
Análise sobre a implementação e utilização de canais de denúncia
na AP

André Bernardo de Lemos Alves

Mestrado em Digitalização na Administração Pública

Orientadora:

Doutora Maria José Sousa, Professora Auxiliar (com Agregação)
ISCTE - Instituto Universitário de Lisboa

Setembro, 2024

Departamento de Ciência Política e Políticas Públicas

Análise sobre a implementação e utilização de canais de denúncia na AP

André Bernardo de Lemos Alves

Mestrado em Digitalização na Administração Pública

Orientador(a):

Doutora Maria José Sousa, Professora Auxiliar (com Agregação)
ISCTE - Instituto Universitário de Lisboa

Setembro, 2024

*À minha família,
Diana, José, Guilherme e Dinis*

Agradecimento

Este trabalho é resultado de um percurso de formação bastante enriquecedor e desafiante na área da Digitalização na Administração Pública, tendo sido desenvolvido no âmbito do Next GenerationEU - PRR.

Traduziu-se numa formação exigente em termos de tempo e disponibilidade, pelo que em primeiro lugar gostaria de agradecer o apoio incondicional da minha família que em todos os momentos, como sempre, me apoiou.

Em segundo lugar, gostaria de agradecer ao corpo docente, que deu contributos importantes ao longo das aulas e soube estimular o pensamento crítico e a capacidade de resolver problemas, cada vez mais complexos, que surgem na Administração Pública.

Por último, gostaria de deixar uma palavra de agradecimento a todos os colegas que me acompanharam nesta jornada e com os quais troquei várias ideias, quer no ISCTE, quer na AMA, sobre como podemos melhorar a atividade da Administração Pública, sobretudo através da tecnologia, com o objetivo de gerar valor para o cidadão e para a sociedade. A todos, o meu “obrigado”.

Resumo

Com o presente trabalho pretende-se analisar de que forma os organismos da Administração Pública (AP) em Portugal estão a implementar e operacionalizar os canais de denúncia, no âmbito da entrada em vigor do Regime Geral de Prevenção da Corrupção (RGPC) e do Regime Geral de Proteção de Denunciantes de Infrações (RGPDI).

Adicionalmente, pretende-se analisar o modo como os canais de denúncia estão a ser utilizados pelos cidadãos e de que forma o recurso a novas tecnologias, como a Inteligência Artificial (IA) e Interoperabilidade da Administração Pública (iAP), podem melhorar a qualidade dos atuais canais de denúncia no combate à fraude e corrupção.

Os cidadãos apresentam um nível médio de conhecimento positivo relativamente a IA e iAP, não existindo diferenças significativas entre estas variáveis. De modo análogo, estas tecnologias foram consideradas confiáveis e úteis para serem aplicadas aos canais de denúncia, o que constitui um importante ponto de partida para a implementação generalizada das mesmas num eventual canal de denúncias único na Administração Pública em Portugal.

Palavras-chave: Canais de denúncia, Inteligência Artificial, Interoperabilidade

Categorias e códigos de classificação (JEL):

D73 Bureaucracy • Administrative Processes in Public Organizations • Corruption

H83 Public Administration • Public Sector Accounting and Audits

Abstract

The present study aims to analyze how public administration entities in Portugal are implementing and operationalizing whistleblowing channels, in the context of introducing the General Regime for the Prevention of Corruption and the General Regime for the Protection of Whistleblowers.

Additionally, the study seeks to examine how citizens are utilizing these whistleblowing channels and how new technologies, such as Artificial Intelligence (AI) and interoperability (iAP), can improve the quality of the current whistleblowing channels in the fight against fraud and corruption.

The citizens present an average level of positive knowledge regarding AI and iAP, with no significant differences between these variables. Similarly, these technologies were considered reliable and useful for application to whistleblowing channels, constituting an important starting point for their widespread implementation in a single whistleblowing channel for the Public Administration in Portugal.

Keywords: Whistleblowing channels, Artificial Intelligence, Interoperability

Categories and classification codes (JEL):

D73 Bureaucracy • Administrative Processes in Public Organizations • Corruption

H83 Public Administration • Public Sector Accounting and Audits

Índice

Resumo.....	v
Abstract	vii
Índice de figuras	xi
Índice de quadros	xiii
CAPÍTULO 1. Introdução.....	1
1.1. A escolha do tema	2
1.1.1. Questões de investigação	4
1.1.2. Hipóteses de investigação	4
1.2. Objetivos de investigação.....	4
1.3. Políticas públicas aplicáveis	5
1.4. Legislação aplicável	7
CAPÍTULO 2. Revisão da Literatura.....	11
2.1. Corrupção	11
2.2. Canais de denúncia	13
2.3. Inteligência Artificial.....	17
2.4. Interoperabilidade.....	18
CAPÍTULO 3. Metodologia de investigação.....	21
3.1. Métodos e técnicas de investigação.....	22
CAPÍTULO 4. Técnicas de recolha de dados	23
4.1. Investigação quantitativa	23
4.1.1. Análise documental e de dados secundários	23
4.1.2. Análise de dados primários	25

CAPÍTULO 5. Análise de resultados	27
5.1. H1: As entidades da AP estão a implementar canais de denúncia de forma similar e correta.....	27
5.2. H2: Os cidadãos utilizam de forma limitada os canais de denúncia devido a falta de confiança e desconhecimento dos mesmos.	31
5.3. H3: A aplicação de IA e iAP em canais de denúncia é vista como útil na melhoria da sua eficiência.....	36
5.4. Síntese do resultado das hipóteses.....	40
CAPÍTULO 6. Conclusões.....	41
6.1. Conclusões.....	41
6.2. Recomendações	42
6.3. Oportunidades de investigação futura	42
Referências bibliográficas	43
Anexo 1	47
Anexo 2	49
Anexo 3	55
Anexo 4	67
Anexo 5	69

Índice de figuras

Figura 2.1 Programa de cumprimento normativo	13
Figura 3.1 Modelo de Análise	21
Figura 4.1 Whistleblowing em Portugal - eixos de abordagem. Fonte: Maia & Simões (2022)	23
Figura 4.2 Entidades abrangidas pelo RGPC	24
Figura 5.1 Valor total e n.º de contratos por entidade adjudicatária	29
Figura 5.2 Total gasto por CPV	30
Figura 5.3 Grau de conhecimento dos cidadãos sobre temas relacionados com a prevenção de corrupção	31
Figura 5.4 Alguma vez teve formação sobre prevenção da corrupção e infrações conexas? ..	32
Figura 5.5 Grau de conhecimento dos cidadãos sobre temas relacionados com a prevenção de corrupção	33
Figura 5.6 Avaliação da capacidade de distinção do que pode constituir uma denúncia	33
Figura 5.7 Grau de confiança relativamente aos canais de denúncia.....	34
Figura 5.8 Alguma vez apresentou uma denúncia?.....	35
Figura 5.9 Nível de conhecimento em IA e iAP	36
Figura 5.10 Nível de confiança em IA e iAP	37
Figura 5.11 Nível de utilidade sobre IA (reporte e tratamento), iAP e Canal de Denúncias único	38
Figura A3.1 Faixa etária dos inquiridos	55
Figura A3.2 Género dos inquiridos	55
Figura A3.3 Formação académica dos inquiridos	55
Figura A3.4 Região onde vive.....	56
Figura A3.5 Exerce funções de chefia ou de coordenação	56
Figura A3.6 Sector no qual trabalha.....	56
Figura A3.7 Área administrativa a que pertence a entidade em que trabalha	57
Figura A3.8 N.º de funcionários da entidade em que trabalha.....	58
Figura A3.9 Avaliação do grau de conhecimento sobre matérias relacionadas com prevenção da corrupção e denúncias	58
Figura A3.10 N.º de inquiridos com formação sobre prevenção da corrupção e infrações	59
Figura A3.11 Distribuição da formação sobre prevenção da corrupção e infrações conexas..	59
Figura A3.12 Avaliação de situações que podem ser objeto de denúncia	59

Figura A3.13 Grau de confiança relativamente aos canais de denúncia.....	60
Figura A3.14 N.º de inquiridos que já apresentaram uma denúncia	60
Figura A3.15 Distribuição das entidades sobre as quais incidiu a denúncia.....	60
Figura A3.16 Distribuição da nacionalidade das entidades sobre as quais incidiu a denúncia	61
Figura A3.17 Distribuição do tipo de irregularidade denunciada	61
Figura A3.18 Distribuição do modo de apresentação da denúncia	62
Figura A3.19 Cumprimento dos prazos relativamente à denúncia	62
Figura A3.20 Dificuldades durante o reporte da denúncia.....	62
Figura A3.21 Conseguiu ultrapassar a dificuldade sentida durante o reporte da denúncia.....	63
Figura A3.22 Sentimento relativamente a represálias após ter apresentado a denúncia.....	63
Figura A3.23 Confiança relativamente ao canal de denúncias utilizado	63
Figura A3.24 Grau de confiança relativamente ao desfecho da denúncia	64
Figura A3.25 Nível de conhecimento relativamente à IA.....	64
Figura A3.26 Nível de conhecimento relativamente à iAP.....	64
Figura A3.27 Nível de utilidade de IA para auxiliar o reporte da denúncia	65
Figura A3.28 Nível de utilidade de IA para auxiliar o tratamento da denúncia	65
Figura A3.29 Nível de utilidade de iAP para melhorar a transferência de dados entre entidades	65
Figura A3.30 Nível de confiança relativamente à utilização de um canal de denúncias com iAP.....	66
Figura A3.31 Nível de confiança relativamente à utilização de um canal de denúncias com IA	66
Figura A3.32 Nível de utilidade relativamente à utilização de um canal de denúncias único na AP com IA e iAP.....	66

Índice de quadros

Quadro 2.1 Síntese das abordagens e técnicas associadas à IA	17
Quadro 3.1 Questões de investigação, hipóteses, métodos e técnicas	22
Quadro 5.1 Distribuição dos contratos por âmbito	27
Quadro 5.2 Distribuição dos contratos de relacionados com a implementação de canal de denúncias	28
Quadro 5.3 Distribuição dos contratos de relacionados com a implementação de canal de denúncias por tipo de procedimento de contratação	28
Quadro 5.4 Entidades adjudicatárias com maior valor total de contratos	29
Quadro 5.5 Avaliação do grau de conhecimento em matérias relacionadas com a prevenção da corrupção	32
Quadro 5.6 Grau de confiança relativamente aos canais de denúncia	34
Quadro 5.7 Sentimento de proteção contra represálias e confiança.....	35
Quadro 5.8 Nível de conhecimento em IA e iAP.....	36
Quadro 5.9 Nível de confiança em IA e iAP.....	37
Quadro 5.11 Perceção de utilidade relativamente a IA e iAP	38
Quadro 5.12 Verificação das hipóteses	40
Quadro A2.1 Questionário utilizado	49
Quadro A4.1 Distribuição dos contratos por entidades adjudicatárias	67
Quadro A5.1 Preço contratual total por CPV.....	69

CAPÍTULO 1

Introdução

A fraude e a corrupção são problemas complexos, com múltiplas causas e requerem soluções integradas para os solucionar. Nos últimos tempos temos assistido a um esforço no sentido de criar mecanismos de prevenção da fraude e corrupção nas organizações públicas e privadas. Com a entrada em vigor do Regime Geral de Prevenção da Corrupção¹ (RGPC) em 2022, passou a ser obrigatório, para algumas entidades, a elaboração de planos de prevenção de riscos de corrupção e infrações conexas, códigos de conduta, programas de formação e a implementação de canais de denúncia. Relativamente aos canais de denúncias, o Regime Geral de Proteção Denunciante de Infrações² (RGPDI) dispõe que as entidades abrangidas por aquele regime devem disponibilizar canais de denúncias de infrações que assegurem a integridade, confidencialidade e anonimato das denúncias e dos denunciante (artigos 9.º e 13.º).

Os canais de denúncia constituem importantes ferramentas no combate à fraude e corrupção na medida em que funcionam como meio de comunicação de irregularidades de cada organização, que por sua vez devem ser tratadas de acordo com a sua especificidade e tendo em conta os direitos do denunciante, previstos no RGPDI. No entanto, estes canais funcionam também como porta de entrada para exposições de outras naturezas para além de denúncias, sendo frequentemente utilizados para fazer reclamações. Utilizações inadequadas dos canais de denúncias levam a gastos de tempo e de recursos nas fases de análise, tratamento e encaminhamento que seriam evitáveis se houvesse uma forma de orientar o possível denunciante no momento da formulação da sua exposição. Do ponto de vista das entidades, as tarefas de análise, tratamento e encaminhamento de denúncias, são atualmente feitas *ad hoc* para cada denúncia, sendo por isso muito exigentes em termos de recursos humanos e de tempo, e pouco automatizadas.

