamente previstas num contrato escrito.

Situação similar, coloca-se aos fornecedores, que processam e/ou armazenam dados pessoais, os quais devem garantir o cumprimento dos requisitos do RGPD.

As metodologias de trabalho devem incluir a avaliação do impacto de proteção de dados (DPIA – *Data Protection Impact Assessment*) nas situações em que as mesmas são obrigatórias e sempre que se considerem úteis.

Será ainda necessário, assegurar a monitorização contínua da aplicação do planeado, assim como implementar medidas de controlo nas várias estruturas organizacionais. monitorização essa que deverá ser assegurada pelo EPD/DPO.

À Auditoria Interna caberá o papel de validar de forma independente, objetiva e rigorosa se os controlos e medidas, são suficientes e efetivos para garantir com razoável grau de confiança, a conformidade com o regulamento e a mitigação dos riscos associados a este processo.

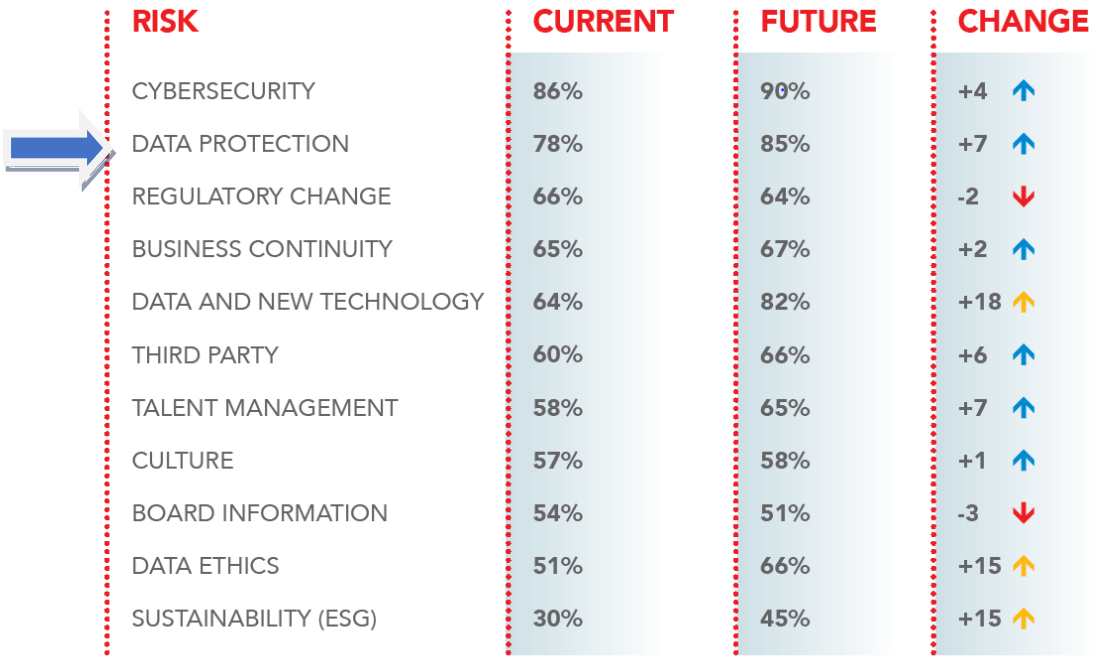
Numa fase, tendencialmente de maior maturidade do processo, as Organizações podem ainda solicitar a certificação da sua conformidade, à comissão nacional de proteção de dados (CNPD) ou a outro organismo habilitado para tal. A obtenção desta certificação pela CNPD, constitui um fator distintivo, que contribuirá para incrementar a confiança da administração, a nível interno, assim como dos clientes e do mercado, a nível externo.

2.3.3 RGPD - O papel da Auditoria Interna vs o papel do Encarregado pela Proteção de Dados

Num dos mais recentes relatórios emitidos pelo IIA - *OnRisk 2020*, é salientada a relevância do papel da Auditoria Interna, que com a sua independência e objetividade se vem reafirmar como um dos três pilares da gestão de riscos, juntamente com o conselho e a gestão executiva.

Neste mesmo documento foram identificados como principais riscos, posicionados num *ranking* de acordo com a sua relevância atual e futura, os seguintes 11 riscos:

Figura 2.9 - *Risk Relevance for 11 Risks Ranking*



Fonte: http://contentz.mkt5790.com/lp/2842/275148/OnRisk-2020-Report_0.pdf

Neste *ranking*, pode-se observar, que a Proteção de Dados é tanto, presentemente como no futuro, o risco que ocupa a segunda posição, apenas ultrapassado pelo risco relativo à cibersegurança, o que vem reforçar a convicção de que as preocupações com o RGPD estão na ordem do dia e são de suma importância para as Organizações.

Pode-se dizer, que uma auditoria ao RGPD, tal como noutras matérias consiste num exame rigoroso, sistemático, independente e objetivo, baseado em factos e evidências, das politicas, procedimentos e controlos implementados pelas organizações, para mitigar os riscos identificados, numa lógica desenvolvimento e de melhoria contínua, tendo por objetivo, avaliar se os resultados obtidos são os planeados (eficácia) e se os mesmos foram implementados em conformidade com os requisitos do RGPD e da forma mais eficiente.

O que implica, entre outros aspetos já referidos, que as Organizações estejam, devidamente esclarecidas e cientes do papel que cabe à Auditoria Interna e o papel que compete ao Encarregado da Proteção de Dados (EPD).

No cerne desta questão, está o legislado como sendo funções do EPD, designadamente na Lei 58/2019, que no seu Art.º 11º, alínea a) define como «Funções do Encarregado da Proteção de Dados», para além das previstas nos Art.ºs 37 e 39.º do RGPD,

> [a]ssegurar a realização de auditorias, quer periódicas, quer não programadas.

Ora, na visão do auditor interno, pese embora, a Lei 58/2019 no seu Art.º 11, alínea a) preveja como uma das funções do EPD «assegurar a realização de auditorias», tal não parece significar que a execução das mesmas, caiba ao EPD ou que esteja ao seu nível de atuação fazê-lo. Tendo como referência o modelo das três linhas de defesa, pode-se constatar que as funções do EPD/DPO, se enquadram no âmbito da segunda linha e não da terceira linha, esta última, correspondendo à Auditoria Interna.

Ainda assim, não parece ser claro para todas as organizações a necessária, existência desta distinção e segregação de funções, entre quem deve assegurar que sejam implementadas medidas, que garantam a conformidade com o regulamento, e quem as deve auditar. Pois, ainda que o EPD/DPO, tivesse competências de auditor, não seria possível garantir a isenção, rigor, independência e objetividade, necessárias à realização de um exercício de auditoria, se quem audita é quem tem, simultaneamente a responsabilidade por garantir a conformidade com o regulamento.

Cabe à Auditoria Interna enquanto terceira linha de defesa, também ao nível do RGPD, realizar as auditorias, de modo a garantir uma validação independente e objetiva, suportada em evidências, da conformidade face aos requisitos do regulamento e legislação, mas, igualmente apurar, se os controlos existentes são efetivos e suficientes

para a mitigação dos riscos. Acresce que, cabe à Auditoria Interna a identificação de oportunidades de melhoria, funcionando como uma alavanca de otimização dos processos e assim contribuir para potenciar a confiança das Organizações e do mercado, afirmando-se como uma mais valia.

A Auditoria Interna e o EPD assumem assim, papeis distintos, mas complementares no que respeita ao sistema de gestão de *compliance* do RGPD, estando a função do EPD ao nível da segunda linha de defesa e cabendo ao Auditoria interna um papel ao nível da terceira linha, que vai muito além da conformidade com o Regulamento.

A Auditoria Interna terá ao nível do RGPD, um papel determinante, simultaneamente de parceiro estratégico, que permitirá não só, assegurar o cumprimento dos requisitos do RGPD, bem como, de evidenciar esse cumprimento, identificando ainda áreas de melhoria ao nível dos controlos, sua eficiência/eficácia, assim como potenciais novos riscos, permitindo à gestão tomar decisões estratégicas de forma mais assertiva.

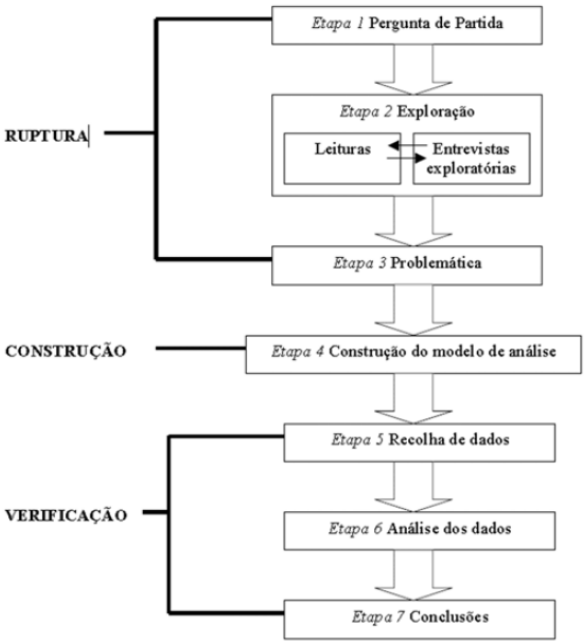
3 Estudo Empírico

3.1 Justificação da opção metodológica do questionário

O método do questionário é um dos métodos mais reconhecido e utilizado na investigação académica, consiste, na aplicação de várias questões a um conjunto de inquiridos que, habitualmente, representa uma população, tendo como finalidade abordar um assunto/temática de interesse para os investigadores (Quivy & Campenhoudt, 1992). Este método de investigação, de acordo com Almeida (1994), apresenta inúmeras vantagens, como por exemplo, a possibilidade de recolher e obter informações relevantes por parte de um elevado número de indivíduos e possibilita a generalização dos resultados da amostra para a população.

Assim, para o desenvolvimento deste questionário foram consideradas as sete etapas preconizadas por Quivy& Campenhoudt (1998) do processo de investigação, veja-se na figura seguinte (Figura 3.1):

FIGURA 3.1 - ETAPAS DO PROCESSO DE INVESTIGAÇÃO



Fonte: (Quivy & Campenhoudt, 1998)

A pergunta de partida é: Qual o papel da Auditoria Interna no RGPD enquanto terceira linha de defesa, por contraponto com as funções atribuídas ao Responsável pela Proteção de Dados, que de acordo com a nova Lei, incluem «assegurar a realização de auditorias […]»?

Tendo por base esta questão, formularam-se as seguintes hipóteses:

Hipótese 1 - Existe relação entre o nível de clareza com que é entendido o papel da Auditoria Interna no RGPD e a observância na Organização do Modelo das Três Linhas de Defesa.

Hipótese 2 - O nível de preparação da Auditoria Interna para corresponder aos novos desafios trazidos pelo RGPD, relaciona-se com a proteção de dados ser uma prioridade na gestão da informação nas Organizações.

Hipótese 3 - Existe relação entre o grau de maturidade (anos) na função de auditor e o entendimento das funções atribuídas no âmbito do RGPD ao EPD/DPO quanto às auditorias a assegurar neste âmbito.

Hipótese 4 – O grau de preparação tecnológica das Organizações para o cumprimento do RGPD está relacionado com existência de um EPD/DPO ou entidade externa responsável pela proteção de dados na Organização.

Hipótese 5 - A existência nas Organizações de um Encarregado da proteção de dados ou entidade externa com esta responsabilidade relaciona-se com os procedimentos vigentes na Organização darem resposta aos requisitos do RGPD.

Hipótese 6 –Existe relação entre o estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD e a preparação da Auditoria Interna para responder aos novos desafios que este novo enquadramento traz.

As quais se pretendem validar através dos resultados obtidos e da interpretação dos mesmos.

3.2 Apresentação dos resultados

O questionário foi elaborado com recurso à plataforma digital *Google forms*, de modo a permitir a resposta direta dos respondentes, de forma anónima e confidencial, tendo o mesmo ficado disponível para preenchimento na plataforma desde 30MAR até 21SET2020.

Este questionário tem como população alvo os auditores internos a exercer funções em Portugal, dada a especificidade do tema e a abordagem, tendo sido tomada como referência o universo total de auditores inscritos no IPAI, 1268, à data de abril de 2020.

O questionário é composto por vinte sete questões fechadas, com múltiplas opções, mas de resposta única e obrigatória, com exceção da pergunta 26, cuja resposta está condicionada pela anteriormente dada à questão 25.

As questões encontram-se assim, repartidas em quatro partes:

Parte I - Caracterização do respondente (questões da 1 à 5) onde se pretendeu caraterizar os respondentes, designadamente, quanto à faixa etária, maturidade na função, área de formação e função que desempenha;

Parte II - Caracterização da Organização e da Função Auditoria Interna (questões da 6 à 12), em que se pretende caraterizar a Organização, pública ou privada, identificar o setor de atividade, o número de trabalhadores, o número de auditores internos, o posicionamento da Auditoria Interna na estrutura hierárquica da empresa, assim como apurar se a mesma segue os *standards* internacionais do IIA e o Modelo das Três Linhas de Defesa.

Parte III – O Regulamento Geral de Proteção de Dados (RGPD) na Organização (questões da 13 à 19), em que se pretende aferir a perceção sobre o grau de conhecimento que a organização tem dos termos e princípios orientadores do RGPD e suas implicações, se foram realizadas ações de formação/sensibilização neste âmbito, compreender ainda, em que medida o RGPD é uma prioridade para a gestão, assim como perceber o grau de maturidade compreensão dos seus termos, da natureza e do impacto do mesmo na Organização, designadamente, se os procedimentos em vigor na

empresa respondem aos requisitos do RGPD e o seu grau de preparação ao nível tecnológico para fazer face às exigências deste regulamento e ainda se existe na Organização um EPD/DPO nomeado.

Parte IV – As Auditorias ao Regulamento Geral de Proteção de Dados (RGPD) (questões da 20 à 27), pretende-se nesta última parte, apurar a perceção sobre o papel da auditoria por contraponto com as responsabilidades atribuídas ao EPD/DPO, nomeadamente sobre o grau de preparação da Auditoria Interna para fazer face aos novos desafios do RGPD, aferir sobre a relevância (ou não) do papel da auditoria na realização das auditorias ao RGPD e enquanto mais valia concretizável em ações de melhoria, ganhos efetivos de eficiência e de confiança para organização, quem realiza o controlo da conformidade com o regulado/legislado no âmbito do RGPD (ao nível da *compliance*) e quem realiza as auditorias ao RGPD.

A divulgação destes questionários foi efetuada maioritariamente por *email* e através do *site* e redes sociais do IPAI, no sentido de obter o maior número possível de respostas, e assim robustecer os resultados deste trabalho.

Pese embora os vários contactos no sentido de potenciar as respostas, estas ficaram muito aquém do expectável, dado que se esperava uma boa taxa de resposta pela novidade do tema e o interesse que suscita. Assim tomando como referência o universo de 1268 auditores internos inscritos no IPAI, e tendo-se obtido 68 respostas, todas válidas, a taxa de resposta foi de 5,36 em termos percentuais.

Dado que o questionário foi lançado a 30 de Março, esta taxa de resposta pouco expressiva, poderá, de algum modo, ser justificada pela pandemia provocada pelo coronavirus, Covid-19, que nos assolou inesperadamente, por todos os constrangimentos e preocupações adicionais com as quais pessoas e Organizações se depararam, assim como a necessedidade de se adaptarem a uma nova realidade com impacto sem precedentes e à escala global, com repercussões ainda latentes.

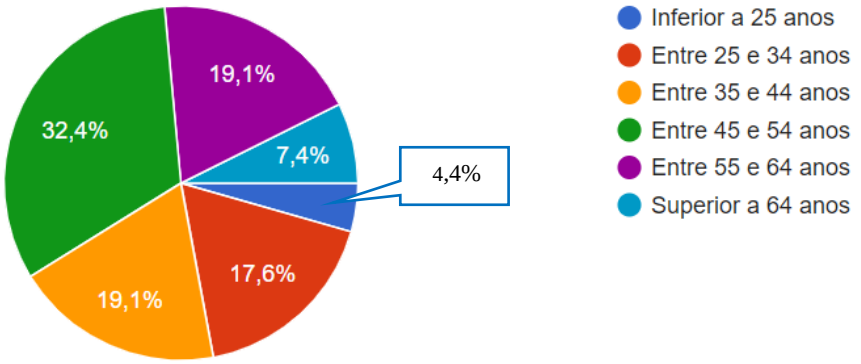
3.3 Estatística descritiva e interpretação dos resultados

Neste capítulo pretende-se demonstrar e interpretar os dados obtidos numa amostra de 68 respostas, taxa de resposta de 5,36%, que apesar de não ser a mais representativa, julgamos ainda assim, permitir responder à pergunta de partida e às hipóteses formuladas.

Os dados a seguir apresentados sob a forma de gráficos, foram construídos automáticamente e extraídos da plataforma *Google forms*, plataforma digital, onde os participantes responderam diretamente às questões. A versão integral destes dados está apensa a este trabalho, no Apendice A.

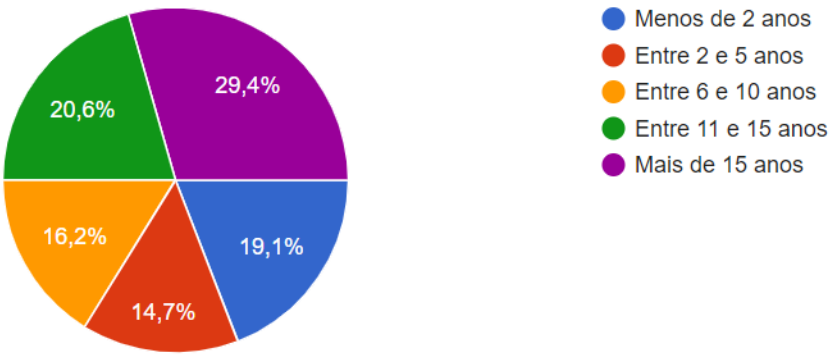
Parte I – Caraterização do Respondente

Gráfico 3.1 - Faixa Etária



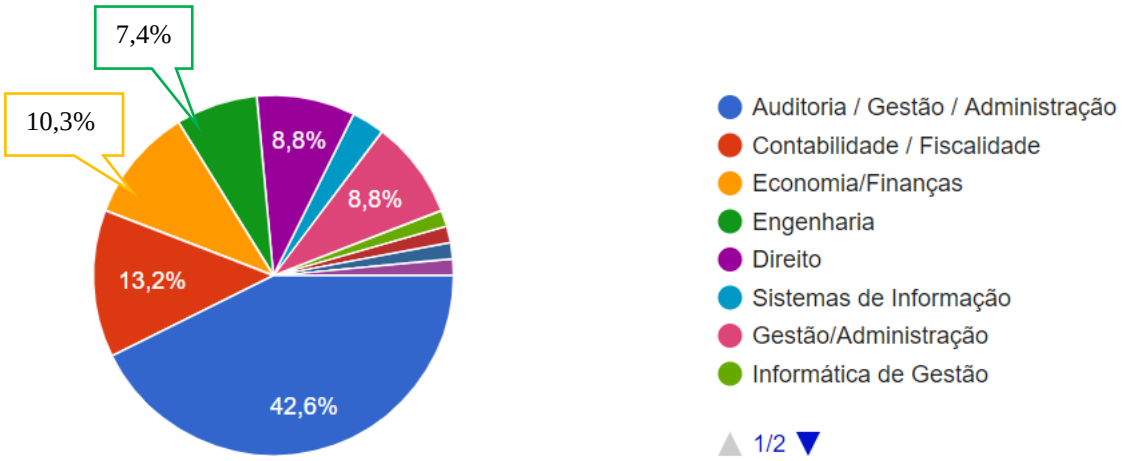
Relativamente à faixa etária, pode-se verificar pela análise ao **Gráfico 3.1**, que **32,4%,** (22 respondentes) se enquadram na faixa etária **dos 45 aos 54 anos**, logo seguida das faixas etárias entre os 55 e 64 anos e 35 e 44 anos, ambas com a mesma percentagem 19,1% (13 respondentes). Em terceiro lugar, não muito afastada está a faixa etária dos 25 aos 34 anos, com 17,6% (12 respondentes). De referir ainda que apenas 7,4% (5 respomdentes) se enquadram na faixa superior a 64 anos e 4,4% (3 respondentes) têm idade inferior a 25 anos.