¹ Aprovado pelo Decreto-Lei n.º 109-E/2021, de 9 de dezembro

² Aprovado pela Lei n.º 93/2021, de 20 de dezembro, que transpôs a Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações de direito da União

Existem no mercado várias soluções de canais de denúncias para empresas e organismos da Administração Pública (AP), que dão resposta aos requisitos legais em vigor. Contudo não se tem conhecimento de que exista atualmente alguma solução em Portugal que incorpore Inteligência Artificial (IA) no sentido de, por um lado, ajudar o denunciante a formular melhor a denúncia, em português ou noutras línguas, e por outro lado, auxiliar a análise e tratamento das mesmas, por parte de cada organização. Adicionalmente, não se tem conhecimento de que existam canais de denúncia que utilizem a interoperabilidade de dados da Administração Pública (iAP).

O presente trabalho tem como objetivo analisar de que forma os organismos da AP em Portugal estão a implementar e a operacionalizar os canais de denúncia, no contexto da entrada em vigor do RGPC e do RGPDI. Pretende-se também analisar de que forma os canais de denúncia estão a ser usados pelos cidadãos e se o recurso a novas tecnologias, como a IA e a iAP, podem melhorar a qualidade dos canais de denúncia existentes, ao nível do registo, análise, tratamento e encaminhamento das denúncias.

1.1. A escolha do tema

A escolha deste tema teve por base o destaque que tem sido dado aos canais de denúncia como importantes ferramentas no combate à fraude e corrupção, principalmente a partir da entrada em vigor do RGPC e do RGPDI. Desde 18 de junho de 2022³ que as entidades abrangidas⁴ pelo RGPC, são obrigadas a disponibilizar canais de denúncia.

Segundo o n.º 3, do artigo 2.º, do Decreto-Lei n.º 109-E/2021, de 9 de dezembro, que cria o Mecanismo Nacional Anticorrupção (MENAC), aquele mecanismo tem, entre outras, as seguintes atribuições no âmbito do RGPC:

- b) Promover e controlar a implementação do RGPC;
- c) Apoiar entidades públicas na adoção e implementação dos programas de cumprimento normativo previstos no RGPC;
- d) Emitir orientações e diretivas a que devem obedecer a adoção e implementação dos programas de cumprimento normativo pelas entidades abrangidas pelo RGPC, devendo essas orientações e diretivas constar do sítio na Internet do MENAC, em local facilmente identificável e com ferramentas de pesquisa;

³ 180 dias após a publicação do RGPC

⁴ Nos termos do artigo 2º do RGPC

e) Planear o controlo e fiscalização do RGPC, articulando-se com as inspeções-gerais ou entidades equiparadas e inspeções regionais relativamente ao setor público;

f) Fiscalizar, em articulação com as inspeções-gerais ou entidades equiparadas e inspeções regionais, a execução do RGPC.

Não obstante o papel de apoio, controlo e fiscalização do RGPC por parte do MENAC, é da responsabilidade de cada entidade a escolha do canal de denúncias a implementar e a sua operacionalização. Relativamente à escolha do canal de denúncias, importa ter presente que o mesmo deve respeitar determinados requisitos ao nível da segurança do denunciante, os quais se encontram presentes nos artigos 9.º e 13.º do RGPDI, designadamente deve garantir a exaustividade, integridade e conservação da denúncia, a confidencialidade da identidade ou o anonimato dos denunciante e a confidencialidade da identidade de terceiros mencionados na denúncia, e de impedir o acesso de pessoas não autorizadas. Tendo em conta esses requisitos, algumas entidades desenvolveram soluções próprias, enquanto outras contrataram soluções no mercado, através de aquisição de plataformas ou de licenças de utilização. Ambas as opções implicam gastos ao nível de tempo e recursos para o desenvolvimento ou contratação destes canais. No presente, existe uma multiplicidade de canais de denúncia, que vai desde o *email*, a plataformas instaladas *on-premises* ou em *cloud*, que dão uma resposta nem sempre adequada aos requisitos legais impostos. Note-se, por exemplo, a criação de um *email* como canal de denúncias dificilmente garante a confidencialidade e o anonimato das denúncias e dos denunciante.

No que respeita à operacionalização dos canais de denúncia, podemos identificar dois tipos de problemas recorrentes: os que são associados à formulação das denúncias (ponto de vista do denunciante) e os que são associados à análise, tratamento e encaminhamento (ponto de vista das entidades).

Do ponto de vista do denunciante, verificam-se utilizações inadequadas dos canais de denúncias. Existem falhas ao nível do registo das denúncias no que respeita à sua completude e natureza, sendo frequente a utilização de canais de denúncias para reportar reclamações, sugestões, exposições, denúncias mal endereçadas, incompletas ou falsas. O *Whistleblowing* não deve ser tido como um sistema de gestão de reclamações indiscriminadas ou alarmistas, sob pena de perder o propósito que esteve na base da sua criação (Simões, 2019). Atualmente existe algum desconhecimento sobre o que se pode considerar denúncia ao abrigo do RGPDI, pelo que frequentemente dão entrada denúncias que na verdade não o são, o que dificulta a sua análise e tratamento.

Do ponto de vista das entidades, verifica-se que a manutenção dos canais de denúncia exige tempo e recursos, de forma a poder ser dada uma resposta adequada ao tratamento das denúncias recebidas.

Com base nos problemas identificados, apresentam-se as seguintes questões de investigação.

1.1.1. Questões de investigação

As questões de investigação abordadas neste trabalho são as seguintes:

Q1. De que forma os organismos da Administração Pública em Portugal estão a implementar e operacionalizar os canais de denúncia em conformidade com as novas exigências legais;

Q2. De que forma os canais de denúncia estão a ser utilizados pelos cidadãos;

Q3. De que forma o recurso a novas tecnologias, como a IA e iAP podem melhorar a qualidade dos atuais canais de denúncia.

1.1.2. Hipóteses de investigação

Atendendo às questões de investigação indicadas, apresentam-se as seguintes hipóteses de investigação:

H1. Hipótese sobre a implementação e operacionalização dos canais de denúncia: *As entidades da AP estão a implementar canais de denúncia de forma similar e correta.* Esta hipótese questiona o facto da implementação dos canais de denúncia na AP poder estar a ser efetuada de forma similar e correta entre todas as entidades abrangidas, de modo a ser possível alcançar sinergias e respeitar a conformidade legal.

H2. Hipótese sobre a utilização de canais de denúncia pelos cidadãos: *Os cidadãos utilizam de forma limitada os canais de denúncia devido a falta de confiança e desconhecimento dos mesmos.* Esta hipótese aborda a eficácia dos canais de denúncia em termos de acesso e confiança.

H3. Hipótese sobre o impacto das novas tecnologias: *A aplicação de IA e iAP em canais de denúncia é vista como útil na melhoria da sua eficiência.* Esta hipótese explora o potencial das novas tecnologias de forma a melhorar os processos existentes.

1.2. Objetivos de investigação

Os objetivos de investigação estão diretamente alinhados com a intenção de testar cada hipótese. Assim, podemos considerar os seguintes objetivos:

O objetivo geral consiste em analisar de que forma a AP está a implementar e operacionalizar os canais de denúncia e analisar como é que estes canais estão a ser utilizados pelos cidadãos, com vista a propor recomendações para o aumento da sua eficácia, através da implementação de tecnologias como a IA e iAP.

Este objetivo geral decompõe-se nos seguintes objetivos específicos:

OE1. Analisar a implementação e operacionalização dos canais de denúncia por parte das entidades da AP;

OE2. Analisar a utilização dos canais de denúncia pelos cidadãos, identificando os fatores que limitam ou facilitam essa utilização;

Este objetivo decompõe-se nos seguintes sub-objetivos:

OE2.1. Avaliar o nível de conhecimento dos cidadãos sobre a existência e funcionamento dos canais de denúncia;

OE2.2. Medir a confiança dos cidadãos nos atuais canais de denúncia;

OE3. Avaliar o impacto de novas tecnologias, como IA e iAP, na eficiência dos canais de denúncia.

Este objetivo decompõe-se nos seguintes sub-objetivos:

OE3.1. Analisar o nível de conhecimento dos cidadãos relativamente à IA e iAP

OE3.2. Analisar o nível de confiança da aplicação de IA e iAP aos canais de denúncia;

OE3.3. Analisar o nível de utilidade percecionada da aplicação de IA e iAP aos canais de denúncia.

1.3. Políticas públicas aplicáveis

Para analisar a implementação e utilização de canais de denúncia na AP existem algumas políticas públicas que importa considerar.

A **Agenda Anticorrupção**, elaborada pelo Governo em 2024, inclui medidas que se afiguram prementes e eficazes para a prevenção e combate de fenómenos corruptivos. Uma das medidas desta agenda consiste em operacionalizar um canal de denúncias, comum a todo o Governo, acessível através de um formulário disponibilizado no Portal do Governo, que assegura a integridade e a confidencialidade das denúncias. Outra medida desta agenda consiste em aprofundar o mecanismo de proteção para os denunciadores de corrupção e de cartéis na contratação pública.

A **Estratégia Nacional de Combate à Corrupção 2020-2024**, aprovada pela Resolução do Conselho de Ministros n.º 37/2021, de 6 de abril, é composta por um conjunto de medidas desenhadas para aumentar a transparência e responsabilidade das entidades públicas. Esta estratégia apresenta alguns pontos que se interligam com o tema deste trabalho designadamente, a intenção reduzir a burocracia, digitalizar as comunicações e informatizar os serviços prestados, facilitar o acesso e melhorar a qualidade da informação, assim como implementar canais de denúncia com uma adequada proteção dos denunciantes.

O **Plano de Recuperação e Resiliência (PRR)**⁵ tem um período de execução até 2026, contemplando um conjunto de reformas e de investimentos destinados a impulsionar o país no caminho da retoma, do crescimento económico sustentado e da convergência com a Europa ao longo da próxima década, tendo como orientação um conceito de sustentabilidade inspirado nos Objetivos de Desenvolvimento Sustentável (ODS) das Nações Unidas.

O PRR divide-se nas seguintes dimensões: Resiliência, Transição Climática e Transição Digital. No âmbito do desenvolvimento de um canal de denúncias único da AP, entende-se que o mesmo poderá ter enquadramento nas seguintes reformas da componente C19. Administração Pública - Digitalização, Interoperabilidade e Cibersegurança:

TD-r34 Serviços Públicos digitais, simples, inclusivos e seguros para os cidadãos e para as empresas

TD-r35 Reforma funcional e orgânica da Administração Pública

TD-r36 Administração Pública capacitada para a Criação de Valor Público

Por sua vez, tem correspondência nos investimentos:

TD-C19-i02 – Serviços Eletrónicos Sustentáveis

Com este investimento pretende-se simplificar a vida dos cidadãos e facilitar o ambiente de negócios, através da partilha de dados entre organismos da AP, de forma a reduzir redundâncias na prestação de informação. Este investimento visa também garantir a interoperabilidade com o Portal Digital Único Europeu, segundo o Regulamento SDG⁶.

TD-C19-i07 - Capacitação da Administração Pública

Com este investimento pretende-se desenvolver a capacidade organizacional em todos os organismos da AP, através de recursos humanos formados, designadamente ao nível da gestão e das tecnologias, para se tirar efetivamente partido das transformações em curso, em particular no digital, com vista a prestar um melhor serviço público.

⁵ <https://recuperarportugal.gov.pt/plano-de-recuperacao-e-resiliencia/>, consultado em 26/1/2024

⁶ Single Digital Gateway - Regulamento (UE) 2018/1724 do Parlamento Europeu e do Conselho, de 2 de outubro de 2018, relativo à criação de uma plataforma digital única para a prestação de acesso a informações, a procedimentos e a serviços de assistência e de resolução de problemas, e que altera o Regulamento (UE) n.º 1024/2012

A Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023, aprovada pela Resolução do Conselho de Ministros n.º 55/2020, de 31 de julho, promove a transformação digital e a simplificação administrativa dentro da Administração Pública. Apresenta 4 eixos, sendo um deles “explorar a tecnologia”, que por sua vez, se decompõe em três objetivos estratégicos: “i) reforçar a governação global das tecnologias; ii) melhorar a interoperabilidade e a integração de serviços, e iii) gerir o ecossistema de dados com segurança e transparência”.