Gráfico 3.2 – Maturidade na Função (em anos)



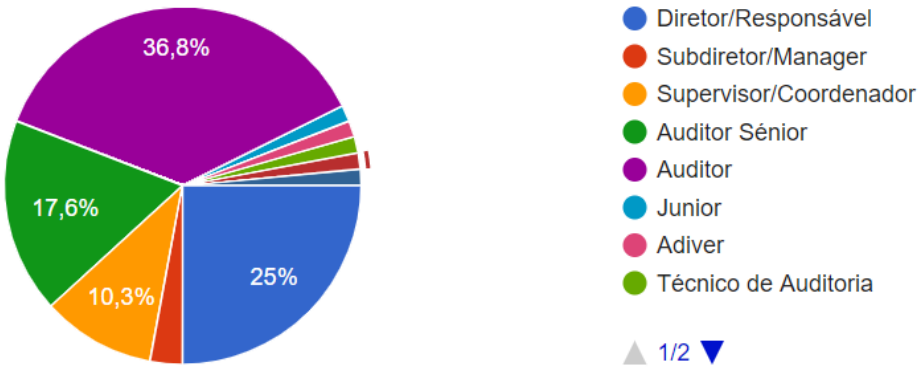
Da análise ao **Gráfico 3.2**, pode-se constatar que em termos de maturidade na função **29,4%** (20 respondentes) **tem mais de 15 anos** na função. A seguir com 20,6% (14 respondentes) tem uma maturidade entre os 11 e os 15 anos, o que nos poderá levar a pensar que 50% dos respondentes estão a um nível senior das suas funções. Por outro lado, com 19,1% (13 respondentes) estão os que exercem funções nesta área há menos de 2 anos, e de seguida 16,2% (11) e 14, 7% (10), respetivamente, exercem funções de Auditoria Interna entre os 6 e os 10 anos e os 2 e 5 anos. O que pode indicar de certa forma o rejuvenescimento da função, apresentando-se coerente com o refletido no Gráfico 1.

Gráfico 3.3 - Área de Formação



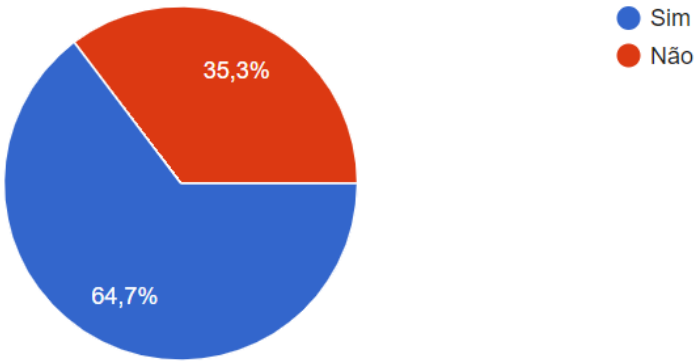
Por observação do **Gráfico 3.3**, constata-se que a principal área de formação correspondente a **42,6%** (29 respondentes) **é a de Auditoria/Gestão/Administração**, seguida de 13,2% (9 respondentes) na área de Contabilidade/Fiscalidade e em seguida empatadas as áreas de Gestão/Administração e de Direito, ambas com uma representatividade percentual de 8,8% (o que corresponde a 6 respondentes em cada área). As áreas de Economia e finanças assim como a de Engenharia apresentam uma representatividade percentual de 10,3% e 7,4%, respetivamente (7 e 5 respondentes), havendo ainda outras áreas de formação abrangidas, apesar de com menor expressão, o que evidencia de certa forma a diversidade de conhecimentos enquadráveis nas funções de auditor interno.

Gráfico 3.4 - Função na Estrutura da Auditoria Interna



O **Gráfico 3.4**, por sua vez identifica a função dos respondentes ao nivel da estrutura da Organização, sendo que conforme se pode verificar, **36,8%** (em número, 25) tem a função de **Auditor**, 25% (17) a de Diretor/Responsável, 17,6% (12) a função de Auditor senior e 10,3% (7) a função de Supervisor/Coordenador. As demais funções têm uma menor representatividade (abaixo dos 3%).

Gráfico 3.5 - É membro do Instituto Português de Auditoria Interna (IPAI)?



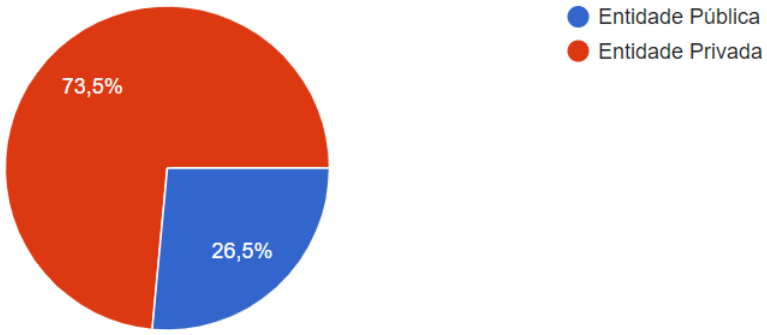
Sendo o IPAI o Organismo em Portugal, que promove a classe dos profissionais de Auditoria Interna um dos seus principais objetivos contribuir para a formação em conhecimentos, metodologias e práticas de Auditoria Interna, no sentido de fomentar a constante evolução da função do Auditor interno, entendeu-se pertinente aferir através deste questionário a representatividade dos seus membros na amostra. Tanto mais que

foi tomado como referência e universo para este trabalho o número total de auditores inscritos no IPAI.

Assim da análise ao **Gráfico 3.5**, pode-se constatar que pese embora a percentagem de membros do IPAI seja de 64,7% (44 em número de respondentes) a percentagem de não membros deste Organismo 35,3% (24 em número) ainda tem alguma expressão. Resultado que nos pode levar a questionar o universo tido em consideração para efeito deste estudo, mas que não obstante parecia constituir um referencial adequado e de fonte fidedigna.

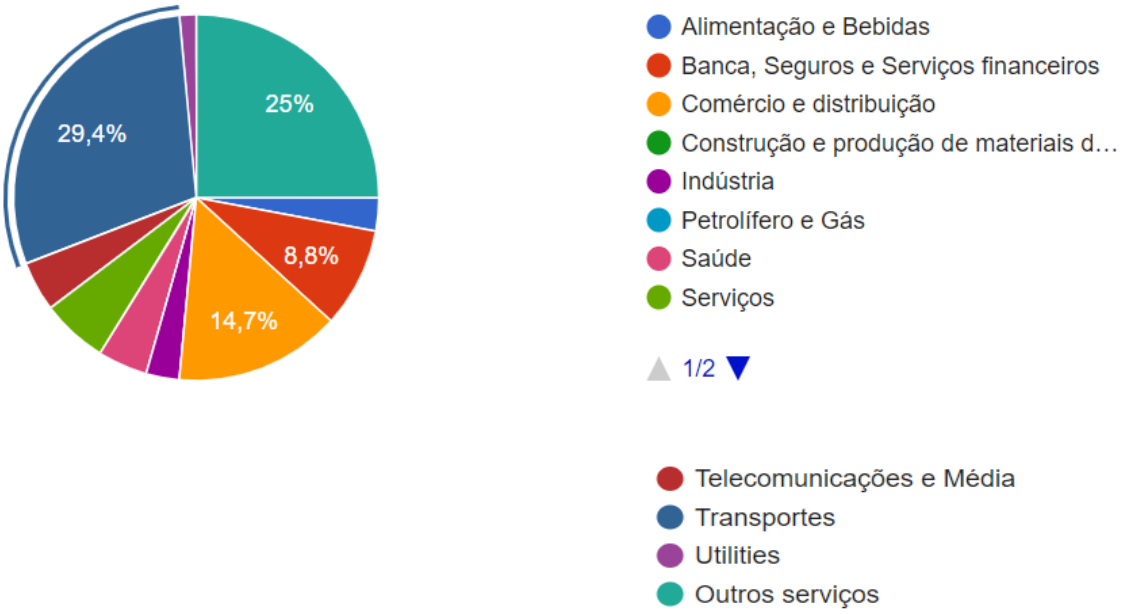
Parte II - Caracterização da Organização e da Função Auditoria Interna

Gráfico 3.6 - Natureza da Organização



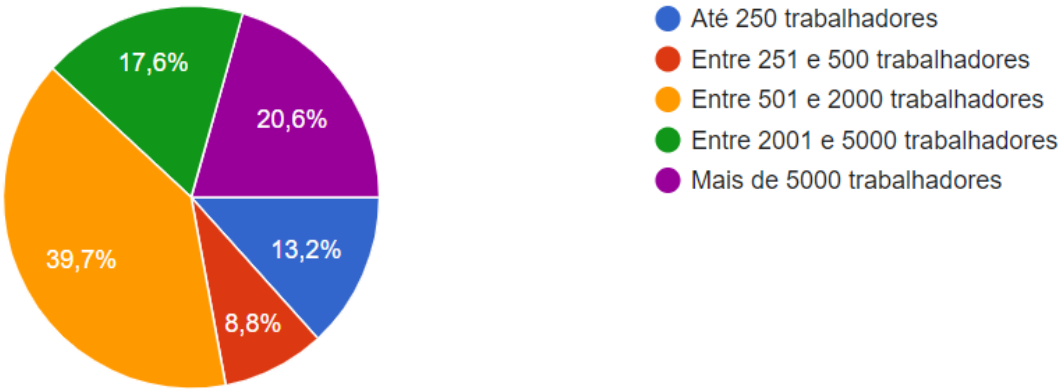
No **Gráfico 3.6**, pode-se verificar que **73,5%** dos respondentes exercem funções em numa Entidade privada e 26,5% numa Entidade Pública.

Gráfico 3.7 - Setor de Atividade da Organização



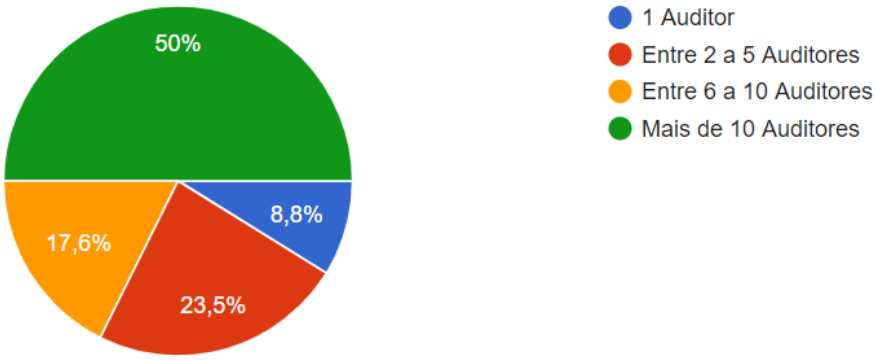
Do que se pode observar no **Gráfico 3.7**, o setor de atividade mais representativo nesta amostra de respondentes com **29,4%** (20 em número) é o setor dos **Transportes**, seguido pelo setor de Outros Serviços com 25% (17). O terceiro lugar cabe ao setor do Comércio e Distribuição, representando 14,7% (10) e a Banca e Seguros Financeiros que representa 8,8% (6 respondentes). Estão ainda representados os setores de atividade dos Serviços, Telecomunicações e Média, Saúde, Alimentação e Bebidas, Indústria e *Utilities*, todos estes com uma representatividade menos expressiva (inferior a 6%).

Gráfico 3.8 - Número de trabalhadores da organização



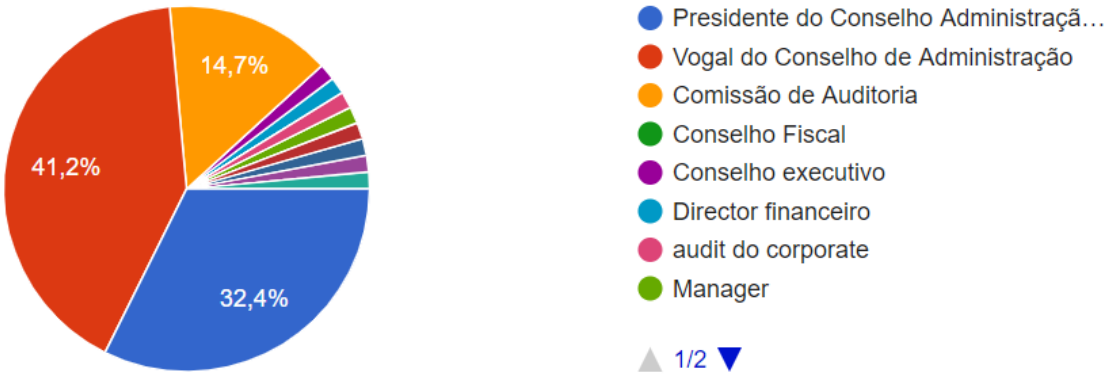
Da análise ao **Gráfico 3.8**, verifica-se que **39,7%** (27) dos respondentes exercem funções em Organizações cujos trabalhadores são em número entre os **500 e 2000**, seguido de 20% (14) que trabalham em Organizações com mais de 5000 trabalhadores. Os terceiros mais representados, 17,6% (12) trabalham em Organizações cujo, o número de trabalhadores se situa entre as 2001 e os 5000. Por sua vez, 13,2% (9) trabalham em empresas com um número que vai até 250 trabalhadores e 8,8% (6) exercem a sua atividade profissional em Organizações cujo, o número de trabalhadores se enquadra no intervalo entre os 251 e os 500 trabalhadores.

Gráfico 3.9 - Número de Auditores Internos na sua Organização



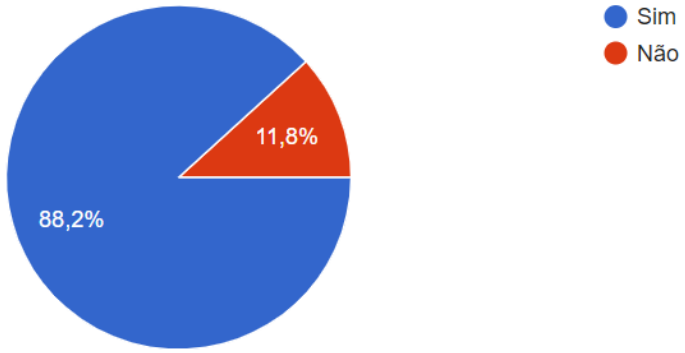
No **Gráfico 3.9** é possivel aferir o número de auditores internos existentes nas Organizações dos respondentes, verificando-se que **50%** estão integrados em equipas com mais de 10 auditores, e que outros 23,5% integram equipas entre 2 a 5 auditores. Enquanto 17,6% estão inntegrados em equipas cujo numero de auditores varia entre os 6 e os 10 auditores. E apenas 8% é auditor único na sua Organização. Resultados que estão alinhados com a informação obtida em resposta à questão anterior, em que 77,9% exerce funções em Organizações de grande dimensão (com mais de 500 trabalhadores, 20% dos quais em organizações com mais de 5000).

Gráfico 3.10 - A quem reporta, hierarquicamente a Auditoria Interna, na sua organização?



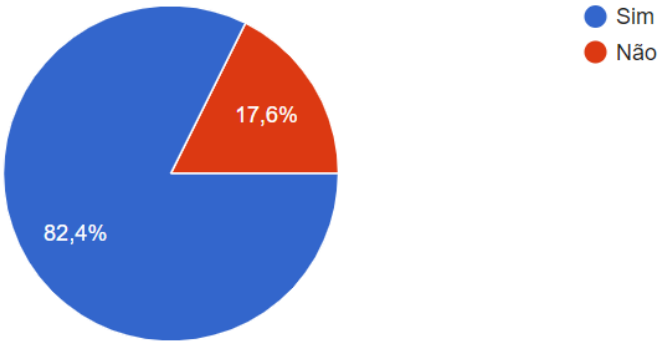
No **Gráfico 3.10** pode-se constatar que **41,2%** (28) dos respondentes referem que a função de auditoria nas suas Organizações, reporta hierarquicamente a um **Vogal do Conselho de Administração**, 32,4% ao Presidente do Conselho de Administração e 14,7% à Comissão de Auditoria.

Gráfico 3.11 – A Auditoria Internana sua Organização, rege-se pelos Standards Internacionais do *Institute of Internal Auditors* (IIA)?



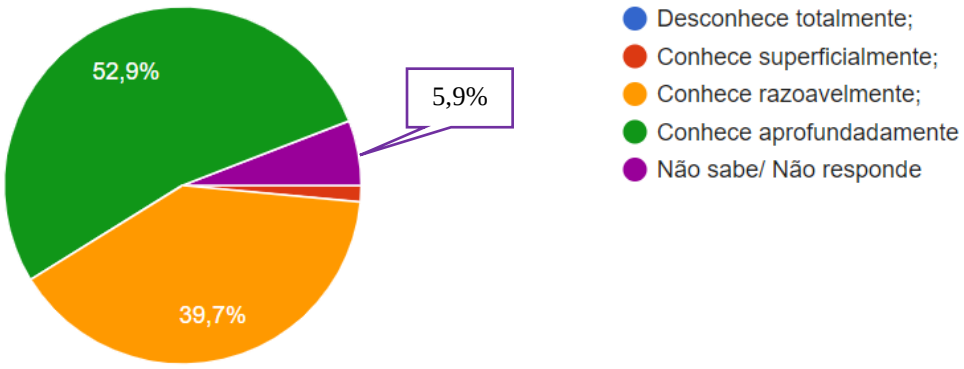
No **Gráfico 3.11** verificamos que 88,2% (60 respondentes) referiram que a Auditoria Interna é regida nas suas Organizações, pelos *standards* internacionais do IIA. E Apenas 11,8% (8) responderam que não seguem estes *Standards*.

Gráfico 3.12 – A sua Organização segue o Modelo das três Linhas de Defesa?



No **Gráfico 3.12** verifica-se que 82,4% (56) dos respondentes referiram que as suas Organizações seguem o Modelo das Três Linhas de Defesa, enquanto que os restantes 17,6% (12) referiu não seguir este Modelo.

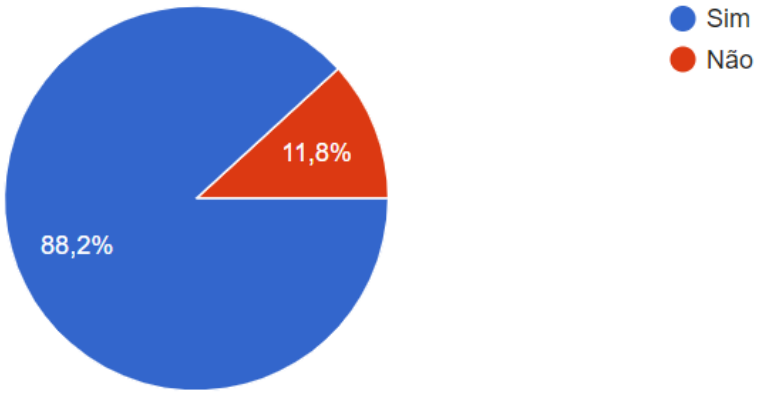
Gráfico 3.13 – Em que medida considera que a sua Organização, conhece os termos e os princípios previstos no Regulamento Geral de Proteção de Dados (RGPD) e as suas implicações?