O **Plano Global Estratégico para a Racionalização e Redução de Custos com as Tecnologias de Informação e de Comunicação, na Administração Pública (PGETIC)**, aprovado pela Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro, tem como objetivo de, através do uso ponderado e racionalizado das TIC, melhorar a eficiência dos processos internos da AP, assim como a qualidade dos serviços prestados ao cidadão e às empresas. O plano é composto por 25 medidas, organizadas em 5 eixos estratégicos de ação, sendo que dois dos eixos são a “redução de custos” e a “implementação de soluções TIC comuns”.

1.4. Legislação aplicável

A implementação de canais de denúncia em Portugal tem enquadramento na legislação que de seguida se apresenta.

O **Regime Geral de Prevenção da Corrupção (RGPC)**, estabelecido pelo Decreto-Lei n.º 109-E/2021, de 9 de dezembro, surge na sequência da aprovação da Estratégia Nacional de Combate à Corrupção, com o intuito de implementar as prioridades nela estabelecidas, melhorar as práticas institucionais em matéria de transparência, prevenir e detetar os riscos de corrupção na ação pública e comprometer o setor privado com a prevenção e repressão da corrupção. Este regime determina também a implementação de sistemas de controlo interno que assegurem a efetividade dos instrumentos integrantes do programa de cumprimento normativo, bem como a transparência e imparcialidade dos procedimentos e decisões, prevendo igualmente um regime sancionatório próprio.

As entidades abrangidas⁷ pelo RGPC adotam e implementam um programa de cumprimento normativo⁸ que inclui pelo menos um plano de prevenção de riscos de corrupção e infrações conexas (PPR), um código de conduta, um programa de formação e um canal de denúncias, a fim de prevenirem, detetarem e sancionarem atos de corrupção e infrações conexas, levados a cabo contra ou através da entidade. Adicionalmente, as entidades abrangidas

⁷ Artigo 2.º do RGPC

⁸ Artigo 5.º do RGPC

designam, como elemento da direção superior ou equiparado, um responsável pelo cumprimento normativo, que garante e controla a aplicação do programa de cumprimento normativo.

No que respeita aos canais de denúncia, o artigo 8.º do RGPC indica que as entidades abrangidas dispõem de canais de denúncia interna e dão seguimento a denúncias de atos de corrupção e infrações conexas nos termos do disposto na legislação que transpõe a Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União (RGPDI).

O **Regime Geral de Proteção de Denunciantes de Infrações (RGPDI)**, aprovado pela Lei n.º 93/2021, de 20 de dezembro, aplica-se a Entidades com 50 ou mais trabalhadores e Pessoas coletivas que desenvolvam a sua atividade nos domínios dos serviços, produtos e mercados financeiros e prevenção do branqueamento de capitais e do financiamento do terrorismo⁹.

Ao abrigo do RGPDI podem ser apresentadas denúncias relacionadas com (i) criminalidade violenta, (ii) especialmente violenta, (iii) altamente organizada, (iv) criminalidade económico-financeira e ainda com (v) violações do direito da União Europeia relativamente às seguintes matérias: Contratação pública; Serviços, produtos e mercados financeiros e prevenção do branqueamento de capitais e do financiamento do terrorismo; Segurança e conformidade dos produtos; Segurança dos transportes; Proteção do ambiente; Proteção contra radiações e segurança nuclear; Segurança dos alimentos para consumo humano e animal, saúde animal e bem-estar animal; Saúde pública; Defesa do consumidor; Proteção da privacidade e dos dados pessoais e segurança da rede e dos sistemas de informação.

De acordo com o artigo 5.º do RGPDI, poderá ser denunciante quem, (i) estando de boa-fé (ou seja, convencido da veracidade dos factos ao momento da denúncia), (ii) tiver conhecimento da infração no âmbito da sua atividade profissional (não se restringindo, desta forma, esta qualificação apenas a trabalhadores). A proteção conferida pelo regime é estendida a terceiros que auxiliem ou estejam ligados ao denunciante.

No âmbito deste regime, as denúncias podem ser feitas por escrito, verbalmente ou de ambas as formas, sendo que os denunciantes gozam dos seguintes direitos:

- Direito à confidencialidade da sua identidade, bem como das informações que, direta ou indiretamente, permitam deduzi-la;
- Direito a proteção jurídica nos termos gerais;

⁹ Artigo 8.º do RGPDI

- Direito a beneficiar de medidas de proteção de testemunhas em processo penal;
- Proibição de atos de retaliação (o Regime prevê uma lista exemplificativa de atos que se presumem ser de retaliação quando praticados nos 2 anos seguintes à denúncia ou divulgação pública).

O **Regulamento Geral sobre a Proteção de Dados (RGPD)**, Regulamento (EU) n.º 679/2016, de 27 de abril, visa proteger os dados pessoais, neste caso em específico, tem como objetivo garantir a confidencialidade e segurança dos dados denunciantes de infrações, e que a informação reportada seja utilizada exclusivamente para os fins adequados.

Revisão da Literatura

No presente capítulo é apresentada uma revisão da literatura sobre os principais temas abordados neste trabalho: corrupção, canais de denúncia, inteligência artificial e interoperabilidade. A existência de corrupção motiva a criação de canais de denúncia, onde possam ser reportadas irregularidades de forma segura e eficaz para o denunciante. A inteligência artificial e a interoperabilidade, por sua vez, afiguram-se como tecnologias de elevada utilidade quando integradas nestes canais, permitindo otimizar os processos de reporte e tratamento de denúncias a vários níveis.

2.1. Corrupção

De um modo geral é possível afirmar que a necessidade de implementação de canais de denúncia é motivada pela existência irregularidades nas organizações, que por vezes podem estar relacionadas com atos de corrupção. A corrupção é um problema complexo e os interessados na sua resolução têm geralmente diferentes perspetivas e objetivos, o que pode dificultar a existência de consenso relativamente às melhores soluções a adotar para o combater. Por conseguinte, a abordagem para lidar com a corrupção deve ser adaptativa e integrada. A implementação de medidas de prevenção deve ser orientada por princípios éticos e acompanhada por um esforço contínuo de monitorização e avaliação para identificar e corrigir as falhas, bem como melhorar os resultados.

A Estratégia Nacional Anticorrupção 2020-2024 indica que não existe uma definição de corrupção comum a todos os países, no entanto é consensual que numa conduta corruptiva se verifica o abuso de um poder ou função públicos de forma a beneficiar um terceiro, contra o pagamento de uma quantia ou outro tipo de vantagem. Na esfera jurídica nacional encontram-se previstos nos artigos 372º a 374 do Código Penal Português os crimes de recebimento indevido de vantagem e os crimes de corrupção. Os crimes de corrupção dividem-se em corrupção ativa ou passiva, conforme o agente esteja respetivamente a oferecer/prometer ou a solicitar/aceitar uma vantagem patrimonial indevida, distinguindo-se ainda, cada uma, conforme o ato solicitado ou a praticar seja ou não contrário aos deveres do cargo do funcionário corrompido.

Na sociedade, o conceito de corrupção alcança um sentido mais abrangente, abarcando outras condutas, também criminalizadas, cometidas no exercício de funções públicas, como o peculato, a participação económica em negócio, a concussão, o abuso de poder, a prevaricação, o tráfico de influência ou o branqueamento.

A nível global, a organização governamental Transparência Internacional define a corrupção como o abuso de um poder confiado para obtenção de benefícios privados. A corrupção pode ser classificada por dimensão (grande, pequena ou política), dependendo do volume de dinheiro perdido e do sector em que ocorre (Transparência e Integridade - Transparency International Portugal, 2019)

A União Europeia publicou o Eurobarómetro sobre “Atitudes dos cidadãos em relação à corrupção na UE em 2024”(Citizens Attitudes towards Corruption in the EU in 2024, 2024)¹⁰. A principal conclusão obtida é que os cidadãos europeus consideram a corrupção inaceitável e duvidam dos esforços dos governos nacionais no seu combate. Da amostra considerada, 65% dos cidadãos consideram que os casos de corrupção de alto nível não são suficientemente investigados e apenas 30 % consideram que os esforços dos governos para combater a corrupção são eficazes. Cerca de 68 % dos cidadãos europeus consideram que a corrupção é generalizada no seu país.

No caso de Portugal a percentagem dos cidadãos portugueses que consideram a corrupção como “comum” subiu para 96%, em comparação com 93% no inquérito realizado em 2023. No entanto, 99% dos inquiridos afirmam não ter sido vítimas nem testemunhado qualquer caso de corrupção no último ano, contra uma média europeia de 94%. Além disso, 93% dos portugueses dizem não conhecer pessoalmente alguém que tenha oferecido ou recebido suborno, em contraste com a média de 88% na União Europeia.

A preocupação com a corrupção é antiga, contudo a partir dos anos 90 começam a surgir estudos mais estruturados sobre este fenómeno.

Mauro (1995) analisa um conjunto de dados tais como índices de corrupção, burocracia, eficiência do sistema judicial e várias categorias de estabilidade política para um conjunto transversal de países, tendo verificado que a corrupção diminui o investimento, reduzindo assim o crescimento económico.

Bardhan (1997) elenca algumas vertentes da corrupção e as suas consequências para os países, especialmente países em desenvolvimento, concluindo que a corrupção tem efeitos negativos na eficiência, investimento e crescimento.

¹⁰ Disponível em <https://europa.eu/eurobarometer/surveys/detail/3217>, consultado a 19/9/2024

Tanzi (1998) apresenta uma revisão de literatura sobre o tema da corrupção, indicando causas, consequências, âmbito em que os casos de corrupção acontecem e possíveis ações corretivas. Neste estudo são também apresentados alguns custos inerentes à corrupção em termos de crescimento económico para os países.

Zheng & Liao (2019) concluem que a eficácia do Estado na investigação da corrupção é crucial para manter um sistema estável, onde a corrupção é minimizada. Quando é possível realizar investigações bem-sucedidas, os funcionários são desencorajados a aceitar subornos e a necessidade de apresentar denúncias diminui.

O estudo *Report to the Nations* (ACFE, 2024) indica que a forma mais eficaz para detetar a fraude ocupacional é a “Denúncia”, tendo alcançado 43% dos casos registados. A fraude ocupacional é uma infração conexas à corrupção, que se traduz numa ação ilícita, na qual um indivíduo tira partido da função ou cargo que desempenha para obter vantagens indevidas e enriquecimento pessoal.

Atualmente é possível afirmar que a corrupção é uma área de estudo interdisciplinar que envolve economia, ciência política, sociologia e direito, com consequências negativas a vários níveis, sendo por isso de extrema importância a sua análise e compreensão no sentido da prevenção de futuros casos.

2.2. Canais de denúncia

A identificação de situações de corrupção e o correto reporte das mesmas é uma tarefa que nem sempre se afigura fácil. A criação de canais de denúncia veio permitir uma melhor comunicação de irregularidades, sendo por isso uma ferramenta importante no combate à corrupção.

O RGPC, estabelece no n.º 1 do artigo 5º a obrigatoriedade de as entidades abrangidas adotarem e implementarem um programa de cumprimento normativo que inclua, pelo menos, um plano de prevenção de riscos de corrupção e infrações conexas (PPR), um código de conduta, um programa de formação e um canal de denúncias, a fim de prevenirem, detetarem e sancionarem atos de corrupção e infrações conexas, levados a cabo contra ou através da entidade.

Programa de cumprimento normativo			
Plano de prevenção de riscos de corrupção e infrações conexas	Código de ética e de conduta	Programa de formação	Canal de denúncia

Figura 2.1 Programa de cumprimento normativo

O canal de denúncias a adotar por cada entidade deve respeitar o estabelecido no RGPDI. Nos artigos 9.º e 13.º são apresentadas características que os canais de denúncias devem apresentar, designadamente devem assegurar a exaustividade, a integridade, a confidencialidade da identidade ou o anonimato dos denunciantes e a confidencialidade da identidade de terceiros mencionados na denúncia, e impedir o acesso de pessoas não autorizadas.