No **Gráfico 3.13**, pretende-se demonstrar em que medida os respondentes consideram que as suas Organizações conhecem os termos e os princípios previstos no Regulamento e as suas implicações.

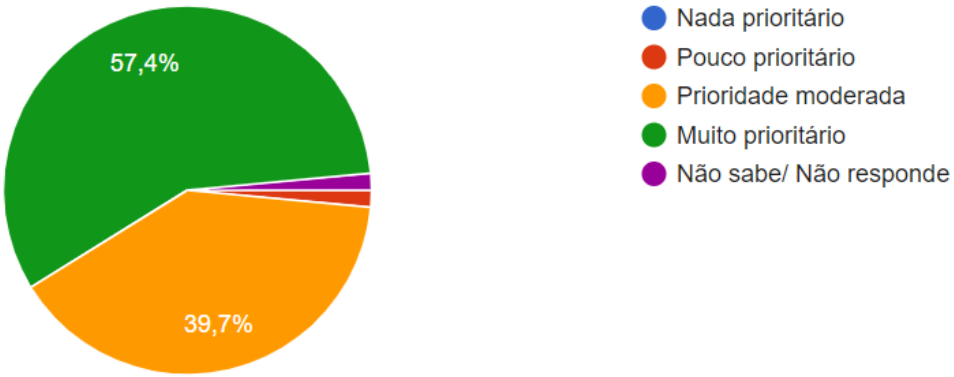
Assim pode-se verificar da análise do mesmo que **52,9%** (36) dos respondentes considera que as suas Organizações **conhecem aprofundadamente** os termos e principios do RGPD, assim como as suas implicações, enquanto que 39,7% (27) considera que as suas Organizações apenas conhecem razoavelmente o RGPD, os seus termos, principios e implicações. 5,9% (4) não sabem/não respondem.

Gráfico 3.14 – Foram efetuadas na sua Organização, ações de formação/ sensibilização sobre os princípios norteadores do Regime Geral de Proteção de Dados (RGPD)?



O **Gráfico 3.14** demonstra que 88,2% (60 respondentes) consideram que foram efetuadas na sua Organização, ações de formação/sensibilização sobre os principios norteadores do RGPD, enquanto que 11,8% (8) referem que não.

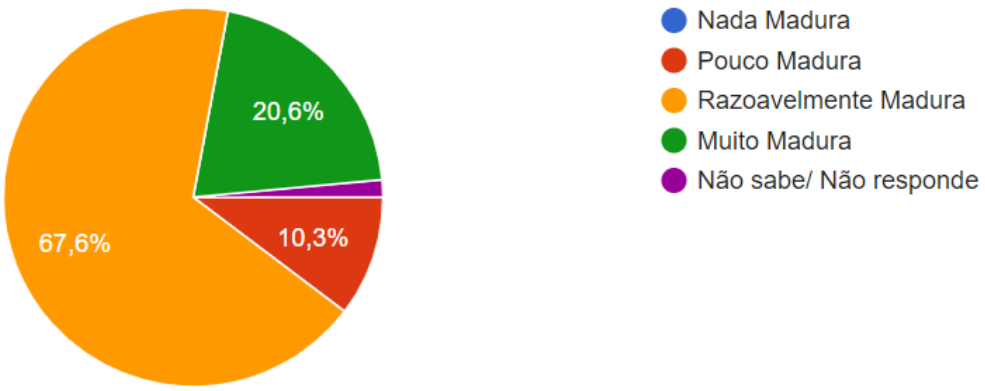
Gráfico 3.15 – Considera que a proteção de dados é uma prioridade na gestão de informação da sua Organização?



Da análise ao **Gráfico 3.15** constata-se que 57,4% (39) dos respondentes considera a Proteção de Dados como algo muito prioritário na gestão da informação das suas

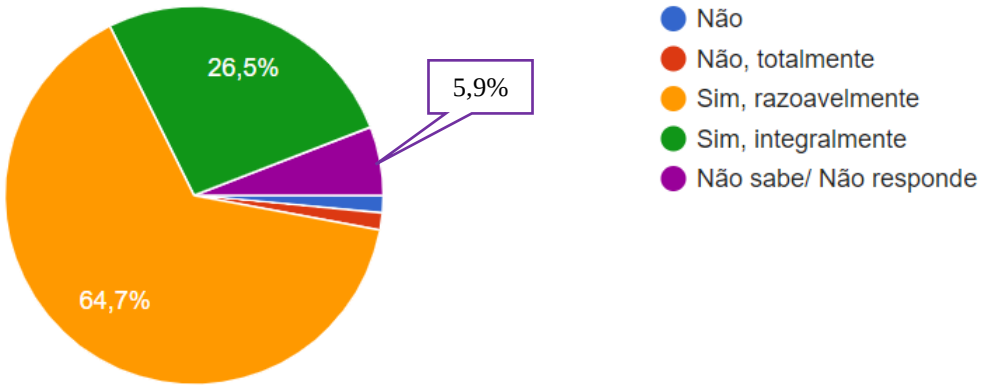
Organizações e 39,7% (27) consideraram-na como de prioridade moderada. Apenas 1 respondente considerou o tema pouco prioritario e outro que não respondeu por desconhecimento.

Gráfico 3.16 - Em que estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD (incluindo a Lei 58/2019), considera que a sua Organização se encontra?



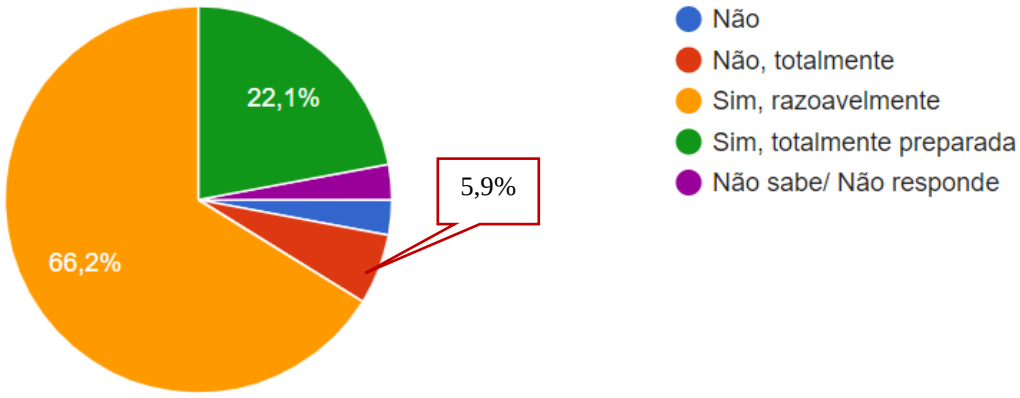
Da análise do **Gráfico 3.16** verifica-se que 67,6% (46) dos respondentes consideram que as suas Organizações se encontram num estágio de razoavel maturidade no que respeita à compreensão da natureza e do impacto do RGPD, incluindo a Lei 58/2019) e que 20% dos respondentes (14) considera a sua organização num estágio muito maduro enquanto 10,3% (7 respondentes) considera pouco maduro o estágio em que as suas Organizações se encontram face ao RGPD compreensão da sua natureza e impacto.

Gráfico 3.17 – Considera que os atuais procedimentos vigentes na sua Organização, respondem aos requisitos do Regulamento Geral de Proteção de Dados (RGPD)?



No **Gráfico 3.17**, pode verificar-se que **64,7%** (44) dos respondentes consideram que os procedimentos atualmente vigemtes na sua Organização **respondem razoavelmente** aos requisitos do RGPD, enquanto 26,5% (18) consideram que respondem integralmente. 5,9% (4) não sabem/não respondem.

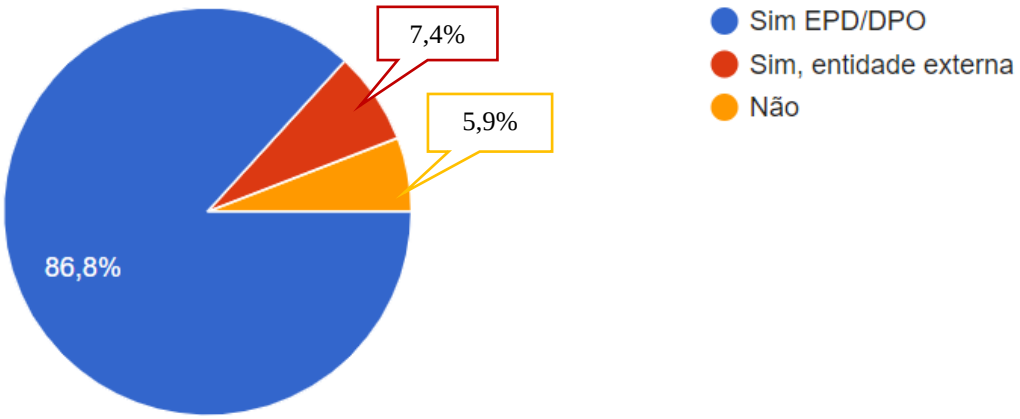
Gráfico 3.18 – Considera que a sua Organização se encontra tecnologicamente preparada para o cumprimento do Regulamento Geral de Proteção de Dados?



O **Gráfico 3.18** pretende demonstrar em que medida os inquiridos consideram que a sua Organização se encontra tecnológicamente preparada para o cumprimento do RGPD,

tendo **66,2%** (45) respondido que sim, razoavelmente e 22,1% (15) que sim, totalmente preparada. 5,9% (4) responderam que não, totalmente.

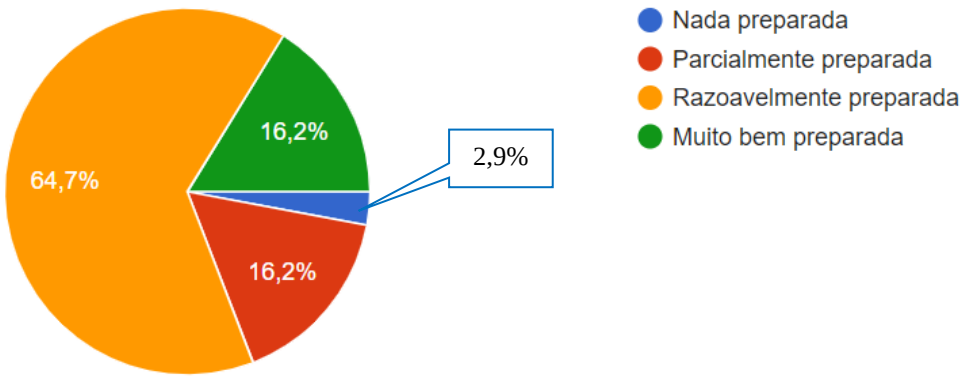
Gráfico 3.19 – Na sua Organização existe um Encarregado da Proteção de Dados/ *Data Protection Officer* ou entidade externa, responsável pela proteção de dados?



O **Gráfico 3.19** demonstra que 86,8% (56) dos respondentes tem nas suas Organizações como responsável pela proteção de dados um EPD/DPO nomeado, e apenas 7,4% (5) referiu recorrerem nas suas Organizações a uma entidade externa. Os restantes 5,9% (4) responderam não existir EPD/DPO nomeado ou entidade externa com responsabilidade ao nível da proteção de dados.

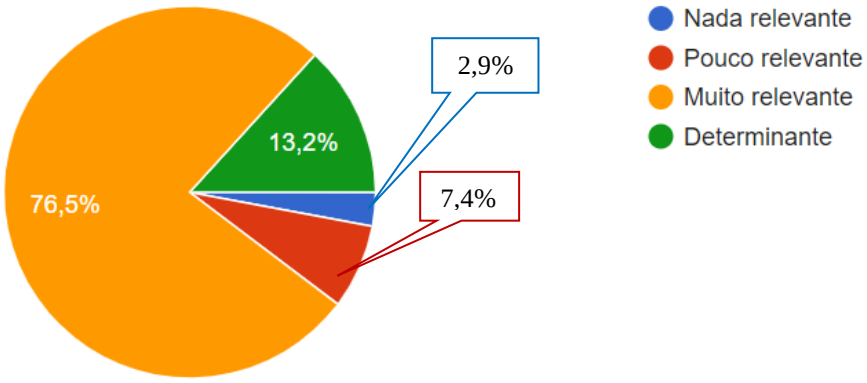
Parte IV – As Auditorias ao Regulamento Geral de Proteção de Dados (RGPD)

Gráfico 3.20 – Considera que na sua Organização, a Auditoria Interna está preparada para corresponder aos novos desafios trazidos pelo RGPD?



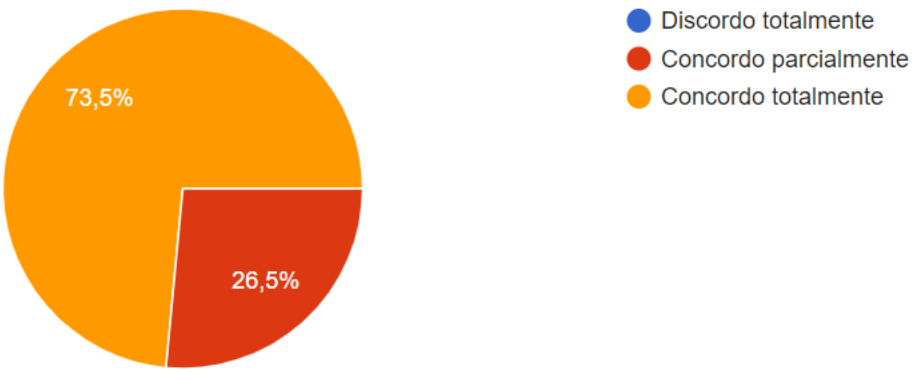
Da análise ao **Gráfico 3.20** constata-se que a maioria dos respondentes**, 64,7%** (44 em número) considera que a auditoria interna, na sua Organização, está **razoavelmente preparada** para corresponder aos novos desafios trazidos pelo RGPD. 16,2% (11) dos respondentes consideram a Auditoria Interna da sua Organização muito bem preparada, empatados com os que consideram que a Auditoria Interna está parcialmente preparada. 2,9% (2) consideram que a Auditoria Interna na sua Organização não está nada preparada para fazer face aos novos desafios trazidos pelo RGPD.

Gráfico 3.21 – Considera que na sua Organização, a Auditoria Interna enquanto 3.ª linha de defesa, assume um papel relevante/determinante para a criação de valor na operacionalização das auditorias ao RGPD?



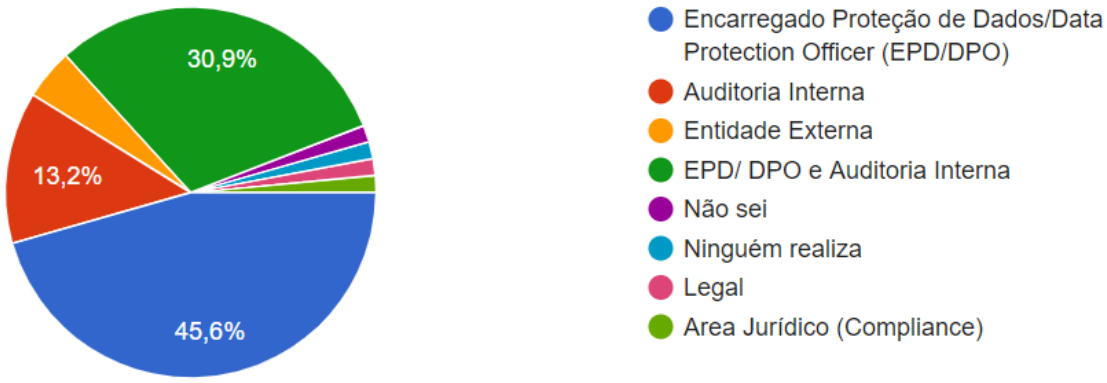
O **Gráfico 3.21** revela que **76,5%** (52) dos respondentes consideram muito relevante o papel da Auditoria Interna enquanto terceira linha de defesa, para a criação de valor na operacionalização das auditorias ao RGPD e 13,2% (9) consideram determinante. Apenas 7,4% (5) dos respondentes consideram pouco relevante e 2,9% (2) nada relevante.

Gráfico 3.22 – Concorda que as auditorias ao RGPD, quando realizadas pela Auditoria Interna enquanto 3.ª linha de defesa, constituem uma mais valia que se concretiza em ações de melhoria, ganhos efetivos de eficiência e de confiança na organização?



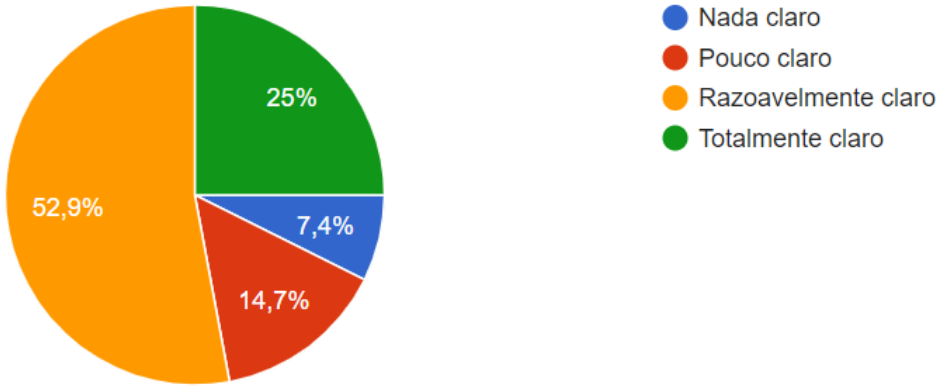
O **Gráfico 3.22** revela que **73.5%** (50) dos respondentes **concorda totalmente** que as auditorias ao RGPD, quando realizadas pela Auditoria Interna enquanto 3ª linha de defesa constituem uma mais valia que se concretiza em ações de melhoria, ganhos efetivos de eficiência e de confiança na Organização. Os restantes 26,5% (18) apenas concorda parcialmente. Não havendo nenhum respondente em desacordo.

Gráfico 3.23 – Na sua Organização quem realiza o controlo da conformidade com o regulado/legislado no âmbito do RGPD (*Compliance*)?