Em função das especificidades de cada organização, pode ser necessário implementar um canal de denúncias interno (artigo 8.º do RGPDI) e um canal de denúncias externo (artigo 12.º do RGPDI), contudo ambos os canais podem ser semelhantes em termos de campos de registo da denúncia. De acordo com o n.º 2 do artigo 9.º, os canais denúncia interna são operados internamente, para efeitos de receção e seguimento de denúncias, por pessoas ou serviços designados para o efeito, devendo ser garantida a independência, a imparcialidade, a confidencialidade, a proteção de dados, o sigilo e a ausência de conflitos de interesses no desempenho das funções. No caso dos canais de denúncias externos, segundo o n.º 2 do artigo 13.º, as entidades competentes designam funcionários responsáveis pelo tratamento de denúncias, que inclui:

- a) Prestar a todas as pessoas interessadas informações sobre os procedimentos de denúncia, garantindo a confidencialidade do aconselhamento e da identidade das pessoas;
- b) Receber e dar seguimento às denúncias;
- c) Prestar informações fundamentadas ao denunciante sobre as medidas previstas ou adotadas para dar seguimento à denúncia e solicitar informações adicionais, se necessário.

Em termos de forma e admissibilidade, os canais de denúncia interna permitem a apresentação de denúncias, por escrito ou verbalmente, por trabalhadores, anónimas ou com identificação do denunciante (n.º 1 do artigo 10.º). A denúncia pode ser apresentada com recurso a meios de autenticação eletrónica com cartão de cidadão ou chave móvel digital, ou com recurso a outros meios de identificação eletrónica emitidos em outros Estados-Membros e reconhecidos para o efeito nos termos do artigo 6.º do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, desde que, em qualquer caso, os meios estejam disponíveis (n.º 3 do artigo 10.º). No que respeita às denúncias externas, a forma e admissibilidade das denúncias é semelhante, contudo não se encontra prevista a autenticação eletrónica (artigo 14.º) para este caso.

Cada organização deverá escolher o canal de denúncias a implementar e designar funcionários para desempenhar as funções anteriormente referidas. Atualmente existem várias soluções no mercado que oferecem canais de denúncias em conformidade com os requisitos legais em vigor. Contudo, não existem evidências da existência de alguma solução em Portugal que incorpore IA na análise e tratamento de denúncias, assim como possibilite a interoperabilidade dos dados entre entidades (iAP).

Na literatura encontramos algumas referências à importância dos canais de denúncia nas organizações e ao desenvolvimento tecnológico que lhes está associado.

Silva & Sousa (2017) apresentam uma análise sobre a influência dos canais de denúncia na decisão de reportar irregularidades financeiras. Os autores concluíram que a presença de um canal de denúncias anónimo aumenta a intenção dos colaboradores com vínculo efetivo em relatar uma irregularidade financeira.

Bazart et al. (2019) investigam a eficiência relativa de auditorias baseadas em denúncias e auditorias aleatórias, concluindo que auditorias baseadas em denúncias são mais eficientes e apresentam um efeito dissuasor mais forte, incentivando maiores níveis de conformidade.

Noor & Mansor (2019) analisam a implementação de canais de denúncia no setor público da Malásia, com recurso a inteligência artificial. Os resultados do estudo indicam que a existência de canais de denúncia reforça o sistema de controlo interno e aumenta a transparência e *accountability* do sector público.

Gao (2020) destaca a utilização da inteligência artificial nos canais de denúncia e compara vários meios de entrada, tais como o online e o telefone. Os resultados obtidos indicam que os canais de denúncia telefónicos apresentaram maior intenção de denúncias quando existe um operador, uma vez que traduzem maior confiança. No entanto, os denunciadores são mais propícios a denunciar em plataformas online que contenham agentes virtuais para gerir as denúncias, pois sentem maior eficiência e controlo no reporte.

Zouvia et al. (2020) identificam as potencialidades da IA aplicada aos canais de denúncia, ao nível do reporte através de assistentes virtuais, tradução ao vivo, verificação mais eficiente das evidências e monitorização proativa.

Putra et al. (2022) abordam, entre várias questões, de que forma a existência de canais de denúncias e o *big data* influenciam a prevenção da fraude e de que forma a prevenção de fraudes está interligada com as áreas de auditoria interna, gestão de risco, canais de denúncia e análise de dados para prevenir comportamentos criminosos.

Previtali & Cerchiello (2022) analisam fatores organizacionais que influenciam o comportamento de denúncia, como a implementação de procedimentos de denúncia e programas de formação anticorrupção. Os autores sugerem que, para além das leis anticorrupção, é fundamental que haja uma mudança cultural nas organizações, apoiada por formação e procedimentos que protejam os denunciantes, de modo a preservar a integridade organizacional.

Mrowiec (2022) apresenta uma revisão de literatura sobre os fatores que influenciam o reporte de denúncias internas nas empresas, sendo que esses fatores podem-se agrupar em áreas específicas, tais como ética, liderança, políticas e procedimentos, clima social, justiça organizacional, formação, canais de denúncia, dimensão e estrutura da organização, entre outras.

Kagias et al. (2023) apresentam um modelo de maturidade para práticas de *whistleblowing*, que pode ser usado para fortalecer os sistemas de denúncia das organizações, de modo a proporcionar um ambiente de controlo mais robusto. O modelo permite também efetuar um *benchmarking* interno e externo para ajudar as organizações a medir o seu progresso em relação à conformidade e à eficácia dos seus canais de denúncia.

Kang (2023) apresenta uma revisão de literatura sobre as denúncias no sector público, sendo o seu principal objetivo analisar definições, teorias, métodos de pesquisa e fatores relacionados com a intenção e comportamento de denuncia irregularidades. O estudo conclui que denunciar irregularidades é uma prática importante para a transparência e eficiência administrativa.

Teodocio & Morales (2024) analisam como o medo e a raiva influenciam a propensão de funcionários públicos a denunciarem atos de corrupção, tendo concluído que emoções como a raiva podem aumentar a probabilidade de um funcionário público agir contra irregularidades, enquanto o medo tendo a impedir a denúncia.

Bloch-Wehba et al. (2024) abordam a crescente influência dos denunciantes no sector da tecnologia e os desafios legais e práticos que enfrentam. Concluem que o sistema legal atual é insuficiente para proteger plenamente os denunciantes, defendendo uma reforma significativa no regime de proteção legal dos mesmos.

Kagias et al. (2024) analisam a aplicação do modelo das três linhas de defesa, utilizado na auditoria interna e gestão de risco, na gestão de denúncias dentro das organizações. O estudo sugere que a aplicação deste modelo pode fortalecer a governança e a transparência organizacional, recomendando que as organizações implementem práticas claras e robustas de denúncia, com papéis e responsabilidades bem definidos, para garantir a eficácia das investigações e promover uma cultura de integridade.

Em suma, é possível afirmar que o desenvolvimento tecnológico associado aos canais de denúncia inclui a utilização da IA para melhorar esses sistemas. Na secção seguinte apresenta-se uma breve revisão de literatura sobre IA.

2.3. Inteligência Artificial

A Inteligência Artificial consiste na capacidade de programas de computador executarem tarefas que normalmente exigem inteligência humana. Em vez de serem explicitamente programados para realizar uma tarefa específica, esses programas são treinados para aprender e aperfeiçoar o seu desempenho ao longo do tempo. A IA reúne ciências, teorias e técnicas (lógica matemática, estatística, probabilidade, neurobiologia computacional e ciência da computação) para conseguir a mimetização das capacidades cognitivas de um humano por uma máquina (AMA, 2022).

A IA abrange uma variedade de abordagens e técnicas das quais se destacam a *Machine Learning*, Redes Neurais, Processamento de Linguagem Natural, Visão Computacional e Sistemas de Recomendação.

Quadro 2.1 Síntese das abordagens e técnicas associadas à IA

<i>Machine Learning</i>	Segundo esta abordagem os algoritmos são projetados para aprender padrões a partir de dados. A aprendizagem pode ser supervisionada, não supervisionada ou por reforço.
Redes Neurais	Estas redes são capazes de aprender representações complexas dos dados e identificar correlações e padrões específicos. Podem ser utilizadas para analisar transações, comportamentos do utilizador, padrões de uso de cartão de crédito, entre outros.
Processamento de Linguagem Natural (PLN)	O PLN pode ser utilizado para analisar textos, como registos de chamadas, descrições de transações ou mensagens de e-mail. Algoritmos de PLN podem ajudar a identificar palavras-chave, padrões linguísticos ou sentimentos suspeitos.
Visão Computacional	A Visão Computacional concentra-se no desenvolvimento de sistemas que podem interpretar, entender e extrair informações visuais de dados do mundo real. Esses dados podem ser imagens, vídeos ou sequências temporais de quadros.
Sistemas de recomendação	Os sistemas de recomendação em IA visam prever e sugerir itens ou conteúdos que podem ter interesse para um utilizador específico. Utilizam algoritmos para analisar padrões de comportamento do utilizador, preferências e interações do passado para fazer recomendações personalizadas.

Em termos de IA, os benefícios previstos da aplicação desta tecnologia aos canais de denúncia encontram-se alinhados com os exemplos de utilização prática da IA no setor da Gestão Administrativa, designadamente: “Disponibilização de interfaces de conversação automatizadas com funcionários virtuais para automatizar cenários de atendimento ao cidadão e às empresas; Reforço da segurança e privacidade nos sistemas informáticos” (AMA, 2022). Adicionalmente, Noor & Mansor (2019) identificam que a utilização de IA nos canais de denúncia melhora a resposta a práticas de corrupção, propondo a sua aplicação em todas as entidades do setor público.

2.4. Interoperabilidade

A iAP visa proporcionar um método fácil e integrado de disponibilização de serviços eletrónicos transversais. Consiste na capacidade das organizações interagirem e agirem em prol de benefícios comuns, através de comunicação e partilha de informação e conhecimento.

A iAP é uma plataforma central orientada para os serviços e tem como objetivo dotar a Administração Pública (AP) de uma ferramenta partilhada, que permita a interligação dos sistemas da AP e a composição e disponibilização de serviços eletrónicos multicanal mais próximos das necessidades dos cidadãos e empresas, através de quatro serviços independentes: Integração, Mensagens, Pagamentos e Autenticação¹¹.

Este serviço é baseado num conceito de disponibilização de serviços partilhados entre diversas Entidades, com o intuito de simplificar a disponibilização destes serviços ao público. A iAP disponibiliza serviços online e a respetiva gestão, comunicação segura entre sistemas de Informação, pagamentos online e serviços de envio e receção de mensagens, entre outras funcionalidades.

A interoperabilidade na Administração Pública tem vindo a ganhar relevância e importância no que respeita à criação e evolução de serviços públicos digitais, de forma a combater a fragmentação e promover a criação de um ecossistema único e comum.

Na literatura existem poucas referências à utilização de interoperabilidade de dados aplicada aos canais de denúncia, contudo alguns autores salientam a importância desta tecnologia em várias áreas da Administração Pública.

¹¹ Fonte: <https://www.iap.gov.pt/web/iap/perguntas-frequentes>, consultado em 26/1/2024

Hellberg & Grönlund (2013) exploram os conflitos e desafios enfrentados na implementação de interoperabilidade em projetos de governo eletrônico, com destaque para o sector da saúde da Suécia. A interoperabilidade é vista como uma forma de integrar serviços e melhorar a eficiência na troca de dados, contudo é suscetível de conflitar com valores como a privacidade e a segurança dos cidadãos.

Cestari et al. (2020) destacam a importância da interoperabilidade para a eficiência e colaboração entre entidades do setor público. Adicionalmente, propõem um modelo de diagnóstico, designado Modelo de Capacidade de Interoperabilidade da Administração Pública (PAICM), que visa avaliar e melhorar a interoperabilidade das organizações públicas em termos de troca de informações, processos e sistemas.

Putra et al. (2022) identificam que a integração de IA e interoperabilidade na Administração pública é suscetível de melhorar os canais de denúncia, aumentar a eficiência, poupar custos e aumentar a competitividade.

No trabalho de Džino et al. (2023), são apresentados desafios e oportunidades associados à digitalização e interoperabilidade no sector público da Bósnia e Herzegovina. Segundo este estudo, a digitalização e a interoperabilidade são fundamentais para melhorar a administração pública, aumentando a produtividade e criando oportunidades de serviço. Ademais, a adoção destas tecnologias apresenta benefícios, não só para as instituições, mas também para a economia e para os cidadãos.

Em suma a iAP é vista como uma ferramenta que promove a eficiência na troca de dados entre entidades, sendo que os benefícios da sua utilização ultrapassam em grande medida as desvantagens que alguns autores identificam, como eventuais falhas na privacidade e segurança dos cidadãos.

Metodologia de investigação

No presente capítulo apresenta-se a metodologia de investigação que é composta pelo modelo de análise e pelos métodos e técnicas que são utilizados.

3.1. Modelo de análise

O modelo de análise é o esquema orientador da conceção teórica da situação que está a ser investigada. Neste caso será utilizado um modelo de análise misto, com base em abordagens qualitativas e quantitativas sobre a implementação dos canais de denúncia e a sua utilização pelos cidadãos. Para esta análise, será feita uma análise documental e de dados secundários. No caso da análise sobre a utilização dos canais de denúncia pelos cidadãos será feita uma análise quantitativa com base na aplicação de um inquérito.

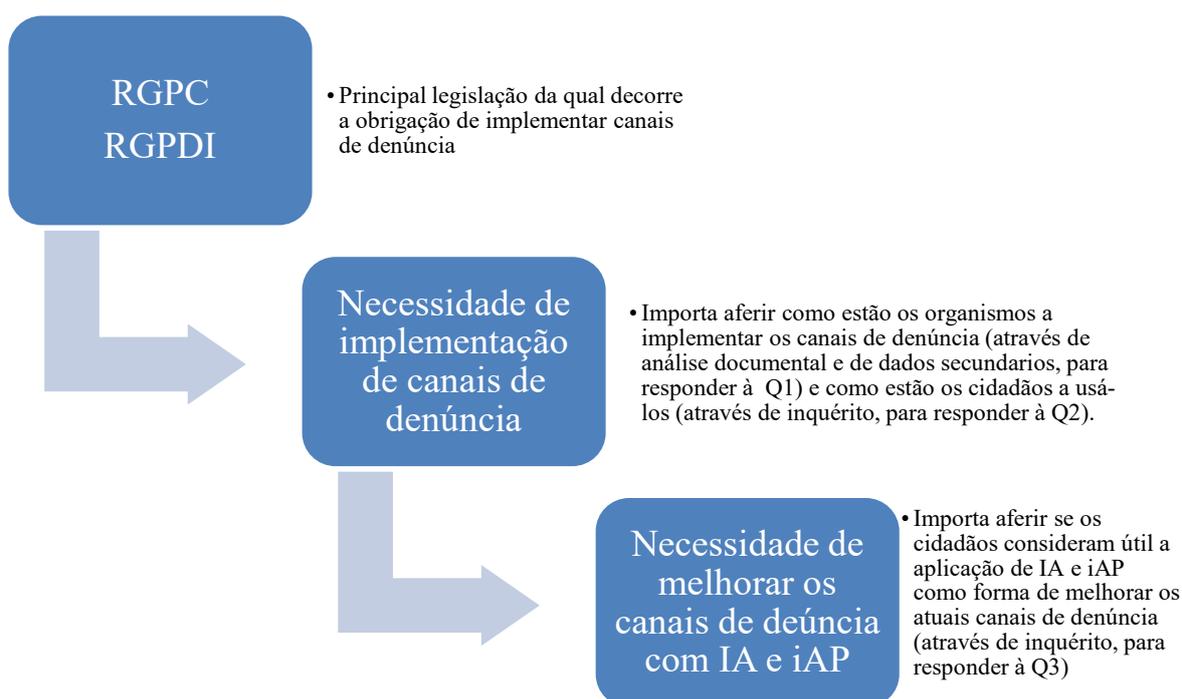


Figura 3.1 Modelo de Análise

De seguida apresenta-se os métodos e técnicas de investigação a utilizar.

3.1. Métodos e técnicas de investigação

A metodologia adotada no presente trabalho é a análise histórico-contextual. A análise histórico-contextual foca-se na compreensão profunda e detalhada de um único contexto histórico, examinando os eventos dentro das circunstâncias específicas em que ocorrem. Tem como objetivo analisar a complexidade de um período específico, tendo em consideração as características culturais, políticas, económicas e sociais que moldaram os eventos históricos. A sua metodologia de aplicação envolve a recolha de dados primários e secundários relativamente a um período específico, procurando compreender os eventos no seu contexto próprio. Como exemplo de análises histórico-contextuais temos os estudos de caso, que são importantes para a produção de descrições contextuais profundas e exaustivas (Landman, 2008).

Atendendo às questões de investigação formuladas em 1.1.1. e das hipóteses apresentadas em 1.1.2., apresentam-se os seguintes métodos e técnicas de análise.

Quadro 3.1 Questões de investigação, hipóteses, métodos e técnicas

Questão de investigação	Hipótese	Métodos e técnicas
Q1. De que forma os organismos da Administração Pública em Portugal estão a implementar e operacionalizar os canais de denúncia em conformidade com as novas exigências legais;	H1. As entidades da AP estão a implementar canais de denúncia de forma similar e correta	Métodos qualitativos e quantitativos; Análise documental e de dados secundários
Q2. De que forma os canais de denúncia estão a ser utilizados pelos cidadãos;	H2. Os cidadãos utilizam de forma limitada os canais de denúncia devido a falta de confiança e desconhecimento dos mesmos	Métodos qualitativos e quantitativos; Análise dados primários através de inquérito
Q3. De que forma o recurso a novas tecnologias, como a IA e iAP podem melhorar a qualidade dos atuais canais de denúncia.	H3. A aplicação de IA e iAP em canais de denúncia é vista como útil na melhoria da sua eficiência	Métodos qualitativos e quantitativos; Análise dados primários através de inquérito

Técnicas de recolha de dados

Neste capítulo apresentam-se as técnicas de recolha de dados utilizadas no processo de investigação.

4.1. Investigação quantitativa

Na realização deste trabalho foram utilizadas as seguintes técnicas de recolha de dados: análise documental e de dados secundários, e análise de dados primários recolhidos por questionário online.

4.1.1. Análise documental e de dados secundários

Em Portugal, o tema dos canais de denúncia tem vindo a ganhar importância essencialmente a partir da entrada em vigor do RGPC e do RGPDI. Na literatura, destacam-se os livros de Maia & Simões (2022) e Simões (2023a) que reúnem vários textos sobre canais de denúncia e proteção de denunciantes. Em Maia & Simões (2022) encontramos um conjunto de 10 artigos sobre a temática do *whistleblowing* em Portugal, organizados segundo dois eixos de abordagem:

"As dinâmicas organizacionais, enquanto realidades importantes para se perceber os cuidados que importa acautelar, relativamente à adoção e subsistência de canais de reporte, no sentido de potenciarem e aprofundarem adequadas culturas organizacionais de integridade."

"Os direitos, deveres e garantias enquanto critérios fundamentais a verificar, relativamente ao modo como a proteção do denunciante deve operar nas organizações."

Figura 4.1 *Whistleblowing em Portugal - eixos de abordagem. Fonte: Maia & Simões (2022)*

Em Simões (2023a) apresenta-se um conjunto de textos de 12 autores que abordam o RGPC e o RGPDI, com destaque para este último, numa perspetiva jurídica e não jurídica, antecipando-se as implicações que surgirão na execução da lei no dia-a-dia. No âmbito do presente trabalho, destaca-se o texto de Lara Reis que questiona se o *Whistleblowing* é uma ferramenta de estratégia, *insource* ou *outsourced*, com a tónica da utilização da tecnologia, designadamente o recurso à Inteligência Artificial e algoritmos ao serviço do *Whistleblowing*.

Em Simões (2023b) encontramos um conjunto de disposições legais mais relevantes sobre a prevenção da corrupção e infrações conexas. Esta coletânea de legislação junta vários diplomas legais em torno dos que institucionalizam, respetivamente, o *Compliance* e o *Whistleblowing*: o RGPC e o RGPDI (Anexo 1).

Em termos práticos, o RGPC determinou a obrigatoriedade de implementação de canais de denúncia para as entidades abrangidas, no prazo de 180 dias após a publicação daquele regime, em 9 de dezembro de 2021. Este prazo revelou-se reduzido para que as entidades pudessem interiorizar o próprio regime e colocá-lo em prática de forma eficaz e eficiente, principalmente ao nível da implementação dos canais de denúncia.

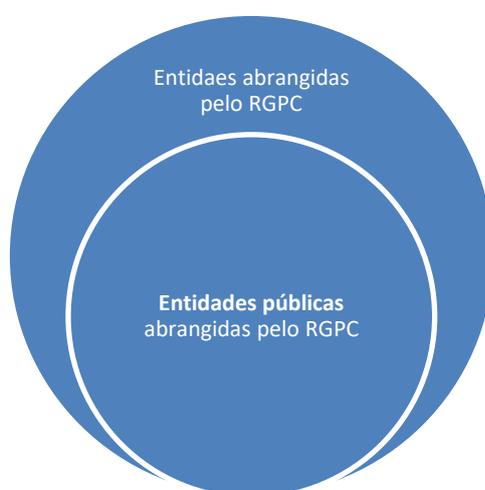


Figura 4.2 Entidades abrangidas pelo RGPC

No caso de entidades que contrataram canais de denúncia e publicitaram essa contratação no portal Base.gov, é possível analisar o número de contratos por entidade adjudicante, entidade adjudicatária, âmbito da contratação, tipo de procedimento e CPV¹².

Atualmente não estão disponíveis estatísticas sobre a utilização de canais de denúncias em Portugal, no entanto notícias apontam para o facto de algumas organizações não se encontrarem a cumprir a legislação, por não terem implementado os respetivos canais¹³. A verificação da existência dos canais de denúncia, entre outras componentes dos programas de cumprimento normativo, é da responsabilidade do MENAC, organismo criado aquando da entrada em vigor

¹² O CPV contém um vocabulário principal para a definição do objeto de um contrato e um vocabulário suplementar para se acrescentar qualquer informação qualitativa (Fonte: <https://ted.europa.eu/pt/simap/cpv>, consultado a 23/09/2024)

¹³ <https://observador.pt/opiniao/um-ano-depois-onde-estao-os-canais-de-denuncia/>, <https://observador.pt/especiais/canal-de-denuncias-obrigatorio-desde-junho-ainda-e-uma-miragem-em-portugal/>, consultados em 25/1/2024

do RGPC. Contudo, passados mais de dois anos após a sua implementação, desconhecem-se os resultados práticos da sua atividade.

4.1.2. Análise de dados primários

Para analisar de que forma os canais de denúncia estão a ser utilizados pelos cidadãos e de que forma o recurso a novas tecnologias, como a IA e iAP podem melhorar a qualidade dos atuais canais de denúncia, foi utilizado um questionário online a 50 cidadãos, dividido em 4 secções:

- Secção 1: Dados sobre o respondente;
- Secção 2: Grau de conhecimento sobre prevenção da corrupção e canais de denúncia;
- Secção 3: Experiência em denunciar irregularidades;
- Secção 4: Inteligência Artificial e Interoperabilidade.

No **anexo 2** encontra-se o detalhe deste questionário e no **anexo 3** apresentam-se os respetivos resultados.

Análise de resultados

No presente capítulo apresentam-se os resultados relativamente às hipóteses formuladas inicialmente.

5.1. H1: As entidades da AP estão a implementar canais de denúncia de forma similar e correta.

Para avaliar se as entidades da AP estão a implementar canais de denúncia de forma similar e correta, analisou-se a informação disponível no portal Base.gov, onde contam 161 contratos relativos a canais de denúncia¹⁴, que se dividem da seguinte forma:

Quadro 5.1 Distribuição dos contratos por âmbito

Âmbito do contrato	Nº de contratos
Implementação de canal de denúncias	97
Implementação de canal de denúncias e outros ¹⁵	23
Apoio jurídico/técnico/consultoria	23
Gestão de denúncias	7
Implementação e gestão de canal de denúncias	7
Formação	2
Armazenagem de dados de canal de denúncias	1
Tratamento de denúncias	1
Total	161

Na sua maioria, os contratos são relativos a implementação dos canais de denúncia e demais matérias relacionadas com *compliance* relativamente a RGPC, RGPDI, RGPD, entre outros. Analisando, especificamente os contratos que incluem a implementação de canais de denúncia, verificaram-se 127 contratos que no total ascenderam a aproximadamente 2M€ de preço contratual (PC), sendo que em média cada entidade despendeu de aproximadamente 10 mil euros na implementação de um canal de denúncias.