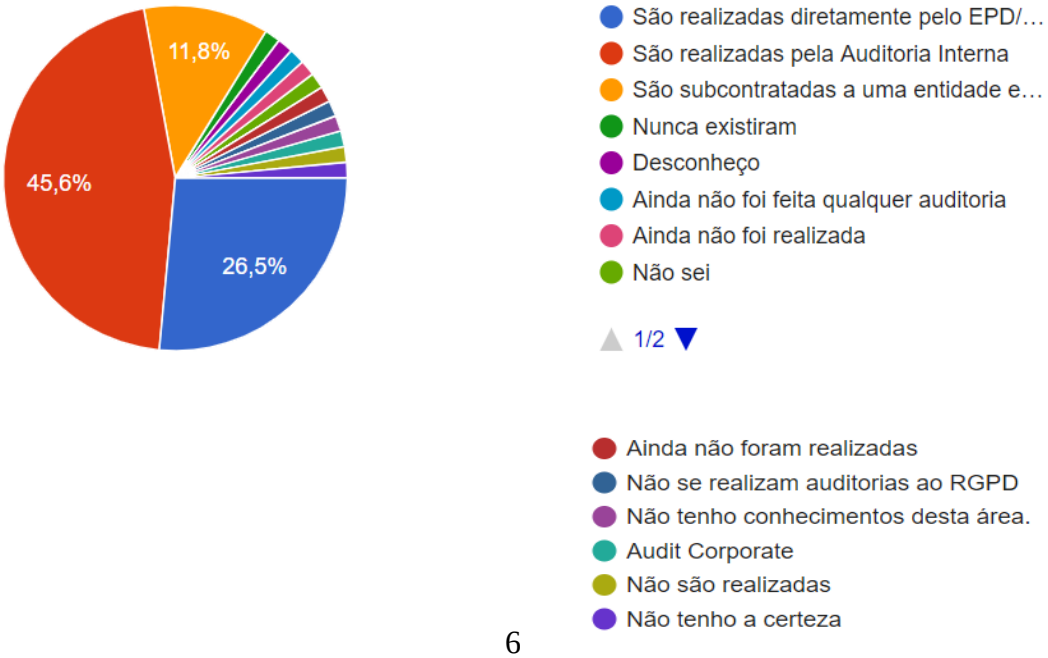
No **Gráfico 3.23** verifica-se que **45,6%** (31) dos respondentes referiram que quem realiza o controlo da conformidade com o regulado/legislado no âmbito do RGPD (*compliance*) nas suas Organizações é o Encarregado pela Proteção de Dados/*Data Protection Officer* (EPD/DPO). 30,9% (21 refere que é o EPD/DPO e a Auditoria Interna13,2% (9) apenas a Auditoria Interna, 4,4% (3) referem ainda Entidade Externa.

Gráfico 3.24 - Em que medida considera que, na sua Organização, está claro o papel do responsável pela proteção de dados (EPD/ DPO) no que respeita às auditorias a realizar ao RGPD?



Da leitura do **Gráfico 24** é visivel que **52,9%** (36) dos respondentes considera **razoavelmente claro** o papel do EPD/DPO no que respeita às auditorias a realizar ao RGPD, enquanto 25% (17) responde totalmente claro e 14,7% (10) pouco claro. Apenas 7,4% (5) consideram nada claro.

Gráfico 3.25 - Na sua Organização, como são asseguradas pelo EPD/DPO as auditorias ao RGPD (quer periódicas quer não programadas) previstas na Lei 58/2019, Art.º 11º, alínea a)?



Conforme se pode verificar no **Gráfico 3.25**, **45,6%** (31) dos respondentes referiu que as auditorias ao RGPD a assegurar pelo EPD/DPO são **realizadas pela Auditoria Interna** 26,5% (18) responderam que estas são realizadas diretamente pelo EPD/DPO. Apenas 11,8% (8) referiram que as mesmas são subcontratadas a uma entidade externa.

As restantes respostas (11) todas distintas e que têm uma representatividade individual de 1,5% representam no total 16,5% uma franja com algum significado e que traz substância qualitativa à informação e que aqui importará pormenorizar.

Verifica-se que há 3 grandes grupos de respostas:

- As que denotam desconhecimento com 4 respostas (6%) - "Desconheço", "Não sei" "Não tenho conhecimentos nesta área", "Não tenho a certeza";

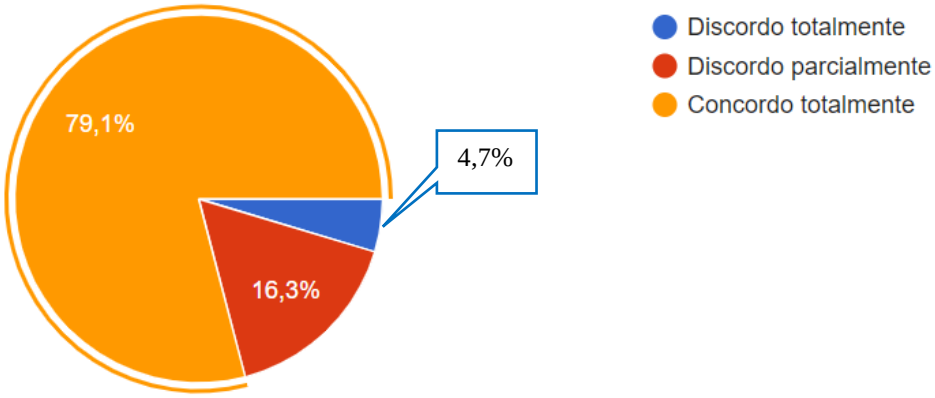
- As que referem a não realização destas auditorias, com 6 respostas (9%) - "Nunca existiram" "Ainda não foi feita qualquer auditoria", "Ainda não foi realizada", "Ainda não foram realizadas", "Não se realizam auditorias ao RGPD", "Não são realizadas";

- E as que se referem a outras áreas como responsáveis por realizar estas auditorias - 1 resposta (1,5%) "*Audit corporate*".

A questão 26 do questionário era de resposta condicionada, dirigida essencialmente a quem na questão 25 respondesse que as auditorias ao RGPD eram realizadas na sua Organização por outra entidade que não a Auditoria Interna o que olhando para o gráfico 25 resultaria em 37 potenciais respostas, no entanto constatou-se que houve 43 respostas no total.

O que não invalida, no entanto, o que se pretende aferir, isto é, caso as auditorias ao RGPD não sejam realizadas pela auditoria interna, em que medida concordam, que esta possa no âmbito do RGPD prestar apoio consultivo ao EPD/DPO ou a entidade externa?

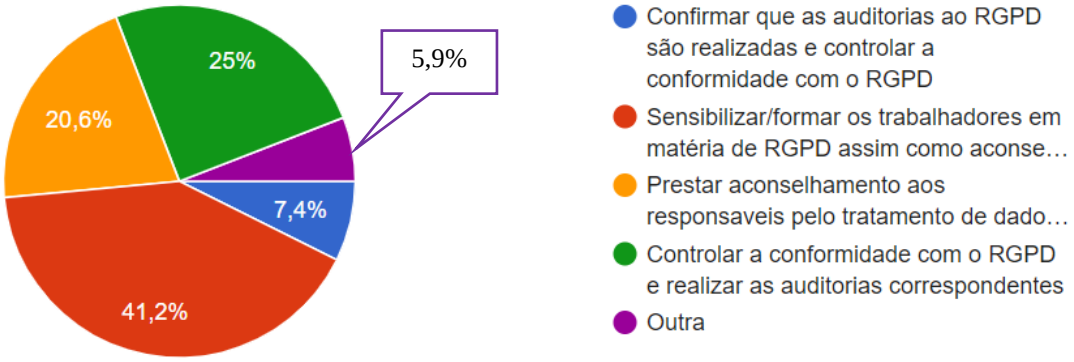
Gráfico 3.26 – Caso as auditorias ao RGPD não sejam realizadas pela Auditoria Interna, em que medida concorda, que esta possa prestar apoio consultivo ao EPD/DPO ou Entidade Externa?



Conforme se pode observar no **Gráfico 3.26**, **79,1%** (34) dos respondentes concordam totalmente que a Auditoria Interna possa apoiar consultivamente o EPD/DPO ou entidade externa, caso não seja esta, a realizar as auditorias no âmbito do RGPD. Por outro lado 16,3% (7) dos respondentes discordam parcialmente e apenas 4,7% (2) discordam totalmente.

Na questão seguinte, 27 e última do questionário, pretende-se perceber quais são as responsabilidades, essencialmente reconhecidas pelos respondentes, ao EDP/DPO, de uma forma mais qualitativa.

Gráfico 3.27 - Considera que na sua Organização as responsabilidades do EPD/DPO, são essencialmente:



Veja-se no **Gráfico 3.27** que, se por um lado **41,2%** (28) dos respondentes considera como uma das principais atribuições é «Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a Proteção de dados». Logo em seguida com **25% (17)** dos respondentes consideram como responsabilidade essencial do EPD/DPO nas suas organizações **«Controlar a conformidade com o RGPD e realizar as auditorias correspondentes»**.

20,6% (14) consideram que é «Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)». Apenas **7,4% (5)** referem como responsabilidade essencial do EPD/DPO **«Confirmar que as auditorias ao RGPD são realizadas e controlar a conformidade com o RGPD»,** os restantes 5,9% (4) respondem «outra».

3.4 Estatística inferencial

A estatística inferencial é um método estatístico que tem como objetivo tirar conclusões com base numa amostra, de modo a que as informações possam ser extrapoladas para o todo, através da utilização de técnicas que permitam obter um razoável grau de confiança nas afirmações feitas, sobre a população/universo, tendo por base os resultados da amostra.

Dado que a taxa de resposta ao questionário, 5,36%, se revelou pouco representativa do universo dos auditores internos (1268), considerou-se que a análise inferencial dos dados permitiria avaliar a partir da amostra o comportamento do universo, presumindo que o universo se comportaria da mesma forma do que a amostra.

Para a validação das hipóteses formuladas utilizaram-se tabelas com os coeficientes de correlação linear de *Pearson*, método estatístico inferencial através do qual se pretende aferir se existe relação linear entre duas variáveis aleatórias e a força dessa relação.

A correlação linear de *Pearson* assume valores de -1 (correlação negativa perfeita) e de 1 (correlação positiva perfeita).

Para a classificação da correlação, consideraram-se os seguintes intervalos:

- correlação **muito forte** quando $|\rho| > 0,9$
- **forte** quando $0,7 < |\rho| < 0,9$
- **moderada** quando $0,5 < |\rho| < 0,7$
- **fraca** quando $0,3 < |\rho| < 0,5$
- **Inexistente ou nula** $|\rho| < 0,3$.

Quando estamos perante uma "correlação perfeita" significa que se ocorrer uma alteração numa das variáveis, tal implica uma alteração perfeitamente identificável na outra variável.

Por outro lado, quando se trata de uma "correlação nula" significa que caso ocorra uma alteração numa das variáveis, tal não altera em nada o comportamento da outra.

De modo a proceder ao estudo inferencial das respostas ao questionário, e validar as hipóteses levantadas, analisaram-se as caraterísticas das respetivas variáveis, com recurso ao *Software* de análise estatística *IBPM SPSS Statístics*, realizando as seguintes correlações:

Hipótese 1 - Existe relação entre o nível de clareza com que é entendido o papel da Auditoria Interna no RGPD e a observância na Organização do Modelo das três linhas de defesa.

Quadro 3.1- Correlação de *Pearson* para validação da Hipótese 1

		12. A sua Organização segue o Modelo das 3 Linhas de Defesa?	24. Em que medida considera que, na sua Organização, está claro o papel do responsável pela proteção de dados (EPD/ DPO) no que respeita às auditorias a realizar ao RGPD?
12. A sua Organização segue o Modelo das 3 Linhas de Defesa?	Correlação de Pearson	1	-,161
	Sig. (2 extremidades)		,189
	N	68	68
24. Em que medida considera que, na sua Organização, está claro o papel do responsável pela proteção de dados (EPD/ DPO) no que respeita às auditorias a realizar ao RGPD?	Correlação de Pearson	-,161	1
	Sig. (2 extremidades)	,189	
	N	68	68

O **Quadro 3.1**, foi extraído da tabela de correlações de *Pearson* e revela que o nível de correlação entre as questões 12 e 24, com o valor de **-0,161** ($|\rho| < 0,3$) o que significa que a **correlação é inexistente ou nula**. Assim, pode afirmar-se que não há relação entre o nível de clareza nas Organizações, do papel do responsável pela Proteção de dados no que respeita às auditorias a realizar ao RGPD e o facto das Organizações seguirem o Modelo das 3 linhas de defesa.

Hipótese 2 - A preparação da Auditoria Interna, nas Organizações, para corresponder aos novos desafios trazidos pelo RGPD, relaciona-se com a proteção de dados ser uma prioridade na gestão da informação para as Organizações.

Quadro 3.2 - Correlação de *Pearson* para validação da Hipótese 2

		15. Considera que a proteção de dados é uma prioridade na gestão de informação da sua Organização?	20. Considera que na sua Organização, a Auditoria Interna está preparada para corresponder aos novos desafios trazidos pelo RGPD?
15. Considera que a proteção de dados é uma prioridade na gestão de informação da sua Organização?	Correlação de Pearson	1	,481**
	Sig. (2 extremidades)		,000
	N	68	68
20. Considera que na sua Organização, a Auditoria Interna está preparada para corresponder aos novos desafios trazidos pelo RGPD?	Correlação de Pearson	,481**	1
	Sig. (2 extremidades)	,000	
	N	68	68

**. A correlação é significativa no nível 0,01 (2 extremidades).

O **Quadro 3.2**, igualmente retirado da tabela de coeficientes de correlação de *Pearson*, reflete uma correlação entre as questões 15 e 20, com o valor de **0,481**, compreendido no intervalo $0{,}3 < |\rho| < 0{,}5$, o que determina que **existe uma correlação significativa**, ainda que de fraca significância, entre a preparação da Auditoria Interna para corresponder aos novos desafios trazidos pelo RGPD, relaciona-se com a proteção de dados ser uma prioridade na gestão da informação para as Organizações.

Hipótese 3 - Existe relação entre o grau de maturidade (anos) na função de auditor e o entendimento das funções atribuídas no âmbito do RGPD ao EPD/DPO quanto às auditorias a assegurar neste âmbito.

Quadro 3.3 - Correlação de *Pearson* para validação da Hipótese 3

		27. Considera que na sua Organização as responsabilidades do EPD/DPO, são essencialmente:	2. Indique há quantos anos exerce funções na Auditoria Interna:
27. Considera que na sua Organização as responsabilidades do EPD/DPO, são essencialmente:	Correlação de Pearson	1	-,092
	Sig. (2 extremidades)		,457
	N	68	68
2. Indique há quantos anos exerce funções na Auditoria Interna:	Correlação de Pearson	-,092	1
	Sig. (2 extremidades)	,457	
	N	68	68

O **Quadro 3.3** retirado da tabela de coeficientes de correlação de *Pearson*, evidencia uma correlação de **-0,092** ($|\rho| < 0,3$) entre as questões 2 e 27, o que significa que **não existe correlação** ou que existe uma **correlação nula** entre a maturidade, em anos, em funções de Auditoria Interna o que a Organização considera que são, essencialmente as responsabilidades do EPD/DPO.

Hipótese 4 – O grau de preparação tecnológica das Organizações para o cumprimento do RGPD está relacionado com existência de um EPD/DPO ou entidade externa responsável pela proteção de dados na Organização.

Quadro 3.4 - Correlação de *Pearson* para validação da Hipótese 4

		19.Na sua Organização existe um encarregado da proteção de dados (EPD)/ data protection officer (DPO) ou entidade externa, responsável pela proteção de dados?	18.Considera que a sua Organização se encontra tecnologicamente preparada para o cumprimento do Regulamento Geral de Proteção de Dados (RGPD)?
19.Na sua Organização existe um encarregado da proteção de dados (EPD)/ data protection officer (DPO) ou entidade externa, responsável pela proteção de dados?	Correlação de Pearson	1	,091
	Sig. (2 extremidades)		,458
	N	68	68
18.Considera que a sua Organização se encontra tecnologicamente preparada para o cumprimento do Regulamento Geral de Proteção de Dados (RGPD)?	Correlação de Pearson	,091	1
	Sig. (2 extremidades)	,458	
	N	68	68

O **Quadro 3.4** retirado da tabela dos coeficientes de correlação de Pearson, reflete uma correlação entre as questões 18 e 19, com o valor de 0,091 ($|\rho| < 0,3$) o que significa que a **correlação é nula ou inexistente** na relação entre a existência nas Organizações de um Encarregado da proteção de dados ou entidade externa responsável pela proteção de dados e o nível de preparação tecnológica da Organizações para o cumprimento do RGPD.

Hipótese 5 - A existência nas Organizações de um Encarregado da proteção de dados ou entidade externa com esta responsabilidade relaciona-se com os procedimentos vigentes na Organização darem resposta aos requisitos do RGPD.

Quadro 3.5 - Correlação de *Pearson* para validação da hipótese 5

		19.Na sua Organização existe um encarregado da proteção de dados (EPD)/ data protection officer (DPO) ou entidade externa, responsável pela proteção de dados?	17.Considera que os atuais procedimentos vigentes na sua Organização, respondem aos requisitos do Regulamento Geral de Proteção de Dados (RGPD)?
19. Na sua Organização existe um encarregado da proteção de dados (EPD)/ data protection officer (DPO) ou entidade externa, responsável pela proteção de dados?	Correlação de Pearson	1	,351**
	Sig. (2 extremidades)		,003
	N	68	68
17. Considera que os atuais procedimentos vigentes na sua Organização, respondem aos requisitos do Regulamento Geral de Proteção de Dados (RGPD)?	Correlação de Pearson	,351**	1
	Sig. (2 extremidades)	,003	
	N	68	68

**. A correlação é significativa no nível 0,01 (2 extremidades).

O **Quadro 3.5**, retirado da tabela de coeficientes de correlação de *Pearson*, evidencia uma correlação entre as questões 17 e 19, com o valor de **0,351**, situado no intervalo $0{,}3 < |\rho| < 0{,}5$, o que determina que **há correlação significativa**, entre a existência nas Organizações de um Encarregado da proteção de dados ou entidade externa com esta responsabilidade e os procedimentos vigentes na Organização darem resposta aos requisitos do RGPD.

Hipótese 6 – Existe relação entre o estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD e a preparação da Auditoria Interna para responder aos novos desafios que este novo enquadramento traz.

Quadro 3.6 - Correlação de *Pearson* para validação da Hipótese 6

		16.Em que estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD (incluindo a Lei 58/2019), considera que a sua Organização se encontra?	20. Considera que na sua Organização, a Auditoria Interna está preparada para corresponder aos novos desafios trazidos pelo RGPD?
16. Em que estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD (incluindo a Lei 58/2019), considera que a sua Organização se encontra?	Correlação de Pearson	1	,454**
	Sig. (2 extremidades)		,000
	N	68	68
20. Considera que na sua Organização, a Auditoria Interna está preparada para corresponder aos novos desafios trazidos pelo RGPD?	Correlação de Pearson	,454**	1
	Sig. (2 extremidades)	,000	
	N	68	68

**. A correlação é significativa no nível 0,01 (2 extremidades).

O **Quadro 3.6**, retirado da tabela de coeficientes de correlação de *Pearson*, evidencia uma correlação entre as questões 16 e 20, com o valor de 0,454, compreendido no intervalo $0{,}3 < |\rho| < 0{,}5$, o que indica que, apesar de com fraca significância, **existe correlação significativa** entre o estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD (incluindo a Lei 58/2019) e a que nível está preparada a Auditoria Interna para corresponder aos novos desafios trazidos pelo RGPD.

3.5 Interpretação dos resultados

3.5.1 Análise unidimensional

- ✓ **58,9%** dos auditores internos respondentes têm **idade superior a 45 anos**, 36,7% têm entre 25 a 44 anos e apenas 4,4% têm menos de 25 anos.
- ✓ **50%** dos respondentes têm entre **11 a 15 anos em funções de auditoria**, 29,4% dos quais tem mais de 15 anos, por outro lado 19,1% têm menos de 2 anos na função.
- ✓ **42,6%** tem formação nas áreas de **Auditoria/Gestão/Administração**, 13,2% nas áreas de Contabilidade/ Fiscalidade e 10,3% em Economia/Finanças.