¹⁴ A pesquisa ocorreu pelos termos “denúncia” e “denuncia” durante o mês de setembro de 2024

¹⁵ Ex: Assistência técnica, assessoria em matéria de proteção de dados, RGPC, RGPDI, gestão de reclamações, planos de prevenção de riscos de corrupção e infrações conexas, entre outros

Quadro 5.2 Distribuição dos contratos de relacionados com a implementação de canal de denúncias

Âmbito do contrato	N.º de contratos	Mín. PC (€)	Máx. PC (€)	Média PC (€)	Desv. Pad PC	Total PC (€)
Implementação de canal de denúncias	97	-	70 974,38	9 956,23	11 789,69	965 753,90
Implementação e gestão de canal de denúncias	7	499,00	46 250,00	16 864,14	15 621,81	118 049,00
Implementação de canal de denúncias e outros	23	2 125,00	263 870,00	38 157,36	59 482,75	877 619,25
Total	127	-	263 870,00	15 444,27	29 202,26	1 961 422,15

Analisando os tipos de procedimento de contratação por âmbito, verifica-se que a implementação de um canal de denúncias ocorreu por ajuste direto na maioria das vezes (74,23%), seguindo-se a consulta prévia (16,49%), o acordo-quadro (6,19%) e o concurso público (3,09%).

Quadro 5.3 Distribuição dos contratos de relacionados com a implementação de canal de denúncias por tipo de procedimento de contratação

Âmbito do contrato	N.º de contratos	%
Implementação de canal de denúncias	97	76,38%
Ajuste Direto Regime Geral	72	74,23%
Ao abrigo de acordo-quadro (art.º 258.º)	6	6,19%
Concurso público	3	3,09%
Consulta Prévia	16	16,49%
Implementação e gestão de canal de denúncias	7	5,51%
Ajuste Direto Regime Geral	5	71,43%
Concurso público	1	14,29%
Consulta Prévia	1	14,29%
Implementação de canal de denúncias e outros	23	18,11%
Ajuste Direto Regime Geral	18	78,26%
Concurso limitado por prévia qualificação	1	4,35%
Consulta Prévia	4	17,39%
Total Geral	127	100,00%

Na tabela seguinte encontra-se uma lista com as 10 entidades adjudicatárias com maior valor total de contratos, sendo que no **Anexo 4** apresenta-se a lista detalha destas entidades. Desta análise constata-se que 3 empresas somam 67.78% do total gasto em canais de denúncia, o que evidencia uma elevada concentração no mercado.

Quadro 5.4 Entidades adjudicatárias com maior valor total de contratos

Empresa	Nº de contratos	% Nº de contratos	Total PC	Total PC %
Fujitsu Technology Solutions, Lda	2	1,57%	422 170	21,52%
Closer - Consultoria, Lda.	18	14,17%	266 817	13,60%
WIREMAZE- Sistemas de Informação, S.A	19	14,96%	133 487	6,81%
Informa D& B (Serviços de gestão de empresas)	10	7,87%	110 153	5,62%
Wemake, Tecnologias de Informação, Lda	3	2,36%	95 418	4,86%
Link Consulting - Tecnologias de Informação, S.A.	5	3,94%	75 475	3,85%
Master Link - Sistemas de Informação, Lda	1	0,79%	60 900	3,10%
Dnxt Azores, Unipessoal Lda	1	0,79%	58 410	2,98%
CCR - Sociedade de Advogados, SP, RL	3	2,36%	57 440	2,93%
Whistleblower Software ApS	15	11,81%	49 244	2,51%

A tabela anterior pode ser representada num gráfico, onde se compara a percentagem total do preço contratual de cada empresa com a percentagem do número de contratos.

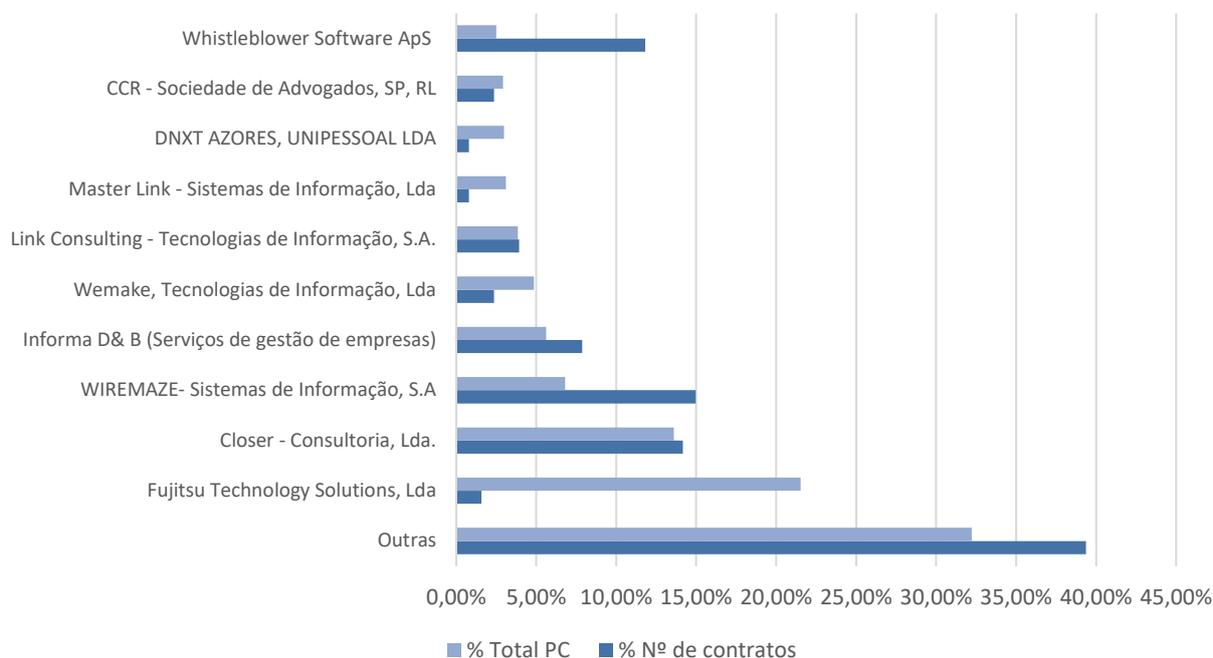


Figura 5.1 Valor total e n.º de contratos por entidade adjudicatária

Foi analisado o gasto total por CPV associado a estes contratos (Anexo 5), destacando-se o seguinte: os serviços técnicos e serviços de TI são os dois maiores grupos de contratos, representando cerca de 29% do total. Os serviços de fornecimento de software e serviços de assistência técnica também são significativos, contribuindo com cerca de 16% do total. Estes resultados sugerem que os referidos serviços são críticos para as entidades adjudicantes.

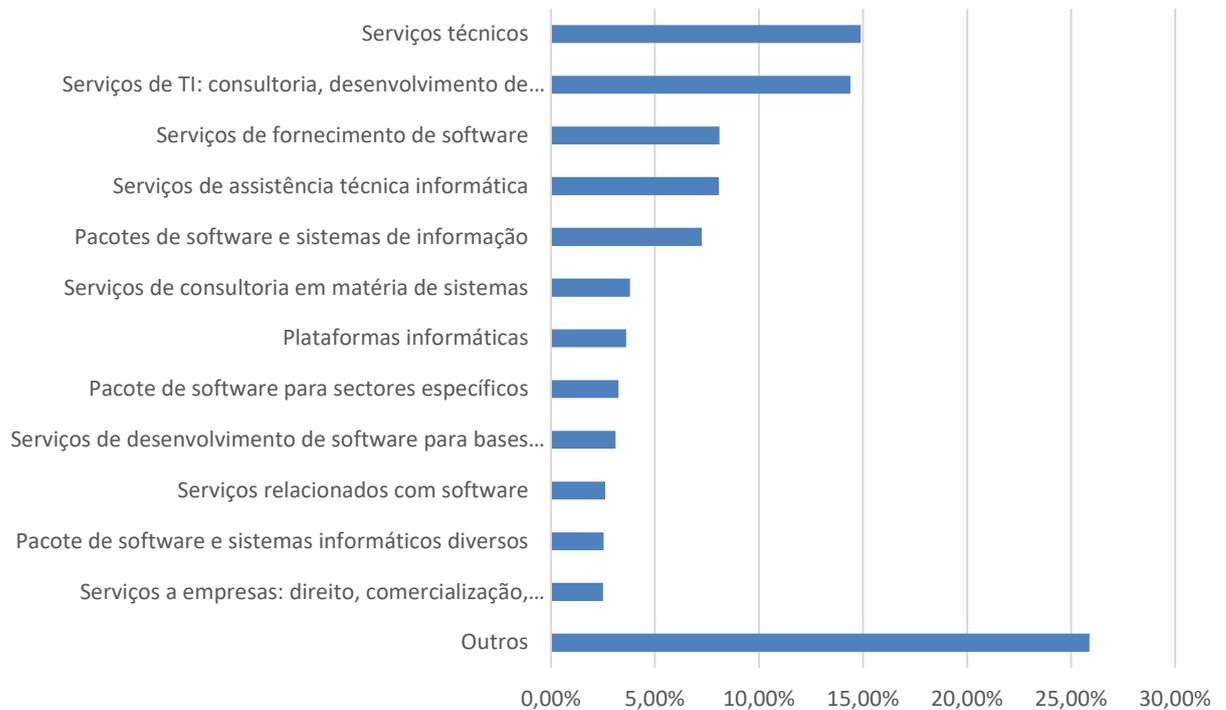


Figura 5.2 Total gasto por CPV

Através desta análise constata-se uma grande variedade de tipos de contratos tendentes à implementação dos canais de denúncia por parte das entidades da AP. Por outro lado, não existe evidência para considerar que essa implementação esteja a ser feita de forma incorreta.

5.2. H2: Os cidadãos utilizam de forma limitada os canais de denúncia devido a falta de confiança e desconhecimento dos mesmos.

Em primeiro lugar importa analisar o grau de conhecimento dos cidadãos sobre esta temática, que se decompõe em vários tópicos: RGPC, RGPDI, Plano de Prevenção de Riscos de Corrupção e Infrações Conexas, Código de conduta, Funcionamento dos canais de denúncia, Distinguir uma denúncia de uma reclamação, Funções do responsável pelo cumprimento normativo, Instrumentos que fazem parte do programa de cumprimento normativo da minha entidade, Políticas e procedimentos de prevenção da corrupção e infrações conexas implementados na sua entidade.

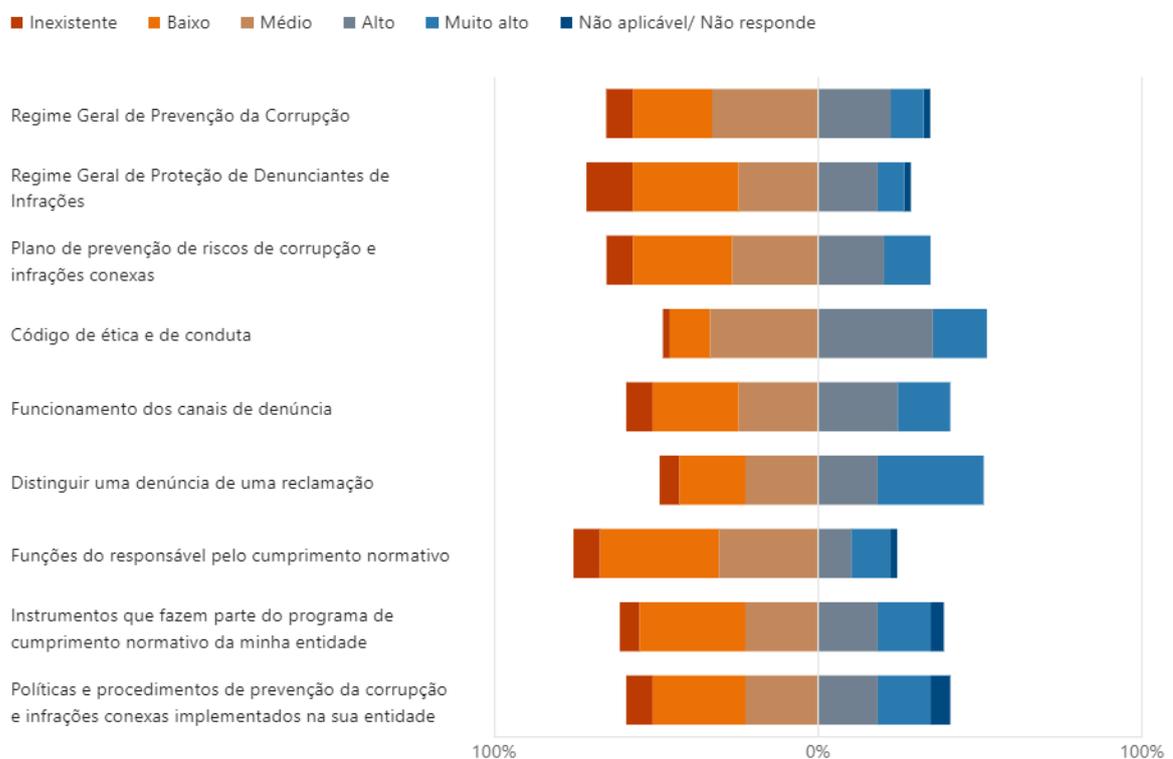


Figura 5.3 Grau de conhecimento dos cidadãos sobre temas relacionados com a prevenção de corrupção

De um modo geral, existe um conhecimento moderado sobre vários tópicos, mas há áreas em que o conhecimento é predominantemente avaliado com baixo, principalmente no que diz respeito à prevenção da corrupção e proteção de denunciantes. Temas como o código de ética e de conduta e a capacidade de distinguir uma denúncia de uma reclamação, apresentam maior nível de conhecimento.