- ✓ **36,8%** da amostra são **Auditores**, 25% são, Diretores/ Responsáveis e 17,6% Auditores seniores.
- ✓ Apenas **64,7%** são **membros** do Instituto Português de Auditoria Interna (**IPAI**).
- ✓ **73,5%** das Organizações respondentes são **entidades privadas**.
- ✓ Os **setores** mais fortemente representados nesta amostra são os dos **Transportes** com **29,4%**, Outros Serviços com 25% e Comércio e Distribuição com 14,7%.
- ✓ **39,7%** dos inquiridos trabalha em Organizações cujo **número de colaboradores** está entre os **500 e os 2000**, 20, 6% em Organizações com mais de 5000 trabalhadores e 17,6% cujo número de trabalhadores está acima dos 2000 e abaixo dos 5000;
- ✓ **50%** dos respondentes exerce funções em Organizações cujas equipas de Auditoria Internat êm **mais de 10 auditores**, 23,5% entre 2 e 5 auditores e 17,6%, entre 6 e 10 auditores, apenas 8,8% das Organizações têm um único auditor interno.
- ✓ **41,2%** refere reportar a **Vogal do Conselho de Administração**, 32,4% ao Presidente do Conselho de Administração e apenas 14,6% a uma Comissão de Auditoria.
- ✓ **88,2%** responde que a Auditoria Interna da sua Organização se **rege pelos Standards** internacionais do *Institute of Internal Auditors* (**IIA**), havendo ainda a registar 11,8% que refere que não.
- ✓ **82,4%** dos respondentes refere que a sua Organização **segue o Modelo das três linhas de Defesa** e 17,6% respondem que não.
- ✓ **52,9%** dos inquiridos considera que a sua Organização, **conhece aprofundadamente** os termos e os princípios previstos no Regulamento Geral de Proteção de Dados (RGPD) e as suas implicações, 39,7% refere que conhece razoavelmente.
- ✓ **88,2%** refere que **foram efetuadas** na sua Organização, **ações de formação**/ **sensibilização** sobre os princípios norteadores do Regime Geral de Proteção de Dados (RGPD), enquanto 11,8% refere que não.

- ✓ **57,4%** Considera a proteção de dados **muito prioritária** na gestão de informação da sua Organização, 39,7% considera de prioridade moderada.
- ✓ **67,6%** considera que a sua Organização em termos de compreensão da natureza e do impacto do RGPD (incluindo a Lei 58/2019) se encontra num estágio de **razoável maturidade**, 20,6% considera muito madura e 10,3% pouco madura.
- ✓ **64,7%** dos respondentes considera que os atuais procedimentos vigentes na sua Organização, **respondem razoavelmente**, aos requisitos do Regulamento Geral de Proteção de Dados (RGPD)e 26,5% considera que respondem integralmente.
- ✓ **66,2%** Considera que a sua Organização se encontra **razoavelmente preparada** ao nível tecnológico para o cumprimento do Regulamento Geral de Proteção de Dados (RGPD) e 22,1% considera que as suas Organizações se encontram totalmente preparadas.
- ✓ **86,8%** dos respondentes refere que na suas Organizações **existe um encarregado da proteção de dados (EPD)/*data protection officer*(DPO),** 7,4% referiu ter uma entidade externa como responsável pela proteção de dados e 5,9% referiu não existir.
- ✓ **64,7%** dos inquiridos considera que na sua Organização, a **Auditoria Interna está razoavelmente preparada** para corresponder aos novos desafios trazidos pelo RGPD, em igualdade de circunstâncias, ambos com 16,2% estão os que consideram as suas Organizações muito bem preparadas e os que consideram que as suas Organizações estão parcialmente preparadas. Apenas 2,9% considera a sua Organização nada preparada.
- ✓ **76,5%** dos respondentes considera que na sua Organização, a **Auditoria Interna** enquanto 3.ª linha de defesa, **assume um papel muito relevante** para a criação de valor na operacionalização das auditorias ao RGPD e 13,2% considera o seu papel determinante. Apenas 7,4% e 2,9% consideram o papel da Auditoria Interna neste âmbito pouco relevante e nada relevante, respetivamente.
- ✓ **73,5%** dos inquiridos **concordam totalmente** que as auditorias ao RGPD, quando realizadas pela Auditoria Interna enquanto 3.ª linha de defesa, constituem uma mais

valia que se concretiza em ações de melhoria, ganhos efetivos de eficiência e de confiança na organização, 26,5% concorda parcialmente.

- ✓ **45,6%** dos respondentes referiu que na sua Organização **quem realiza o controlo da conformidade** com o regulado/legislado no âmbito do RGPD (***Compliance***) é o Encarregado Proteção de Dados/*DataProtection Officer* **(EPD/DPO),** 30,9% respondeu ser o EPD/ DPO e Auditoria Interna. 13,2% referiu ser a Auditoria Interna 4,4% Entidade externa.

- ✓ **52,9%** dos inquiridos consideram que, na sua Organização, **está razoavelmente claro o papel do responsável pela proteção de dados** (EPD/ DPO) no que respeita às auditorias a realizar ao RGPD, 25% considera totalmente claro e apenas 14, 7% e 7,4% consideram pouco claro e nada claro, respetivamente.

- ✓ **45,6%** dos respondentes referiram que na sua Organização, **as auditorias ao RGPD** (quer periódicas quer não programadas) previstas na Lei 58/2019, Art.º 11º, alínea a), a assegurar pelo EPD/DPO, **são realizadas pela Auditoria Interna**, 26,5% referiu que são realizadas diretamente pelo EPD/DPO e 11,8% referiram que estas são subcontratadas a Entidade externa. Houve ainda quem referisse desconhecer e quem indicasse não terem sido efetuadas à data auditorias neste âmbito.

- ✓ **79,1%** dos respondentes **concorda totalmente que a Auditoria Interna** possa **prestar apoio consultivo ao EPD**/DPO ou Entidade Externa, no caso desta não realizar as auditorias ao RGPD. 16,3% discorda parcialmente e 4,7% discorda totalmente.

- ✓ **41,2%** dos inquiridos considera que na sua Organização **as responsabilidades do EPD/DPO,** são essencialmente: **"Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados"**, 25% considera que será "Controlar a conformidade com o RGPD e realizar as auditorias correspondentes", 20,6% responde "Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados", apenas **7,4% considera que será "Confirmar que as auditorias ao RGPD são realizadas e controlar a conformidade com o RGPD"** e 5,9% "Outra".

3.5.2 Análise Inferencial

Da análise inferencial às hipóteses levantadas, constatou-se o seguinte:

Relativamente à **Hipótese 1** em que se pretendia validar a existência de relação entre o nível de clareza com que é entendido o papel da Auditoria Interna no RGPD (por contraponto com as funções atribuídas ao EPD/DPO) e a observância na Organização do Modelo das três linhas de defesa. Através da correlação de *Pearson* entre duas variáveis, as questões 12 e 24 do questionário, verificou-se a **inexistência de qualquer correlação** entre elas, o que significa que **o presumido na Hipótese 1, não se confirma.**

Quanto à **Hipótese 2,** em que se pretendia validar a existência de relação entre o nível de preparação da Auditoria Interna para corresponder aos novos desafios trazidos pelo RGPD e a proteção de dados ser uma prioridade na gestão da informação nas Organizações, constatando-se pela correlação de *Pearson* entre duas variáveis, as questões 15 e 20 do questionário, **existir uma correlação significativa, confirmando-se o admitido na Hipótese 2.**

Com a formulação da **Hipótese 3** pretendia validar-se a existência de relação entre o grau de maturidade (anos) na função de auditor e o entendimento das funções atribuídas no âmbito do RGPD ao EPD/DPO quanto às auditorias a assegurar neste âmbito, tendo-se verificado por correlação de *Pearson* entre duas variáveis, as questões 2 e 27 do questionário, a **inexistência de qualquer correlação** entre elas. O que significa que **o presumido na Hipótese 3, não se confirma.**

A **Hipótese 4** pretendia validar a relação entre o grau de preparação tecnológica das Organizações para o cumprimento do RGPD e a existência de um EPD/DPO ou entidade externa responsável pela proteção de dados na Organização. Através da correlação de *Pearson* entre duas variáveis, as questões 18 e 19 do questionário, verificou-se a **inexistência de qualquer correlação** entre estas, o que significa que **o presumido na Hipótese 4, não se confirma.**

Com a **Hipótese 5** pretendia validar-se a relação entre a existência nas Organizações de um Encarregado da proteção de dados ou entidade externa com esta responsabilidade com os procedimentos vigentes na Organização darem resposta aos requisitos do

RGPD. constatando-se pela correlação de *Pearson* entre duas variáveis, as questões 17 e 19 do questionário, **existir uma correlação significativa, confirmando-se o admitido na Hipótese 5.**

Com a formulação da Hipótese 6 pretendia-se validar a existência de relação entre o estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD e a preparação da Auditoria Internapara responder aos novos desafios que este novo enquadramento traz. Tendo-se constatado através da correlação de *Pearson* entre duas variáveis, as questões 16 e 20 do questionário, **existir uma correlação significativa, confirmando-se o admitido na Hipótese 6.**

4 Conclusão

Vivem-se tempos desafiantes para a maioria das Organizações, em que a necessidade de se reinventarem os negócios se tornou uma constante, tempos de grande imprevisibilidade e em que tudo acontece a uma velocidade furiosa. Situação que a pandemia por Covid 19 à escala global, e por consequência uma crise económica sem precedentes, veio acentuar.

Por outro lado, não é de hoje que os auditores internos consideram no âmbito dos seus trabalhos e preocupações os riscos associados às novas tecnologias de informação e informáticos. A crescente utilização do correio eletrónico e das redes sociais como meio preferencial de comunicação e de desenvolvimento do negócio, nomeadamente os negócio *on-line*, veio potenciar os riscos relacionados com a segurança da informação e com a proteção dos dados, razão pela qual os auditores internos viram uma vez mais a necessidade de se prepararem para os novos desafios e munir-se de competências e ferramentas que lhes permitissem dar resposta e se possível antecipar-se às novas necessidades deste mundo cada vez mais informatizado, dominado pelo digital e de tecnologias avançadas, em que a robótica e/ou a inteligência artificial já não são obra da ficção cientifica, mas uma realidade atual e em franca expansão.

A Auditoria Interna tem vindo assim e cada vez mais a alargar a sua esfera de atuação e a assumir-se como um parceiro estratégico da gestão, cujo foco é a criação de valor para as Organizações, algo que agora se torna, ainda mais vital e que para os auditores internos constitui uma oportunidade.

Assim, nesta Dissertação procurou-se compreender qual o papel da Auditoria Interna, enquanto terceira linha de defesa, no RGPD, por contraponto com as funções atribuídas ao Responsável pela Proteção de Dados, que, de acordo com a nova Lei, incluem «assegurar a realização de auditorias […]».

As conclusões obtidas a partir deste estudo, tiveram como principal constrangimento o facto do número de respostas aos questionários ter sido inferior ao esperado, dado que o tema seria à partida aliciante quer pela sua atualidade quer pela utilidade. Ainda assim a taxa de resposta foi abaixo do expectável, o que se julga ser em parte justificado pelo

facto da divulgação do questionário ter ocorrido a 30 de Março, em plena fase de confinamento, decorrente da pandemia por Covid-19 e consequente impacto, tanto ao nivel pessoal como profissional.

Há ainda a referir que, os métodos de investigação utilizados, suportados na análise estatística das respostas ao questionário, embora permitam evidenciar relações, não facultam qualquer explicação que clarifique o sentido dessas relações.

Pese embora, as referidas limitações, entende-se que o estudo realizado permite responder com razoável confiança, à questão formulada como ponto de partida.

Assim, constata-se que:

Apesar da maioria dos inquiridos ter respondido que as suas Organizações seguem o Modelo das Três Linhas de Defesa, há uma parte significativa dos respondentes que referem que na sua Organização, as auditorias ao RGPD são realizadas diretamente pelo EPD/DPO.

Acresce que, apenas uma quarta parte dos respondentes consideram que, nas suas Organizações, está totalmente claro o papel do responsável pela proteção de dados, a maioria considera que está razoavelmente claro. Os restantes consideram pouco e nada claro respetivamente (mais de 20%)

De referir ainda que embora a maioria considere que, quer a Auditoria Interna quer as suas Organizações, são conhecedoras e estão preparadas para responder aos requisitos e novos desafios trazidos pelo RGPD, constatou-se que ao nível do entendimento do que são as funções essenciais do EPD/DPO, a maioria considera que será "Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados", o que não deixa de ser uma das funções relevantes, mas não o *core* desta função.

Um quarto dos respondentes considera como função essencial do EPD/DPO «Controlar a conformidade com o RGPD e realizar as auditorias correspondentes" (funções da 3ª linha) e apenas uma minoria (menos de 10%) considerou que será "Confirmar que as auditorias ao RGPD são realizadas e controlar a conformidade com o RGPD" (funções de 2ª linha).

Face ao exposto considera-se evidenciado que não é claro para a maioria dos respondentes, o papel da Auditoria Interna no RGPD enquanto 3ª linha de defesa, por contraponto com as funções atribuídas ao EPD/DPO (de 2ª linha).

Quanto às hipóteses formuladas, o estudo possibilitou concluir que:

Não existe relação entre o nível de clareza com que é entendido o papel da Auditoria Interna no RGPD e a observância na Organização do Modelo das três linhas de defesa. Refutando assim a Hipótese 1.

Por outro lado, constatou-se que o nível de preparação da Auditoria Interna para corresponder aos novos desafios trazidos pelo RGPD, relaciona-se com a proteção de dados ser uma prioridade na gestão da informação nas Organizações. Validando assim a Hipótese 2.

Verificou-se ainda, a inexistência de relação entre o grau de maturidade (anos) na função de auditor e o entendimento das funções atribuídas no âmbito do RGPD ao EPD/DPO quanto às auditorias a assegurar neste âmbito. Refutando a Hipótese 3.

De igual forma se verificou que o grau de preparação tecnológica das Organizações para o cumprimento do RGPD não se relaciona com existência de um EPD/DPO ou entidade externa responsável pela proteção de dados, na Organização. Refutando a Hipótese 4.

Constatou-se, no entanto, que a existência nas Organizações de um Encarregado da proteção de dados ou entidade externa com esta responsabilidade se relaciona com os procedimentos vigentes na Organização darem resposta aos requisitos do RGPD. Validando assim a Hipótese 5.

Mais se verificou a existência de relação entre o estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD e a preparação da Auditoria Interna para responder aos novos desafios que este novo enquadramento traz. Validando a Hipótese 6.

A análise das hipóteses veio assim, corroborar e robustecer o apurado na análise descritiva.

Em suma, pode-se concluir desta investigação, que a Auditoria Interna o EPD assumem, papeis distintos, mas complementares no que respeita ao sistema de gestão de

compliance do RGPD, estando a função do EPD ao nível da segunda linha de defesa e cabendo ao auditor interno um papel ao nível da terceira linha que vai muito além da conformidade com o Regulamento e cuja objetividade e independência que a carateriza, não é sinónimo de isolamento.

A Auditoria Interna terá ao nível do RGPD, tal como noutros âmbitos, um papel determinante para as Organizações, de parceiro estratégico, cujo olhar isento e transversal, permitirá não só assegurar e evidenciar o cumprimento dos requisitos do RGPD, mas sobretudo a criação de valor, nomeadamente através da identificação de áreas de melhoria ao nível dos controlos sua eficiência/eficácia e potenciais novos riscos, possibilitando à gestão tomar decisões estratégicas de forma mais assertiva e antecipada. Posição que a revisão do Modelo das Três Linhas veio reforçar.

No entanto, ficou demonstrado que não é totalmente claro o papel da Auditoria Interna no Regulamento Geral de Proteção de Dados enquanto terceira linha de defesa, por contraponto com as funções atribuídas ao EPD/DPO no que respeita à realização das auditorias neste âmbito, face ao que é determinado pelo novo Regulamento/Lei.

Como sugestão para trabalhos futuros e face ao enquadramento atual, considero de toda a pertinência estudar o impacto da pandemia por Covid 19 na função de Auditoria Interna.

5 Bibliografia

ANDERSON, Alan W - ***THE GOAL OF THE AUDIT*** - www.kscpa.org/writable/files/Self-Study/AAE/13._aae_self-study.pdf.

Batista da Costa, Carlos, **Auditoria Financeira - Teoria e Prática**, Letras e Conceitos, Lisboa, 11ª Edição, 2017.

Bento, A. (2012, maio). Como Fazer Uma Revisão da Literatura: Considerações Teóricas e Práticas. Revista JÁ (Associação Académica da Universidade da Madeira), n.º 65, ano VII (p.p. 42-44). ISSN: 1647-8975. http://www3.uma.pt/bento/Repositorio/Revisaodaliteratura.pdf. Consultado em março 2020.

Chartered Institut of Internal Auditors – **What is Internal Audit?** - https://www.iia.org.uk. Consultado em fevereiro de 2020.

Declaração de Posicionamento do IIA: **As três linhas de defesa no gerenciamento eficaz de riscos e controles** (2013). https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control%20Portuguese.pdf. Consultado em abril 2020.

Ferreira, P. L. (2005). *Estatística descritiva e inferencial*. *Faculdade de Economia – Universidade de Coimbra*. https://estudogeral.sib.uc.pt/bitstream/10316/9961/1/AP200501.pdf. Consultado em julho/agosto de 2020.

IIA - *Institute of Internal Auditors* ***The Impact of Globalization on Internal Auditors: The Evolution of Internal Auditing*** (2002). https://na.theiia.org/about-us/Public%20Documents/Sawyer_Award_2002.pdf. Consultado em maio 2020.

IIA - *Institute of Internal Auditors* (2017). ***International standards for the professional practice of internal auditing***. https://na.theiia.org/standardsguidance/Public Documents/IPPF-Standards-2017.pdf

IIA - Institute of Internal Auditors **– Documento de Exposição – *Três Linhas de Defesa*** (junho 2019): https://na.theiia.org/translations/PublicDocuments/3LOD-IIA-Exposure-Document-Portuguese.pdf

IIA - *Institute of Internal Auditors* - ***ONRISK A Guide to Understanding, Aligning, And Optimizing Risk 2020***. http://contentz.mkt5790.com/lp/2842/275148/OnRisk-2020-Report_0.pdf Consultado em agosto 2020.

IIA Portugal - IPAI – **O Modelo das Três Linhas do IIA** – uma atualização das Três Linhas de Defesa (12/08/2020): https://www.ipai.pt/fotos/gca/o_modelo_das_tres_linhas_do_iia_v_jlp_3ago2020_vlcs_final_12ago2020_1597332421.pdf

IIA – *Institute of Internal Auditors* - **Alavancar o COSO nas três linhas de Defesa** (2015): https://global.theiia.org/translations/PublicDocuments/COSO-2015-3LOD-Thought-Paper-Portuguese.pdf. Consultado em abril 2020.

IPAI - Instituto Português de Auditoria Interna. (2013). *Enquadramento internacional de práticas profissionais de Auditoria Interna*.

IPAI - Marques, B. M & Mendes, F.F (2020) **Auditoria RGPD – Gestão da Privacidade Visão e o Papel do Auditor,** Lisboa.

Lei nº 58/2019 de 08 de Agosto de 2019: https://dre.pt/web/guest/pesquisa/-/search/122195231/details/normal?q=lei+58%2F2019. Consultada em novembro de 2019.

Lei nº 59/2019 de 08 de Agosto de 2019: https://dre.pt/web/guest/pesquisa/-/search/123815983/details/normal?q=lei+59%2F2019. Consultada em novembro de 2019.

LISBOA, Ibraim – **Manual de Auditoria Interna– Conceitos e práticas para implementar a auditoria interna**. Portal de Auditoria: www.portaldeauditoria.com.br.

Lopes, Petter (2019) RIPD e DPIA, o que são e quando usar: https://periciacomputacional.com/ripd-e-dpia-o-que-sao-e-quando-usar/. Consultado em agosto/setembro 2020.

Magalhães, F. (2018). **Regulamento Geral de Proteção de Dados**. Ordem dos Contabilistas Certificados. https://www.occ.pt/fotos/editor2/rgpd-fmagalhaesmanual.pdf Consultado em janeiro 2020.

MARKS, Norman - **A Look into the Future: the next evolution of internal Audit Continuous Risk and Control Assurance, 2009** - www.iia.nl/SiteFiles/CRCA Final.pdf.

Miranda, M.L. (2019) Auditoria InternaOperacional - **Enquadramento Histórico e Evolução da Auditoria Interna**. Lisboa.

Morais, G. (2008). **A importância da Auditoria Interna para a gestão: caso das empresas portuguesas.** *18 - Congresso Brasileiro de Contabilidade* (pp. 1–15). Brasil. http://www.congressocfc.org.br/hotsite/trabalhos_1/570.pdf

Oliveira, N. M. F. de. (2013). **O papel da Auditoria Interna na monitorização do processo de governação das organizações.** Instituto Superior de Contabilidade e Administração de Lisboa.

Ordem dos Contabilistas Certificados. **Guia prático sobre o novo Regulamento Geral de Proteção de Dados (RGPD)**: https://www.occ.pt/fotos/editor2/gprpd-ultima3maio2018.docx**.** Consultado em junho de 2020.

Pinheiro, J. L. (2014). **Auditoria Interna: Manual Prático para Auditores Internos**. Lisboa: Rei dos Livros.

Quivy, R. &, & Campenhoudt, L. Van. (1998). **Manual de investigação em ciências sociais**. *Gradiva*, 289. https://d1wqtxts1xzle7.cloudfront.net/39505931/manual_investigacao_quivy.pdf?14

46065341=&response-content-disposition=inline%3B+filename%3DRaymond_Quivy.pdf. Consultado em julho de 2020.

RAMAMOORTI, Sridhar – ***Internal Audting: history, evolution and prospects*** – *The Institute of Internal Auditors Research Foundation,* pp. 1-23, 2003.

Rangel, A. R. (2016). **As três linhas de Defesa e a Cultura de Gestão do Risco Operacional**.https://www.linkedin.com/pulse/3-linhas-de-defesa-e-cultura-gest%C3%A3o-do-risco-alexandre-rangel. Consultado em maio 2020.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Consultado em novembro de 2019.

Rebula, U. **Estatística Aplicada** - https://drive.google.com/file/d/1lWTXEBVu7bvdQcqvnO6mRu5j5vRerpkX/view. Consultado em setembro 2020.

Saldanha, Nuno (2019) **RGPD Guia para uma Auditoria de Conformidade** - Dados Privacidade, Implementação, Controlo, Compliance, FCA - Editora de informática Lda. Lisboa, 1ªEdição.

SAWYER, Lawrence B.; [et. al.] – ***Sawyer's Internal Auditing – The practice of Modern Internal Auditing***. EUA: *The Institute of Internal Auditors,* 2005. ISBN 0-89413-509-0.

Séneca, H. (2018), Exame Informática - **CNPD: Hospital do Barreiro multado em 400 mil euros por permitir acessos indevidos a processos clínicos** https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2018-10-19-cnpd-hospital-do-barreiro-multado-em-400-mil-euros-por-permitir-acessos-indevidos-a-processos-clinicos/

Swinkels, W. H. A. (2012). **Exploration of a theory of internal audit**: a study on the theoretical foundations of internal audit in relation to the nature and the control systems of Dutch Public Listed Firms (PP. 25-69). Eburon.

Teixeira, J. M., Revista Hits, artigo de opinião - **Auditoria Internado Compliance à Criação de Valor** https://www.pwc.pt/pt/hits/artigos-opiniao/jose-teixeira.html, consultado em junho 2020.

Universidade de Brasília – **Um pouco da história da Auditoria Interna**- http://unb2.unb.br/administracao/auditoria_interna/artigos/um_pouco_de_historia_da_auditoria_interna. Consultado em março de 2020.

APÊNDICES

APÊNDICE A

Questionáro e Respostas (*Google Forms*)

APÊNDICE A – QUESTIONÁRO E RESPOSTAS (*GOOGLE FORMS*)

3. Qual a sua área de Formação?	4.Qual a sua função na estrutura da Auditoria Interna?	5.É membro do Instituto Português de Auditoria Interna (IPAI)?	6.Qual a natureza da sua organização?	7.Qual o setor de atividade da sua Organização?	8.Qual o número de trabalhadores da sua organização?	9.Qual o número de Auditores Internos na sua Organização?	10.A quem reporta, hierarquicamente a Auditoria Interna, na sua organização?	11.A Auditoria Interna na sua Organização, rege-se pelos Standards Internacionais do Institute of Internal Auditors (IIA)?	12.A sua Organização segue o Modelo das 3 Linhas de Defesa?	13.Em que medida considera que a sua Organização, conhece os termos e os princípios previstos no Regulamento Geral de Proteção de Dados (RGPD) e as suas implicações?	14.Foram efetuadas na sua Organização, ações de formação/ sensibilização sobre os princípios norteadores do Regime Geral de Proteção de Dados	15.Considera que a proteção de dados é uma prioridade na gestão de informação da sua Organização?	16.Em que estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD (incluindo a Lei 58/2019), considera que a sua Organização se encontra?	17.Considera que os atuais procedimentos vigentes na sua Organização, respondem aos requisitos do Regulamento Geral de Proteção de Dados (RGPD)?	18.Considera que a sua Organização se encontra tecnologicamente preparada para o cumprimento do Regulamento Geral de Proteção de Dados (RGPD)?	19.Na sua Organização existe um encarregado da proteção de dados (EPD)/ data protection officer (DPO) ou entidade externa, responsável pela proteção de dados?	20. Considera que na sua Organização, a Auditoria Interna está preparada para corresponder aos novos desafios trazidos pelo RGPD?	21.Considera que na sua Organização, a auditoria interna enquanto 3.ª linha de defesa, assume um papel relevante/determinante e para a criação de valor na operacionalização das	22.Concorda que as auditorias ao RGPD, quando realizadas pela Auditoria Interna enquanto 3.ª linha de defesa, constituem uma mais valia que se concretiza em ações de melhoria, ganhos efetivos de	23.Na sua Organização quem realiza o controlo da conformidade com o regulado/legislado no âmbito do RGPD (Compliance)?	24.Em que medida considera que, na sua Organização, está claro o papel do responsável pela proteção de dados (EPD/ DPO) no que respeita às auditorias a realizar ao RGPD?	25.Na sua Organização, como são asseguradas pelo EPD/DPO as auditorias ao RGPD (quer periódicas quer não programadas) previstas na Lei 58/2019, Art.º 11º, alínea a)?	26.Caso as auditorias ao RGPD não sejam realizadas pela Auditoria Interna, em que medida concorda, que esta possa prestar apoio consultivo ao EPD/DPO ou Entidade Externa?	27. Considera que na sua Organização as responsabilidades do EPD/DPO, são essencialmente:
Engenharia	Auditor Sénior	Sim	Entidade Privada	Serviços	Entre 251 e 500 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Muito Madura	Sim, integralmente	Sim, totalmente preparada	Sim EPD/DPO	Muito bem preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Razoavelmente claro	São realizadas diretamente p	Concordo totalmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Informática de Gestão	Auditor	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Intern	Totalmente claro	São realizadas pela Auditoria	Discordo parcialmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Engenharia	Auditor Sénior	Sim	Entidade Privada	Outros serviços	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Muito Madura	Sim, integralmente	Sim, totalmente preparada	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Auditoria Interna	Totalmente claro	São realizadas pela Auditoria	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Engenharia	Auditor	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Razoavelmente claro	São realizadas pela Auditoria	Concordo totalmente	Prestar aconselhamento aos responsaveis pelo tratamento de dados e cooperar com a
Direito	Auditor	Não	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Intern	Totalmente claro	Não tenho a certeza	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e
Engenharia	Auditor	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Conselho executivo	Sim	Sim	Conhece razoavelmente;	Sim	Muito prioritário	Razoavelmente Madura	Sim, integralmente	Sim, totalmente preparada	Sim EPD/DPO	Parcialmente preparada	Muito relevante	Concordo parcialmente	Encarregado Proteção de Da	Razoavelmente claro	São subcontratadas a uma ent	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e
Engenharia	Supervisor/Coordenador	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Não sabe/ Não responde	Não sabe/ Não responde	Sim EPD/DPO	Muito bem preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Totalmente claro	São realizadas pela Auditoria	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Gestão/Administração	Auditor	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Sim, integralmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Auditoria Interna	Razoavelmente claro	São realizadas pela Auditoria	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Ciências - Biologia	Auditor	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Muito Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Muito bem preparada	Muito relevante	Concordo parcialmente	Encarregado Proteção de Da	Razoavelmente claro	Não tenho conhecimentos do	Discordo parcialmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria	Auditor	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Intern	Totalmente claro	São realizadas pela Auditoria	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Contabilidade / Fiscalidade	Diretor/Responsável	Sim	Entidade Privada	Comércio e distribuição	Entre 2001 e 5000 trabalhadores	Entre 2 a 5 Auditores	Director financeiro	Não	Não	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, integralmente	Sim, totalmente preparada	Sim EPD/DPO	Razoavelmente preparada	Pouco relevante	Concordo totalmente	Encarregado Proteção de Da	Razoavelmente claro	São realizadas diretamente p	Concordo totalmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Gestão/Administração	Diretor/Responsável	Não	Entidade Privada	Comércio e distribuição	Mais de 5000 trabalhadores	Entre 2 a 5 Auditores	audit do corporate	Sim	Sim	Conhece aprofundadamente	Sim	Prioridade moderada	Muito Madura	Sim, integralmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Totalmente claro	Audit Corporate		Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Contabilidade / Fiscalidade	Junior	Não	Entidade Privada	Serviços	Até 250 trabalhadores	Entre 2 a 5 Auditores	Manager	Sim	Não	Conhece aprofundadamente	Sim	Muito prioritário	Muito Madura	Sim, integralmente	Sim, totalmente preparada	Sim EPD/DPO	Muito bem preparada	Determinante	Concordo totalmente	EPD/ DPO e Auditoria Intern	Totalmente claro	São realizadas pela Auditoria	Interna	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Contabilidade / Fiscalidade	Auditor	Não	Entidade Pública	Comércio e distribuição	Entre 251 e 500 trabalhadores	Entre 2 a 5 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece razoavelmente;	Não	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Auditoria Interna	Razoavelmente claro	São realizadas pela Auditoria	Interna	Prestar aconselhamento aos responsaveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Contabilidade / Fiscalidade	Auditor	Não	Entidade Pública	Comércio e distribuição	Entre 251 e 500 trabalhadores	Entre 2 a 5 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece razoavelmente;	Não	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Auditoria Interna	Razoavelmente claro	São realizadas pela Auditoria	Interna	Prestar aconselhamento aos responsaveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Economia/Finanças	Supervisor/Coordenador	Não	Entidade Pública	Outros serviços	Entre 2001 e 5000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Não sabe/ Não responde	Não	Prioridade moderada	Pouco Madura	Sim, razoavelmente	Sim, razoavelmente	Não	Nada preparada	Nada relevante	Concordo totalmente	Ninguém realiza	Nada claro	Não se realizam auditorias ao RGPD		Outra
Gestão/Administração	Diretor/Responsável	Sim	Entidade Pública	Saúde	Até 250 trabalhadores	1 Auditor	Presidente do Conselho Adm	Sim	Sim	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Parcialmente preparada	Pouco relevante	Concordo totalmente	Encarregado Proteção de Da	Pouco claro	Ainda não foram realizadas	Discordo parcialmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Sistemas de Informação	Adiver	Sim	Entidade Privada	Telecomunicações e Média	Até 250 trabalhadores	1 Auditor	Presidente do Conselho Adm	Sim	Não	Conhece aprofundadamente	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, totalmente preparada	Sim EPD/DPO	Parcialmente preparada	Muito relevante	Concordo totalmente	Entidade Externa	Totalmente claro	São realizadas diretamente p	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Economia/Finanças	Diretor/Responsável	Sim	Entidade Privada	Outros serviços	Entre 501 e 2000 trabalhadores	Entre 6 a 10 Auditores	Comissão de Auditoria	Sim	Sim	Conhece aprofundadamente	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Determinante	Concordo totalmente	Auditoria Interna	Razoavelmente claro	São realizadas pela Auditoria	Interna	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Gestão/Administração	Diretor/Responsável	Sim	Entidade Pública	Outros serviços	Até 250 trabalhadores	Entre 2 a 5 Auditores	Presidente do Conselho Adm	Sim	Sim	Não sabe/ Não responde	Não	Prioridade moderada	Pouco Madura	Não sabe/ Não responde	Não sabe/ Não responde	Sim EPD/DPO	Muito bem preparada	Nada relevante	Concordo totalmente	Encarregado Proteção de Da	Nada claro	Ainda não foi feita qualquer a	Concordo totalmente	Outra
Direito	Técnico de Auditoria	Não	Entidade Privada	Banca, Seguros e Serviços fi	Entre 251 e 500 trabalhadores	Entre 2 a 5 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece razoavelmente;	Sim	Muito prioritário	Razoavelmente Madura	Sim, integralmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Area Jurídico (Compliance)	Razoavelmente claro	São realizadas diretamente p	Concordo totalmente	Confirmar que as auditorias ao RGPD são realizadas e controlar a conformidade com o RGPD
Gestão/Administração	Auditor Sénior	Não	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo parcialmente	Auditoria Interna	Razoavelmente claro	São realizadas pela Auditoria	Interna	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Gestão/Administração	Auditor Sénior	Não	Entidade Privada	Serviços	Até 250 trabalhadores	Entre 2 a 5 Auditores	Comissão de Auditoria	Sim	Sim	Conhece razoavelmente;	Não	Pouco prioritário	Pouco Madura	Sim, razoavelmente	Não, totalmente	Sim EPD/DPO	Parcialmente preparada	Muito relevante	Concordo parcialmente	Encarregado Proteção de Da	Razoavelmente claro	São realizadas diretamente p	Concordo totalmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Contabilidade / Fiscalidade	Auditor Sénior	Sim	Entidade Privada	Telecomunicações e Média	Mais de 5000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Muito Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Intern	Razoavelmente claro	São realizadas pela Auditoria	Interna	Confirmar que as auditorias ao RGPD são realizadas e controlar a conformidade com o RGPD
Economia/Finanças	Diretor/Responsável	Sim	Entidade Pública	Saúde	Entre 2001 e 5000 trabalhadores	Entre 2 a 5 Auditores	Vogal do Conselho de Admin	Sim	Não	Conhece aprofundadamente	Sim	Muito prioritário	Pouco Madura	Não	Não	Sim EPD/DPO	Razoavelmente preparada	Determinante	Concordo parcialmente	Encarregado Proteção de Da	Nada claro	São realizadas diretamente p	Concordo totalmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Auditoria / Gestão / Administração	Diretor/Responsável	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Entre 6 a 10 Auditores	Vogal do Conselho de Admin	Não	Não	Conhece aprofundadamente	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Parcialmente preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Razoavelmente claro	São subcontratadas a uma ent	Concordo totalmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Auditoria / Gestão / Administração	Auditor	Não	Entidade Privada	Banca, Seguros e Serviços fi	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Comissão de Auditoria	Sim	Sim	Conhece razoavelmente;	Sim	Muito prioritário	Pouco Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo parcialmente	EPD/ DPO e Auditoria Intern	Pouco claro	São realizadas pela Auditoria	Interna	Prestar aconselhamento aos responsaveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Auditoria / Gestão / Administração	Supervisor/Coordenador	Sim	Entidade Privada	Comércio e distribuição	Mais de 5000 trabalhadores	Mais de 10 Auditores	Presidente da Comissão Exec	Não	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo parcialmente	Encarregado Proteção de Da	Razoavelmente claro	São realizadas diretamente p	Concordo totalmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Auditoria / Gestão / Administração	Auditor	Sim	Entidade Pública	Outros serviços	Entre 501 e 2000 trabalhadores	Entre 2 a 5 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece aprofundadamente	Não	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Razoavelmente claro	São subcontratadas a uma ent	Concordo totalmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Direito	Diretor/Responsável	Sim	Entidade Pública	Transportes	Entre 2001 e 5000 trabalhadores	Entre 6 a 10 Auditores	Presidente do Conselho Adm	Não	Sim	Conhece razoavelmente;	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo parcialmente	Entidade Externa	Razoavelmente claro	São subcontratadas a uma ent	Concordo totalmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Contabilidade / Fiscalidade	nenhuma	Não	Entidade Privada	Comércio e distribuição	Entre 501 e 2000 trabalhadores	1 Auditor	Vogal do Conselho de Admin	Não	Não	Conhece aprofundadamente	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, totalmente preparada	Sim, entidade externa	Parcialmente preparada	Pouco relevante	Concordo totalmente	Entidade Externa	Nada claro	São subcontratadas a uma ent	Concordo totalmente	Prestar aconselhamento aos responsaveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Auditoria / Gestão / Administração	Auditor	Não	Entidade Privada	Serviços	Até 250 trabalhadores	Entre 2 a 5 Auditores	Comissão de Auditoria	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, integralmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Determinante	Concordo totalmente	EPD/ DPO e Auditoria Intern	Razoavelmente claro	São realizadas pela Auditoria	Interna	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Gestão Recursos Humanos	Auditor	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Muito bem preparada	Determinante	Concordo totalmente	Encarregado Proteção de Da	Totalmente claro	São realizadas pela Auditoria	Concordo totalmente	Confirmar que as auditorias ao RGPD são realizadas e controlar a conformidade com o RGPD
Auditoria / Gestão / Administração	Auditor Sénior	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Intern	Razoavelmente claro	São realizadas pela Auditoria	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria / Gestão / Administração	Auditor	Sim	Entidade Privada	Outros serviços	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admin	Sim	Sim	Conhece aprofundadamente	Sim	Prioridade moderada	Muito Madura	Sim, integralmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Intern	Totalmente claro	São realizadas pela Auditoria	Interna	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria / Gestão / Administração	Diretor/Responsável	Sim	Entidade Pública	Saúde	Entre 2001 e 5000 trabalhadores	1 Auditor	Presidente do Conselho Adm	Sim	Sim	Conhece aprofundadamente	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Não, totalmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Totalmente claro	São realizadas diretamente p	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados

APÊNDICE A – QUESTIONÁRO E RESPOSTAS (*GOOGLE FORMS*)