A distribuição dos dados indica que, em alguns tópicos há uma concentração de respostas em torno de valores baixos, como por exemplo as funções do responsável pelo cumprimento normativo, e noutros tópicos os dados são mais dispersos, como é o caso da capacidade de distinguir uma denúncia de uma reclamação.

Quadro 5.5 Avaliação do grau de conhecimento em matérias relacionadas com a prevenção da corrupção

Avaliação do grau de conhecimento	Moda	Mediana	Assimetria	Curtose
Regime Geral de Prevenção da Corrupção	3 - Médio	3 - Médio	0,090	2,287
Regime Geral de Proteção de Denunciantes de Infrações	2 - Baixo	3 - Médio	0,291	2,241
Plano de prevenção de riscos de corrupção e infrações conexas	2 - Baixo	3 - Médio	0,217	2,061
Código de ética e de conduta	4 - Alto	4 - Alto	-0,222	2,455
Funcionamento dos canais de denúncia	2 - Baixo	3 - Médio	0,040	1,955
Distinguir uma denúncia de uma reclamação	5 - Muito alto	4 - Alto	-0,299	1,856
Funções do responsável pelo cumprimento normativo	2 - Baixo	4 - Alto	0,541	2,575
Instrumentos que fazem parte do programa de cumprimento normativo da minha entidade	2 - Baixo	3 - Médio	0,276	1,938
Políticas e procedimentos de prevenção da corrupção e infrações conexas implementados na sua entidade	2 - Baixo	3 - Médio	0,189	1,930

Adicionalmente, verificou-se que a maioria dos inquiridos (48%) não teve formação sobre prevenção da corrupção e infrações conexas.

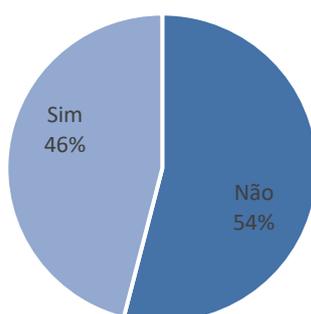


Figura 5.4 Alguma vez teve formação sobre prevenção da corrupção e infrações conexas?

Do conjunto de inquiridos que afirmaram ter tido formação sobre prevenção da corrupção e infrações conexas, a maioria teve formações curtas, de duração igual ou inferior a 2 horas.

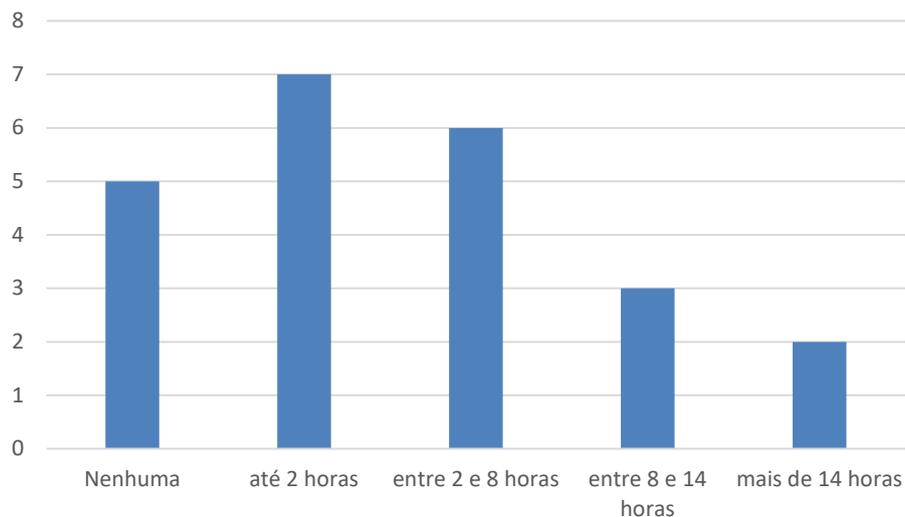


Figura 5.5 Grau de conhecimento dos cidadãos sobre temas relacionados com a prevenção de corrupção

Quanto à capacidade de distinção do que pode constituir uma denúncia, os inquiridos tendem em escolher a resposta correta, à exceção da questão “obtenção de informação incompleta por parte de funcionário público”.

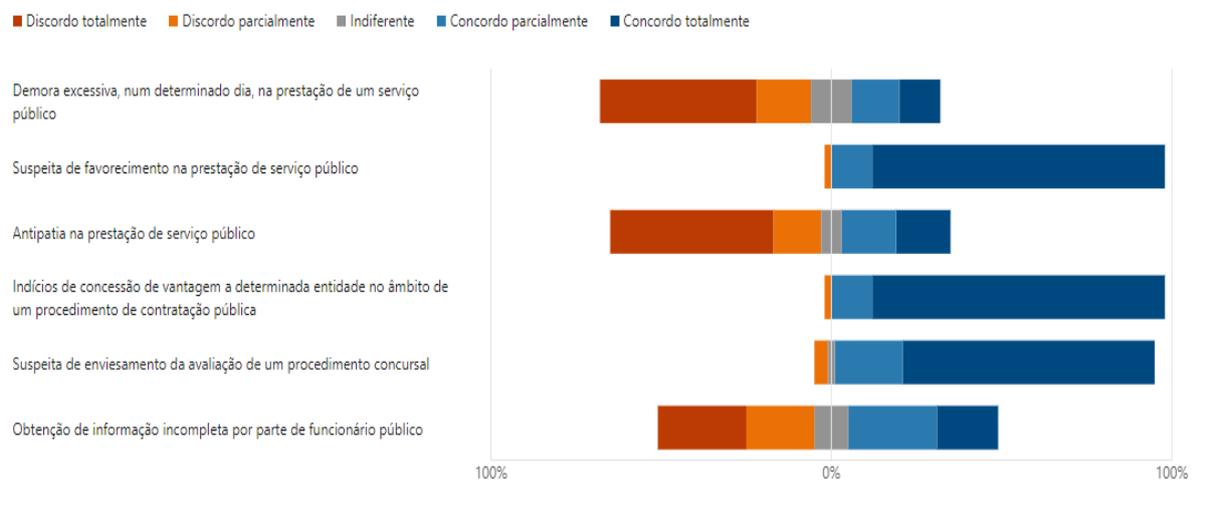


Figura 5.6 Avaliação da capacidade de distinção do que pode constituir uma denúncia

O grau de confiança relativamente aos canais de denúncia obteve um valor médio de 5,388 numa escala de 0-10, o que sugere uma perceção moderada de confiança por parte dos inquiridos. No entanto, há uma dispersão significativa nas respostas, o que indica que os níveis de confiança variam bastante. O enviesamento negativo sugere que mais respondentes tendem a dar respostas acima da média, mas esse enviesamento não é muito expressivo. A curtose negativa indica uma distribuição ligeiramente achatada, o que implica que as respostas estão distribuídas entre os valores mais baixos e mais altos das observações.

Quadro 5.6 Grau de confiança relativamente aos canais de denúncia

	Min.	Máx.	Média	Desv. Pad.	Enviesamento	Curtose
Grau de confiança	0	10	5,388	2,244	- 0,383	- 0,322

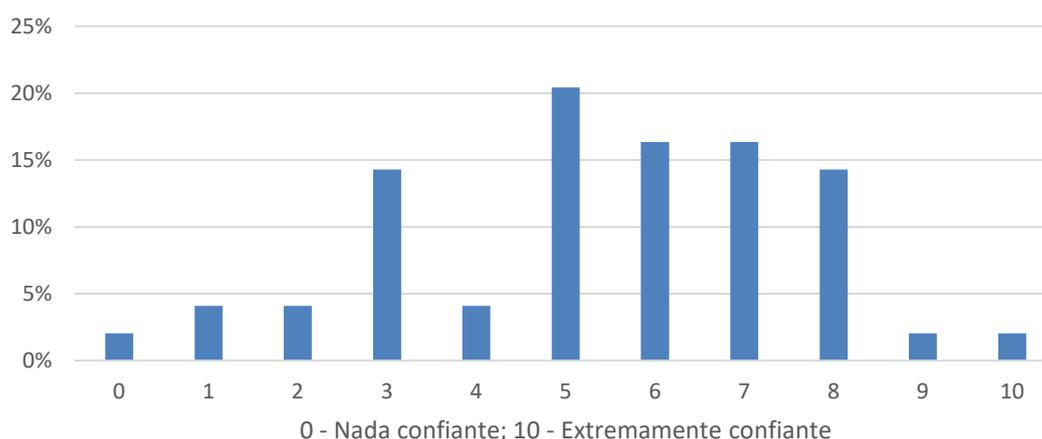


Figura 5.7 Grau de confiança relativamente aos canais de denúncia

Perante a questão “alguma vez apresentou uma denúncia sobre uma irregularidade praticada numa organização”, 10 respondentes afirmaram ter apresentado pelo menos uma denúncia relativamente a uma entidade nacional. Deste universo, 70% afirmaram ter apresentado a denúncia sobre uma entidade pública. Em termos de tipos de irregularidades denunciadas, verificaram-se os seguintes: contratação pública, segurança e conformidade dos produtos, defesa do consumidor, proteção da privacidade e dos dados pessoais e segurança, entre outros.

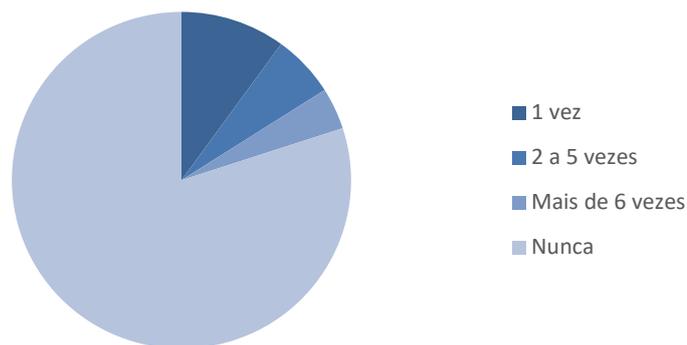


Figura 5.8 Alguma vez apresentou uma denúncia?

Quanto ao modo de apresentação das denúncias, 50% dos inquiridos indicou ter feito por escrito através de plataforma eletrónica, 40% por escrito através de email e 10% por escrito através de carta. 50% dos inquiridos indicaram ter tido alguma dificuldade durante o reporte da denúncia, sendo que 80% não conseguiu ultrapassar essa dificuldade.

Para os inquiridos que identificaram ter apresentado alguma denúncia, questionou-se quanto ao sentimento de proteção de represálias, grau de confiança relativamente ao canal usado e grau de confiança relativamente ao desfecho da denúncia, tendo os resultados médios sido relativamente baixos (<4,300), com alta variabilidade nas respostas.