3. Qual a sua área de Formação?	4.Qual a sua função na estrutura da Auditoria Interna?	5.É membro do Instituto Português de Auditoria Interna (IPAI)?	6.Qual a natureza da sua organização?	7.Qual o setor de atividade da sua Organização?	8.Qual o número de trabalhadores da sua organização?	9.Qual o número de Auditores Internos na sua Organização?	10.A quem reporta, hierarquicamente a Auditoria Interna, na sua organização?	11.A Auditoria Interna na sua Organização, rege-se pelos Standards Internacionais do Institute of Internal Auditors (IIA)?	12.A sua Organização segue o Modelo das 3 Linhas de Defesa?	13.Em que medida considera que a sua Organização, conhece os termos e os princípios previstos no Regulamento Geral de Proteção de Dados (RGPD) e as suas implicações?	14.Foram efetuadas na sua Organização, ações de formação/ sensibilização sobre os princípios norteadores do Regime Geral de Proteção de Dados	15.Considera que a proteção de dados é uma prioridade na gestão de informação da sua Organização?	16.Em que estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD (incluindo a Lei 58/2019), considera que a sua Organização se encontra?	17.Considera que os atuais procedimentos vigentes na sua Organização, respondem aos requisitos do Regulamento Geral de Proteção de Dados (RGPD)?	18.Considera que a sua Organização se encontra tecnologicamente preparada para o cumprimento do Regulamento Geral de Proteção de Dados (RGPD)?	19.Na sua Organização existe um encarregado da proteção de dados (EPD)/ data protection officer (DPO) ou entidade externa, responsável pela proteção de dados?	20. Considera que na sua Organização, a Auditoria Interna está preparada para corresponder aos novos desafios trazidos pelo RGPD?	21.Considera que na sua Organização, a auditoria interna enquanto 3.ª linha de defesa, assume um papel relevante/determinante e para a criação de valor na operacionalização das	22.Concorda que as auditorias ao RGPD, quando realizadas pela Auditoria Interna enquanto 3.ª linha de defesa, constituem uma mais valia que se concretiza em ações de melhoria, ganhos efetivos de	23.Na sua Organização quem realiza o controlo da conformidade com o regulado/legislado no âmbito do RGPD (Compliance)?	24.Em que medida considera que, na sua Organização, está claro o papel do responsável pela proteção de dados (EPD/ DPO) ao que respeita às auditorias a realizar ao RGPD?	25.Na sua Organização, como são asseguradas pelo EPD/DPO as auditorias ao RGPD (quer periódicas quer não programadas) previstas na Lei 58/2019, Art.º 11º, alínea a)?	26.Caso as auditorias ao RGPD não sejam realizadas pela Auditoria Interna, em que medida concorda, que esta possa prestar apoio consultivo ao EPD/DPO ou Entidade Externa?	27. Considera que na sua Organização as responsabilidades do EPD/DPO, são essencialmente:
Auditoria / Gestão / Administração	Auditor	Não	Entidade Privada	Outros serviços	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Conselho Executivo	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, integralmente	Sim, razoavelmente	Sim EPD/DPO	Muito bem preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Totalmente claro	São realizadas diretamente p	Discordo parcialmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Auditoria / Gestão / Administração	Auditor Sénior	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admi	Sim	Sim	Conhece aprofundadamente	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Auditoria Interna	Razoavelmente claro	São realizadas pela Auditoria	Concordo totalmente	Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Auditoria / Gestão / Administração	Auditor	Não	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admi	Sim	Sim	Conhece razoavelmente;	Sim	Muito prioritário	Muito Madura	Sim, integralmente	Sim, totalmente preparada	Sim EPD/DPO	Muito bem preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Totalmente claro	São realizadas pela Auditoria	Interna	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Contabilidade / Fiscalidade	Diretor/Responsável	Sim	Entidade Privada	Alimentação e Bebidas	Entre 501 e 2000 trabalhadores	Entre 2 a 5 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece razoavelmente;	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Não, totalmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Razoavelmente claro	São realizadas pela Auditoria	Interna	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria / Gestão / Administração	Subdiretor/Manager	Sim	Entidade Privada	Comércio e distribuição	Entre 2001 e 5000 trabalhadores	1 Auditor	Country Business & Compli	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Interr	Totalmente claro	São realizadas diretamente pelo EPD/DPO		Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Economia/Finanças	Auditor Sénior	Sim	Entidade Pública	Outros serviços	Até 250 trabalhadores	Entre 6 a 10 Auditores	Presidente do Conselho Adm	Não	Não	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Parcialmente preparada	Pouco relevante	Concordo totalmente	Encarregado Proteção de Da	Pouco claro	Não são realizadas	Discordo parcialmente	Outra
Auditoria / Gestão / Administração	Auditor	Sim	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admi	Sim	Sim	Conhece aprofundadamente	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Totalmente claro	São realizadas pela Auditoria	Interna	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Direito	Auditor Sénior	Não	Entidade Pública	Outros serviços	Mais de 5000 trabalhadores	Mais de 10 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece razoavelmente;	Sim	Muito prioritário	Muito Madura	Sim, integralmente	Sim, razoavelmente	Sim EPD/DPO	Parcialmente preparada	Muito relevante	Concordo parcialmente	Auditoria Interna	Pouco claro	São realizadas pela Auditoria	Interna	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Auditoria / Gestão / Administração	Auditor	Sim	Entidade Privada	Banca, Seguros e Serviços fi	Entre 501 e 2000 trabalhadores	Mais de 10 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo parcialmente	Encarregado Proteção de Da	Razoavelmente claro	São realizadas diretamente p	Concordo totalmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Auditoria / Gestão / Administração	Auditor	Sim	Entidade Privada	Transportes	Mais de 5000 trabalhadores	Mais de 10 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece razoavelmente;	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Interr	Razoavelmente claro	São realizadas diretamente p	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria / Gestão / Administração	Supervisor/Coordenador	Não	Entidade Privada	Banca, Seguros e Serviços fi	Entre 501 e 2000 trabalhadores	Entre 6 a 10 Auditores	Comissão de Auditoria	Sim	Sim	Conhece aprofundadamente	Sim	Prioridade moderada	Razoavelmente Madura	Sim, integralmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo parcialmente	EPD/ DPO e Auditoria Interr	Razoavelmente claro	São realizadas pela Auditoria	Interna	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria / Gestão / Administração	Auditor	Sim	Entidade Privada	Comércio e distribuição	Mais de 5000 trabalhadores	Mais de 10 Auditores	Comissão de Auditoria	Sim	Sim	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Determinante	Concordo totalmente	EPD/ DPO e Auditoria Interr	Pouco claro	São realizadas pela Auditoria	Interna	Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Auditoria / Gestão / Administração	Auditor Sénior	Sim	Entidade Privada	Comércio e distribuição	Mais de 5000 trabalhadores	Mais de 10 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece superficialmente;	Sim	Prioridade moderada	Pouco Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Interr	Pouco claro	São realizadas diretamente p	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria / Gestão / Administração	Auditor	Sim	Entidade Privada	Outros serviços	Mais de 5000 trabalhadores	Mais de 10 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo parcialmente	Encarregado Proteção de Da	Pouco claro	São realizadas diretamente p	Discordo totalmente	Confirmar que as auditorias ao RGPD são realizadas e controlar a conformidade com o RGPD
Contabilidade / Fiscalidade	Supervisor/Coordenador	Sim	Entidade Privada	Telecomunicações e Média	Mais de 5000 trabalhadores	Mais de 10 Auditores	Comissão de Auditoria	Sim	Sim	Conhece razoavelmente;	Não	Muito prioritário	Pouco Madura	Sim, razoavelmente	Não, totalmente	Sim EPD/DPO	Parcialmente preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Pouco claro	Nunca existiram	Concordo totalmente	Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Auditoria / Gestão / Administração	Auditor	Não	Entidade Pública	Outros serviços	Até 250 trabalhadores	Mais de 10 Auditores	Presidente do Conselho Adm	Sim	Não	Conhece razoavelmente;	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo parcialmente	Encarregado Proteção de Da	Razoavelmente claro	São realizadas pela Auditoria	Interna	Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Economia/Finanças	Diretor/Responsável	Sim	Entidade Privada	Transportes	Mais de 5000 trabalhadores	Mais de 10 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, totalmente preparada	Sim EPD/DPO	Muito bem preparada	Muito relevante	Concordo totalmente	Legal	Razoavelmente claro	São realizadas pela Auditoria	Interna	Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Auditoria / Gestão / Administração	Diretor/Responsável	Sim	Entidade Privada	Outros serviços	Entre 2001 e 5000 trabalhadores	Entre 6 a 10 Auditores	Vogal do Conselho de Admi	Sim	Sim	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Não, totalmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Interr	Pouco claro	São subcontratadas a uma ent	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria / Gestão / Administração	Supervisor/Coordenador	Não	Entidade Pública	Outros serviços	Entre 2001 e 5000 trabalhadores	Entre 2 a 5 Auditores	Presidente da Câmara	Não	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, totalmente preparada	Sim, entidade externa	Razoavelmente preparada	Muito relevante	Concordo parcialmente	Encarregado Proteção de Da	Razoavelmente claro	São realizadas pela Auditoria	Interna	Confirmar que as auditorias ao RGPD são realizadas e controlar a conformidade com o RGPD
Economia/Finanças	Diretor/Responsável	Sim	Entidade Pública	Transportes	Entre 501 e 2000 trabalhadores	Entre 6 a 10 Auditores	Vogal do Conselho de Admi	Não	Sim	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Parcialmente preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Razoavelmente claro	São subcontratadas a uma ent	Concordo totalmente	Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Auditoria / Gestão / Administração	Auditor	Não	Entidade Pública	Outros serviços	Mais de 5000 trabalhadores	Entre 6 a 10 Auditores	Comissão de Auditoria	Não	Não	Não sabe/ Não responde	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Não	Parcialmente preparada	Pouco relevante	Concordo totalmente	Auditoria Interna	Pouco claro	São realizadas pela Auditoria	Interna	Outra
Auditoria / Gestão / Administração	Neste momento sou Manager	Não	Entidade Privada	Transportes	Entre 501 e 2000 trabalhadores	Entre 6 a 10 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Muito Madura	Sim, integralmente	Sim, totalmente preparada	Sim EPD/DPO	Muito bem preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Razoavelmente claro	Desconheço	Discordo parcialmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Economia/Finanças	Diretor/Responsável	Não	Entidade Pública	Utilities	Entre 2001 e 5000 trabalhadores	Entre 6 a 10 Auditores	Vogal do Conselho de Admi	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Muito Madura	Sim, integralmente	Sim, totalmente preparada	Sim, entidade externa	Razoavelmente preparada	Muito relevante	Concordo parcialmente	EPD/ DPO e Auditoria Interr	Razoavelmente claro	São realizadas pela Auditoria	Interna	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Auditoria / Gestão / Administração	Diretor/Responsável	Sim	Entidade Privada	Comércio e distribuição	Mais de 5000 trabalhadores	Mais de 10 Auditores	Presidente do Conselho Adm	Sim	Sim	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Interr	Razoavelmente claro	São realizadas diretamente p	Concordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria / Gestão / Administração	Diretor/Responsável	Sim	Entidade Privada	Indústria	Entre 251 e 500 trabalhadores	Entre 2 a 5 Auditores	Presidente do Conselho Adm	Não	Sim	Conhece razoavelmente;	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, entidade externa	Razoavelmente preparada	Razoavelmente preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Interr	Razoavelmente claro	São subcontratadas a uma ent	Concordo totalmente	Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
Direito	Auditor	Não	Entidade Privada	Outros serviços	Entre 251 e 500 trabalhadores	Mais de 10 Auditores	Vogal do Conselho de Admi	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Muito Madura	Sim, razoavelmente	Sim, totalmente preparada	Sim EPD/DPO	Razoavelmente preparada	Determinante	Concordo totalmente	EPD/ DPO e Auditoria Interr	Razoavelmente claro	São realizadas pela Auditoria	Interna	Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Auditoria / Gestão / Administração	Auditor Sénior	Sim	Entidade Privada	Indústria	Mais de 5000 trabalhadores	Entre 6 a 10 Auditores	Comissão de Auditoria	Sim	Sim	Não sabe/ Não responde	Não	Não sabe/ Não responde	Não sabe/ Não responde	Não sabe/ Não responde	Não	Não	Nada preparada	Determinante	Concordo totalmente	Não sei	Nada claro	Não sei	Concordo totalmente	Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Sistemas de Informação	Subdiretor/Manager	Não	Entidade Privada	Banca, Seguros e Serviços fi	Até 250 trabalhadores	1 Auditor	Presidente do Conselho Adm	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo parcialmente	EPD/ DPO e Auditoria Interr	Razoavelmente claro	São realizadas pela Auditoria	Interna	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria / Gestão / Administração	Auditor	Sim	Entidade Privada	Outros serviços	Entre 2001 e 5000 trabalhadores	Entre 6 a 10 Auditores	Vogal do Conselho de Admi	Sim	Não	Conhece razoavelmente;	Sim	Prioridade moderada	Razoavelmente Madura	Não sabe/ Não responde	Sim, razoavelmente	Não	Razoavelmente preparada	Determinante	Concordo parcialmente	Encarregado Proteção de Da	Razoavelmente claro	São realizadas diretamente p	Discordo parcialmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
Auditoria / Gestão / Administração	Supervisor/Coordenador	Sim	Entidade Privada	Alimentação e Bebidas	Mais de 5000 trabalhadores	Entre 2 a 5 Auditores	Vogal do Conselho de Admi	Sim	Sim	Conhece aprofundadamente	Sim	Muito prioritário	Muito Madura	Sim, integralmente	Sim, totalmente preparada	Sim EPD/DPO	Muito bem preparada	Muito relevante	Concordo totalmente	EPD/ DPO e Auditoria Interr	Totalmente claro	São realizadas diretamente p	Concordo totalmente	Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
Direito	Auditor Sénior	Não	Entidade Pública	Outros serviços	Entre 2001 e 5000 trabalhadores	Entre 2 a 5 Auditores	Vogal do Conselho de Admi	Sim	Não	Conhece aprofundadamente	Sim	Muito prioritário	Razoavelmente Madura	Sim, razoavelmente	Sim, razoavelmente	Sim EPD/DPO	Razoavelmente preparada	Muito relevante	Concordo totalmente	Encarregado Proteção de Da	Razoavelmente claro	Ainda não foi realizada	Discordo totalmente	Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados

APÊNDICE B

Questionário Versão Integral (*Google Forms*)

A P Ê N D I C E B – Q U E S T I O N Á R O – V E R S Ã O I N T E G R A L
(G O O G L E F O R M S)

O Papel da Auditoria Interna no Regime Geral de Proteção de Dados, enquanto 3.ªLinha de Defesa

Chamo-me Sandra Diogo, sou aluna do 2.º Ano do Mestrado em Auditoria, do Instituto Superior de Contabilidade e Administração de Lisboa (ISCAL) e encontro-me a desenvolver a Dissertação de Mestrado, sobre o tema em referência. O presente questionário enquadra-se na fase exploratória do processo de investigação científica e as seguintes questões têm como objetivo validar, à luz do Modelo das 3 linhas de Defesa, o papel da Auditoria Interna no âmbito do RGPD enquanto 3.ª linha de Defesa - por contraponto com as funções atribuídas ao encarregado pela proteção de dados, com responsabilidades ao nível do controlo da conformidade com o Regulamento e de assegurar a realização de auditorias neste âmbito. Gostaria de poder contar com a sua experiência para enriquecer esta investigação, o questionário que se segue demora, aproximadamente 5 minutos a responder. A resposta a estas questões será de extrema relevância para as conclusões sustentadas do estudo em apreço. Toda a informação recolhida é anónima e confidencial, destinando-se exclusivamente para análise estatística no âmbito da presente investigação. Agradeço desde já a sua participação. Sandra Alonso Diogo.

Parte I - Caracterização do respondente

1. Qual a sua idade?

- Inferior a 25 anos
- Entre 25 e 34 anos
- Entre 35 e 44 anos
- Entre 45 e 54 anos
- Entre 55 e 64 anos
- Superior a 64 anos

2. Indique há quantos anos exerce funções na Auditoria Interna:

- Menos de 2 anos
- Entre 2 e 5 anos
- Entre 6 e 10 anos
- Entre 11 e 15 anos
- Mais de 15 anos

3. Qual a sua área de Formação?

- Auditoria / Gestão / Administração
- Contabilidade / Fiscalidade
- Economia/Finanças
- Engenharia
- Direito
- Sistemas de Informação

4. Qual a sua função na estrutura da Auditoria Interna?

- Diretor/Responsável
- Subdiretor/Manager
- Supervisor/Coordenador
- Auditor Sénior
- Auditor
- Outra:

5. É membro do Instituto Português de Auditoria Interna(IPAI)?

- Sim
- Não

Parte II - Caracterização da Organização e da Função Auditoria Interna

6. Qual a natureza da sua organização?

- Entidade Pública
- Entidade Privada

7. Qual o setor de atividade da sua Organização?

- Alimentação e Bebidas
- Banca, Seguros e Serviços financeiros
- Comércio e distribuição
- Construção e produção de materiais de construção
- Indústria
- Petrolífero e Gás
- Saúde
- Serviços
- Telecomunicações e Média
- Transportes
- Utilities
- Outros serviços

8. Qual o número de trabalhadores da sua organização?

- Até 250 trabalhadores
- Entre 251 e 500 trabalhadores
- Entre 501 e 2000 trabalhadores
- Entre 2001 e 5000 trabalhadores
- Mais de 5000 trabalhadores

9. Qual o número de Auditores Internos na sua Organização?

- 1 Auditor
- Entre 2 a 5 Auditores
- Entre 6 a 10 Auditores
- Mais de 10 Auditores

10. A quem reporta, hierarquicamente a Auditoria Interna, na sua organização?

- Presidente do Conselho Administração / Diretor Geral
- Vogal do Conselho de Administração
- Comissão de Auditoria
- Conselho Fiscal
- Outra:

11. A Auditoria Interna na sua Organização, rege-se pelos *Standards Internacionais do Institute of Internal Auditors* (IIA)?

- Sim
- Não

12. A sua Organização segue o Modelo das 3 Linhas de Defesa?

- Sim
- Não

Parte III – O Regulamento Geral de Proteção de Dados (RGPD) na Organização

13. Em que medida considera que a sua Organização, conhece os termos e os princípios previstos no Regulamento Geral de Proteção de Dados (RGPD) e as suas implicações?

- Desconhece totalmente;
- Conhece superficialmente;
- Conhece razoavelmente;
- Conhece aprofundadamente
- Não sabe/ Não responde

14. Foram efetuadas na sua Organização, ações de formação/ sensibilização sobre os princípios norteadores do Regime Geral de Proteção de Dados (RGPD)?

- Sim
- Não

15. Considera que a proteção de dados é uma prioridade na gestão de informação da sua Organização?

- Nada prioritário
- Pouco prioritário
- Prioridade moderada
- Muito prioritário
- Não sabe/ Não responde

16. Em que estágio de maturidade em termos de compreensão da natureza e do impacto do RGPD (incluindo a Lei 58/2019), considera que a sua Organização se encontra?

- Nada Madura
- Pouco Madura
- Razoavelmente Madura
- Muito Madura
- Não sabe/ Não responde

17. Considera que os atuais procedimentos vigentes na sua Organização,respondem aos requisitos do Regulamento Geral de Proteção de Dados (RGPD)?

- Não
- Não, totalmente
- Sim, razoavelmente
- Sim, integralmente
- Não sabe/ Não responde

18. Considera que a sua Organização se encontra tecnologicamente preparada para o cumprimento do Regulamento Geral de Proteção de Dados (RGPD)?

- Não
- Não, totalmente
- Sim, razoavelmente
- Sim, totalmente preparada
- Não sabe/ Não responde

19. Na sua Organização existe um encarregado da proteção de dados (EPD)/Data Protection Officer (DPO) ou entidade externa, responsável pela proteção de dados?

- Sim EPD/DPO
- Sim, entidade externa
- Não

Parte IV – As Auditorias ao Regulamento Geral de Proteção de Dados (RGPD)

20. Considera que na sua Organização, a Auditoria Interna está preparada para corresponder aos novos desafios trazidos pelo RGPD?

- Nada preparada
- Parcialmente preparada
- Razoavelmente preparada
- Muito bem preparada

21. Considera que na sua Organização, a Auditoria Interna enquanto 3.ª linha de defesa, assume um papel relevante/determinante para a criação de valor na operacionalização das auditorias ao RGPD?

- Nada relevante
- Pouco relevante
- Muito relevante
- Determinante

22. Concorda que as auditorias ao RGPD, quando realizadas pela Auditoria Interna enquanto 3.ª linha de defesa, constituem uma mais valia que se concretiza em ações de melhoria, ganhos efetivos de eficiência e de confiança na organização?

- Discordo totalmente
- Concordo parcialmente
- Concordo totalmente

23. Na sua Organização quem realiza o controlo da conformidade com o regulado/legislado no âmbito do RGPD (Compliance)?

- Encarregado Proteção de Dados/Data Protection Officer (EPD/DPO)
- Auditoria Interna
- Entidade Externa
- EPD/ DPO e Auditoria Interna

24. Em que medida considera que, na sua Organização, está claro o papel do responsável pela proteção de dados (EPD/ DPO) no que respeita às auditorias a realizar ao RGPD?

- Nada claro
- Pouco claro
- Razoavelmente claro
- Totalmente claro

25. Na sua Organização, como são asseguradas pelo EPD/DPO as auditorias aoRGPD (quer periódicas quer não programadas) previstas na Lei 58/2019, Art.º 11º, alinea a)?

- São realizadas diretamente pelo EPD/DPO
- São realizadas pela Auditoria Interna
- São subcontratadas a uma entidade externa
- Outra

Nota: Caso tenha respondido na questão 25 que as auditorias ao RGPD são realizadas pela Auditoria Interna, pode avançar diretamente para a questão 27.

26. Caso as auditorias ao RGPD não sejam realizadas pela Auditoria Interna, emque medida concorda, que esta possa prestar apoio consultivo ao EPD/DPO ouEntidade Externa?

- Discordo totalmente
- Discordo parcialmente
- Concordo totalmente

27. Considera que na sua Organização as responsabilidades do EPD/DPO, são essencialmente:

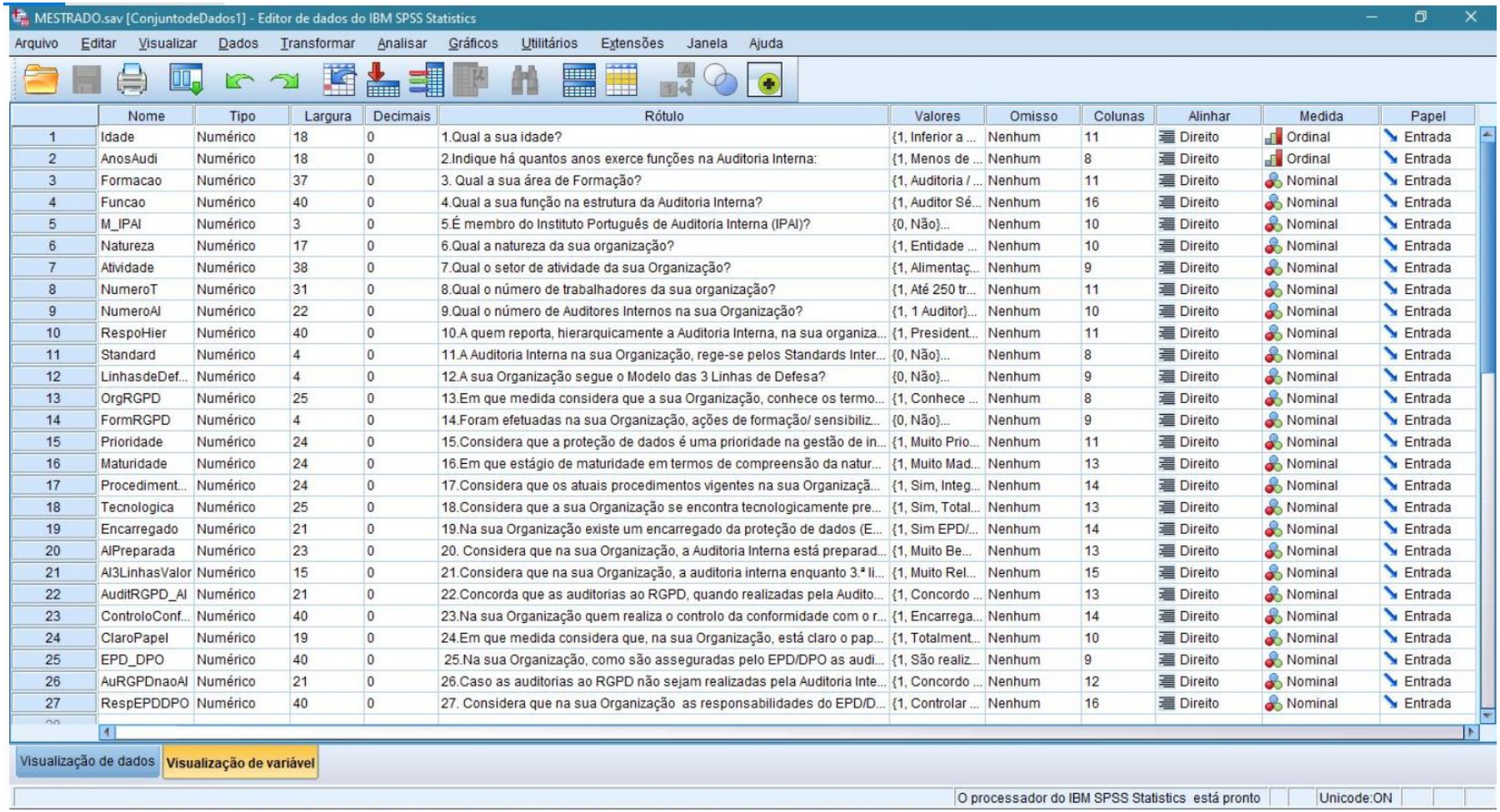
- Confirmar que as auditorias ao RGPD são realizadas e controlar a conformidade com o RGPD
- Sensibilizar/formar os trabalhadores em matéria de RGPD assim como aconselhar e controlar as avaliações de impacto sobre a proteção de dados
- Prestar aconselhamento aos responsáveis pelo tratamento de dados e cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados)
- Controlar a conformidade com o RGPD e realizar as auditorias correspondentes
- Outra

_____FIM_____

APÊNDICE C

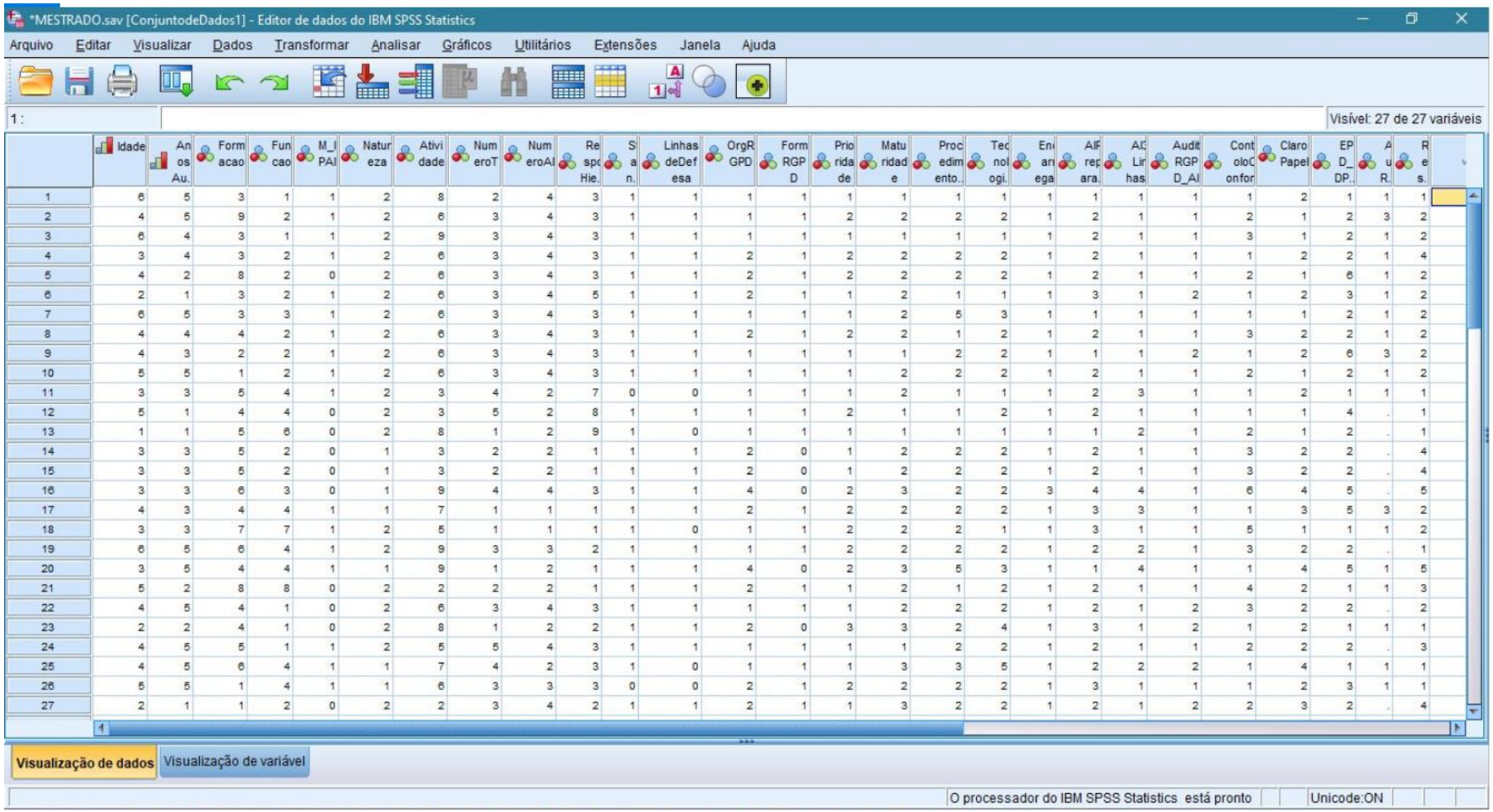
S*PSS* - Tratamento Estatístico Inferencial

APÊNDICE C – SPSS- TRATAMENTO ESTATÍSTICO INFERENCIAL

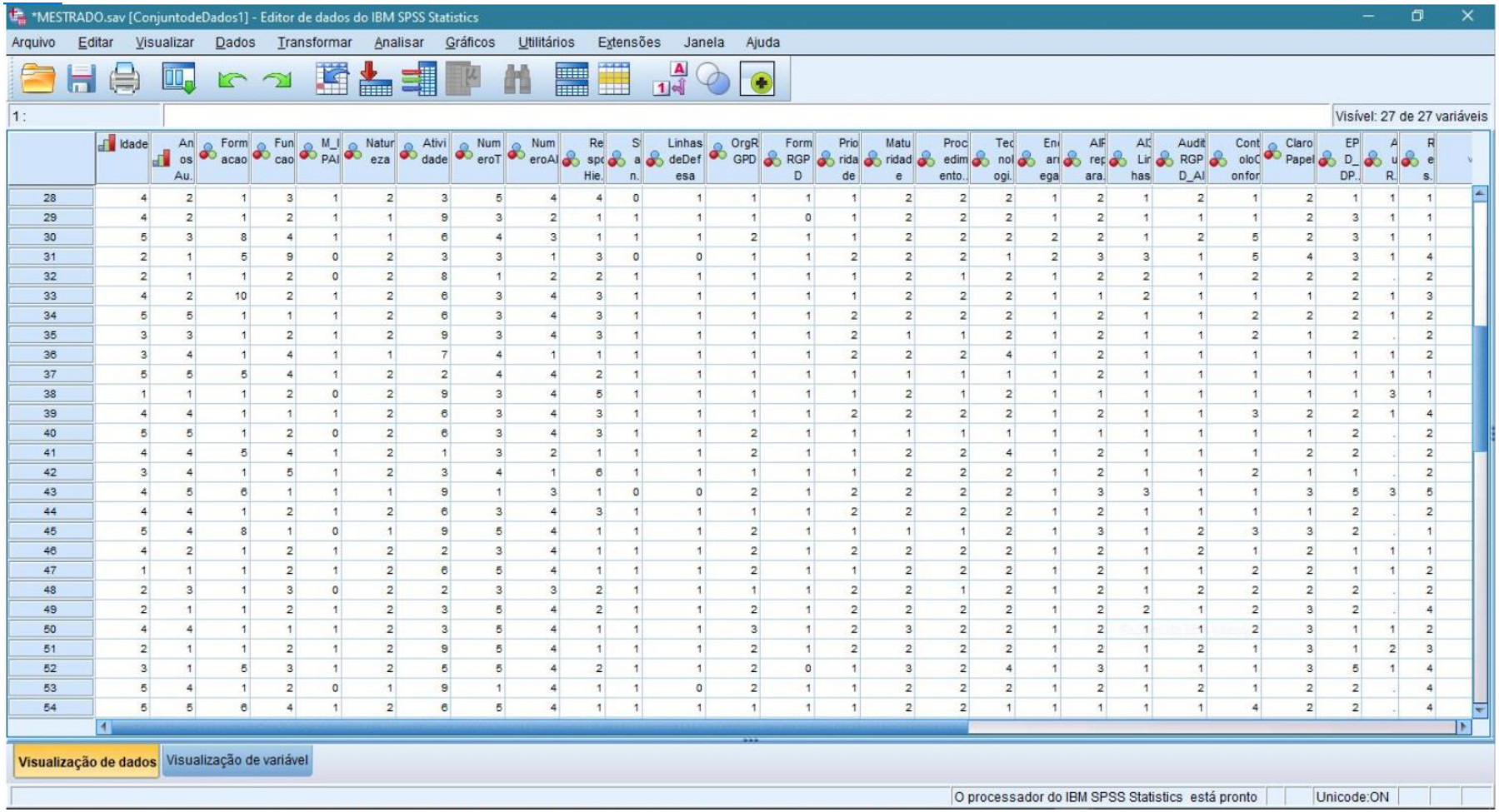


	Nome	Tipo	Largura	Decimais	Rótulo	Valores	Omisso	Colunas	Alinhar	Medida	Papel
1	Idade	Numérico	18	0	1.Qual a sua idade?	{1, Inferior a ...	Nenhum	11	Direito	Ordinal	Entrada
2	AnosAudi	Numérico	18	0	2.Indique há quantos anos exerce funções na Auditoria Interna:	{1, Menos de ...	Nenhum	8	Direito	Ordinal	Entrada
3	Formacao	Numérico	37	0	3. Qual a sua área de Formação?	{1, Auditoria / ...	Nenhum	11	Direito	Nominal	Entrada
4	Funcao	Numérico	40	0	4.Qual a sua função na estrutura da Auditoria Interna?	{1, Auditor Sé...	Nenhum	16	Direito	Nominal	Entrada
5	M_IPAI	Numérico	3	0	5.É membro do Instituto Português de Auditoria Interna (IPAI)?	{0, Não}...	Nenhum	10	Direito	Nominal	Entrada
6	Natureza	Numérico	17	0	6.Qual a natureza da sua organização?	{1, Entidade ...	Nenhum	10	Direito	Nominal	Entrada
7	Atividade	Numérico	38	0	7.Qual o setor de atividade da sua Organização?	{1, Alimentaç...	Nenhum	9	Direito	Nominal	Entrada
8	NumeroT	Numérico	31	0	8.Qual o número de trabalhadores da sua organização?	{1, Até 250 tr...	Nenhum	11	Direito	Nominal	Entrada
9	NumeroAI	Numérico	22	0	9.Qual o número de Auditores Internos na sua Organização?	{1, 1 Auditor}...	Nenhum	10	Direito	Nominal	Entrada
10	RespoHier	Numérico	40	0	10.A quem reporta, hierarquicamente a Auditoria Interna, na sua organiza...	{1, President...	Nenhum	11	Direito	Nominal	Entrada
11	Standard	Numérico	4	0	11.A Auditoria Interna na sua Organização, rege-se pelos Standards Inter...	{0, Não}...	Nenhum	8	Direito	Nominal	Entrada
12	LinhasdeDef...	Numérico	4	0	12.A sua Organização segue o Modelo das 3 Linhas de Defesa?	{0, Não}...	Nenhum	9	Direito	Nominal	Entrada
13	OrgRGPD	Numérico	25	0	13.Em que medida considera que a sua Organização, conhece os termo...	{1, Conhece ...	Nenhum	8	Direito	Nominal	Entrada
14	FormRGPD	Numérico	4	0	14.Foram efetuadas na sua Organização, ações de formação/ sensibiliz...	{0, Não}...	Nenhum	9	Direito	Nominal	Entrada
15	Prioridade	Numérico	24	0	15.Considera que a proteção de dados é uma prioridade na gestão de in...	{1, Muito Prio...	Nenhum	11	Direito	Nominal	Entrada
16	Maturidade	Numérico	24	0	16.Em que estágio de maturidade em termos de compreensão da natur...	{1, Muito Mad...	Nenhum	13	Direito	Nominal	Entrada
17	Procediment...	Numérico	24	0	17.Considera que os atuais procedimentos vigentes na sua Organizaçã...	{1, Sim, Integ...	Nenhum	14	Direito	Nominal	Entrada
18	Tecnologica	Numérico	25	0	18.Considera que a sua Organização se encontra tecnologicamente pre...	{1, Sim, Total...	Nenhum	13	Direito	Nominal	Entrada
19	Encarregado	Numérico	21	0	19.Na sua Organização existe um encarregado da proteção de dados (E...	{1, Sim EPD/...	Nenhum	14	Direito	Nominal	Entrada
20	AIPreparada	Numérico	23	0	20. Considera que na sua Organização, a Auditoria Interna está preparad...	{1, Muito Be...	Nenhum	13	Direito	Nominal	Entrada
21	AI3LinhasValor	Numérico	15	0	21.Considera que na sua Organização, a auditoria interna enquanto 3.ª li...	{1, Muito Rel...	Nenhum	15	Direito	Nominal	Entrada
22	AuditRGPD_AI	Numérico	21	0	22.Concorda que as auditorias ao RGPD, quando realizadas pela Audito...	{1, Concordo ...	Nenhum	13	Direito	Nominal	Entrada
23	ControloConf...	Numérico	40	0	23.Na sua Organização quem realiza o controlo da conformidade com o r...	{1, Encarrega...	Nenhum	14	Direito	Nominal	Entrada
24	ClaroPapel	Numérico	19	0	24.Em que medida considera que, na sua Organização, está claro o pap...	{1, Totalment...	Nenhum	10	Direito	Nominal	Entrada
25	EPD_DPO	Numérico	40	0	25.Na sua Organização, como são asseguradas pelo EPD/DPO as audi...	{1, São realiz...	Nenhum	9	Direito	Nominal	Entrada
26	AuRGPDnaoAI	Numérico	21	0	26.Caso as auditorias ao RGPD não sejam realizadas pela Auditoria Inte...	{1, Concordo ...	Nenhum	12	Direito	Nominal	Entrada
27	RespEPDDPO	Numérico	40	0	27. Considera que na sua Organização as responsabilidades do EPD/D...	{1, Controlar ...	Nenhum	16	Direito	Nominal	Entrada

APÊNDICE C – SPSS- TRATAMENTO ESTATÍSTICO INFERENCIAL



APÊNDICE C – SPSS- TRATAMENTO ESTATÍSTICO INFERENCIAL



APÊNDICE C – SPSS- TRATAMENTO ESTATÍSTICO INFERENCIAL