Quadro 5.7 Sentimento de proteção contra represálias e confiança

	Min.	Máx.	Média	Desv. Pad.	Enviesamento	Curtose
Sentiu-se protegido de represálias?	0	10	4,300	3,773	0,004	- 1,652
Grau de confiança relativamente ao canal utilizado?	0	8	3,500	3,567	0,331	- 2,116
Grau de confiança relativamente ao desfecho da denúncia efetuada?	0	9	3,300	3,653	0,537	- 1,592

Em suma, face aos resultados obtidos, existe evidência para considerar que os cidadãos utilizam de forma limitada os canais de denúncia devido a alguma falta de confiança e desconhecimento sobre os mesmos.

5.3. H3: A aplicação de IA e iAP em canais de denúncia é vista como útil na melhoria da sua eficiência

Para analisar esta hipótese, em primeiro lugar tentou aferir-se o conhecimento dos inquiridos sobre IA e iAP e o seu nível de confiança sobre estas tecnologias. Numa escala de 0-10, os níveis de conhecimento médio ascenderam a 6,654 e 5,340, respetivamente, sugerindo que os respondentes têm em média um maior nível de conhecimento sobre IA do que sobre iAP. Os níveis de conhecimento sobre IA apresentaram menos variação, e os níveis de conhecimento sobre iAP registaram mais dispersão.

Posteriormente foi calculado o teste T-student para amostras emparelhadas, concluindo-se não existir evidência suficiente para rejeitar a hipótese nula, o que significa que não existe diferença significativa entre o nível de conhecimento em IA e iAP (p-value=0.110).

Quadro 5.8 Nível de conhecimento em IA e iAP

	Min.	Máx.	Média	Desv. Pad.	Enviesamento	Curtose	T-student
Nível de conhecimento IA	1	10	6,654	2,121	- 0,164	- 0,371	1,627
Nível de conhecimento iAP	1	10	5,340	2,861	- 0,456	- 1,015	(0,110)

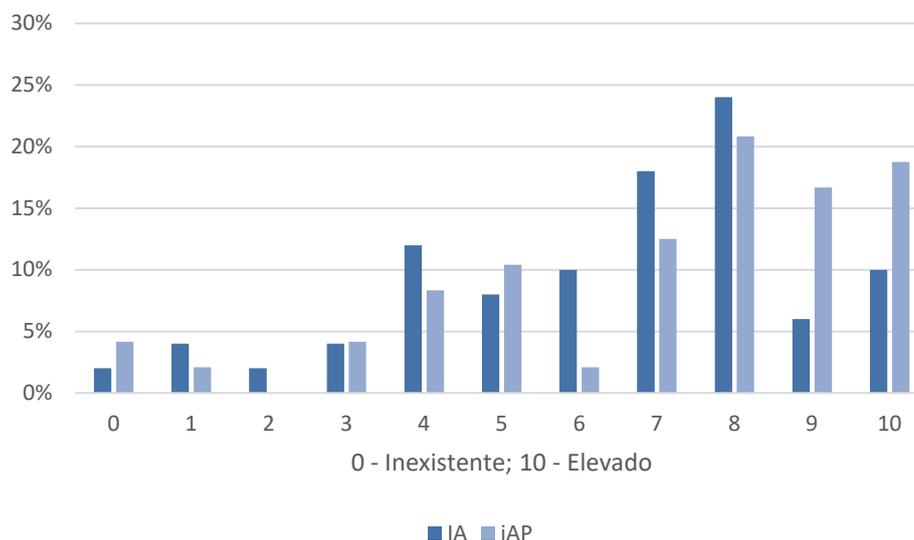


Figura 5.9 Nível de conhecimento em IA e iAP

Posteriormente questionou-se quanto ao nível de confiança em utilizar um canal de denúncias dotados de IA e iAP. Os valores médios alcançados foram de 6.400 para a IA e 7.042 para a iAP. De modo semelhante ao nível de conhecimento, foi calculado o teste T-student para amostras emparelhadas, concluindo-se não existir evidência suficiente para rejeitar a hipótese nula de que existe uma diferença significativa entre os níveis de confiança em usar um canal de denúncias com IA e iAP. Ambas as tecnologias são vistas como positivas pelos inquiridos, embora a iAP seja considerada como de maior confiança.

Quadro 5.9 Nível de confiança em IA e iAP

	Min.	Max.	Média	Desvio padrão	Enviesamento	Curtose	T-student
Nível de confiança IA	0	10	6,400	2,491	-0,685	-0,021	1.729
Nível de confiança iAP	0	10	7,042	2,713	-1,007	0,382	(0,090)

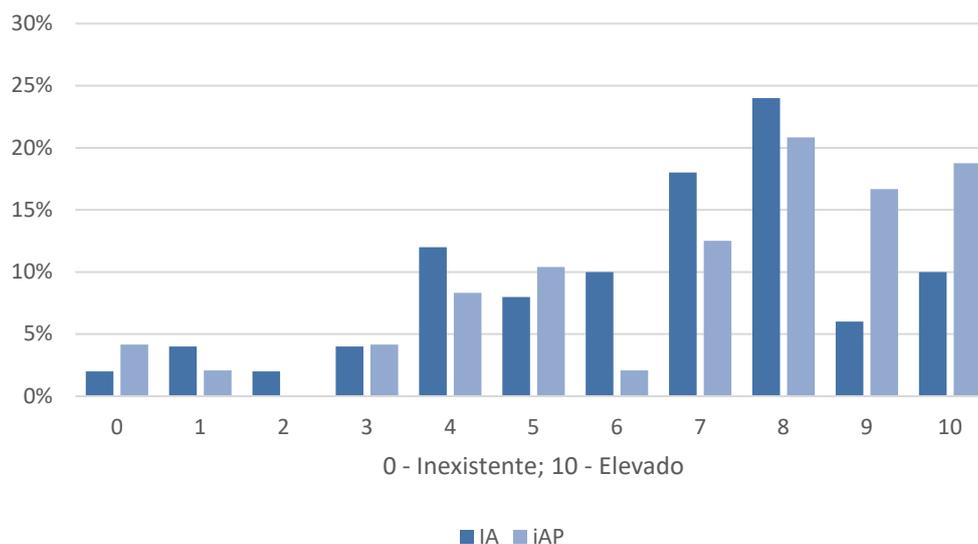


Figura 5.10 Nível de confiança em IA e iAP

De seguida questionou-se os inquiridos se consideram útil a integração de IA num canal de denúncias, de forma a auxiliar o denunciante no reporte da mesma, por exemplo, através de um assistente virtual, e a auxiliar o tratamento de cada denúncia (por exemplo, na fase de triagem). Foi colocada uma questão semelhante relativamente à utilidade de utilização de iAP. Por fim, questionou-se a utilidade da existência de um canal de denúncias único na Administração Pública, dotado de Inteligência Artificial e Interoperabilidade.

Quadro 5.11 Perceção de utilidade relativamente a IA e iAP

	Min.	Máx.	Média	Desv. Pad.	Enviesamento	Curtose	ANOVA
Utilidade de IA para o reporte	0	10	6,100	2,794	-0,563	-	0,398
Utilidade de IA para a tratamento	0	10	6,680	2,766	-0,798	-	0,338
Utilidade de iAP	0	10	7,265	2,699	-1,097	0,723	1.250 (0.292)
Utilidade de canal de denúncias único, com IA e iAP	0	10	6,469	3,103	-0,853	-	0,185

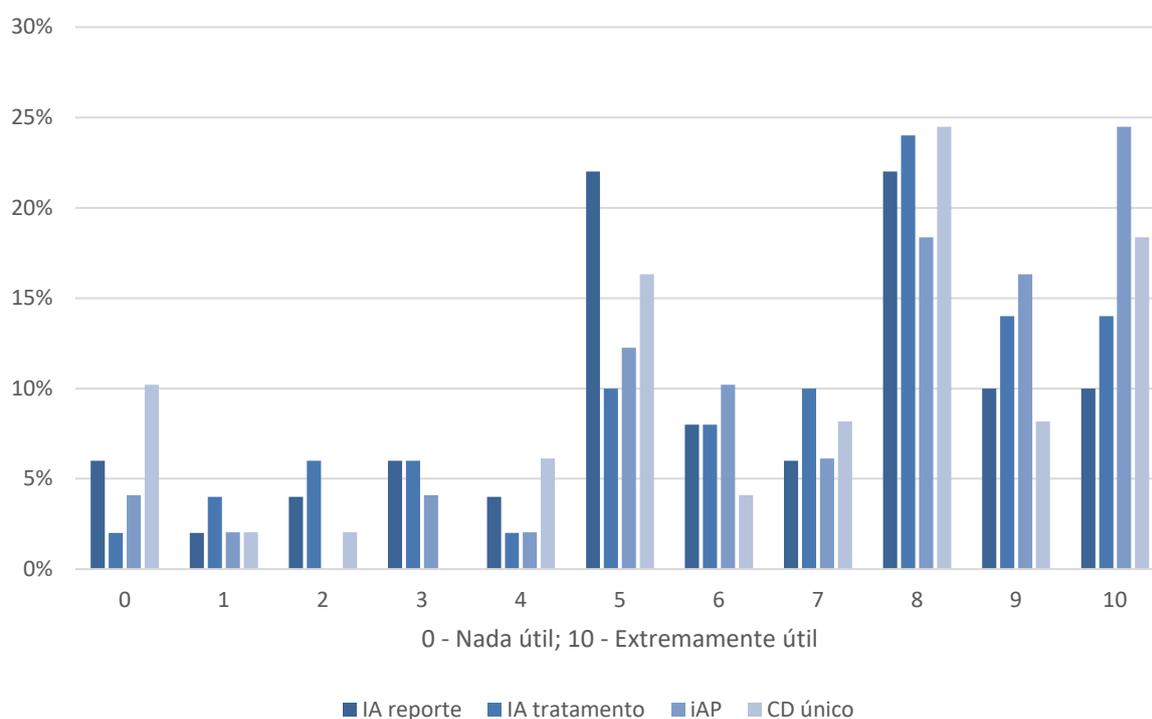


Figura 5.11 Nível de utilidade sobre IA (reporte e tratamento), iAP e Canal de Denúncias único

As quatro variáveis apresentam valores médios semelhantes, entre 6 e 7, indicando que os inquiridos consideram úteis a IA para o reporte e tratamento, a iAP e a eventual existência de um canal de denúncias único na AP dotado destas duas tecnologias. Apesar da iAP ter registado a média mais alta (7.265) e a IA para o reporte a média mais baixa (6.100), as diferenças não são consideradas significativas, conforme se pode verificar através do resultado do teste ANOVA.

O enviesamento negativo em todas as variáveis sugere que os respondentes tendem a atribuir valores mais altos de utilidade, sendo a iAP a mais favorecida. Os valores da curtose variam entre ligeiramente platicurticos e leptocurticos, indicando que enquanto algumas distribuições são mais achatadas, a distribuição relativa à utilidade da iAP é mais concentrada em torno da média.

Em conclusão, as quatro variáveis são consideradas similarmente úteis pelos inquiridos, com a iAP a ser ligeiramente mais valorizada. No entanto, essas diferenças não são estatisticamente significativas, conforme indicado pelo p-value do teste ANOVA. Assim, existe evidência para considerar que a aplicação de IA e iAP em canais de denúncia, é vista como útil na melhoria da sua eficiência.

5.4. Síntese do resultado das hipóteses

Em síntese, relativamente à primeira hipótese podemos afirmar que as entidades da AP estão a implementar canais de denúncia de várias formas, mediante vários tipos de aquisição. Pese embora não se tenham analisado casos de desenvolvimento de soluções internas, é possível constatar que várias entidades utilizaram procedimentos de contratação distintos para contratar soluções de canais de denúncia idênticas entre si. No entanto, não existem evidências para considerar que essa implementação não seja correta do ponto de vista legal.

Quanto à segunda e terceira hipóteses, as mesmas não deverão ser rejeitadas. Com efeito, existem evidências para considerar que os cidadãos utilizam os canais de denúncia de forma limitada devido a falta de confiança e desconhecimento dos mesmos e que a aplicação de IA e iAP em canais de denúncia é vista como útil na melhoria da sua eficiência.

Quadro 5.12 Verificação das hipóteses

Questão de investigação	Hipótese	Verificação
Q1. De que forma os organismos da Administração Pública em Portugal estão a implementar e operacionalizar os canais de denúncia em conformidade com as novas exigências legais;	H1. As entidades da AP estão a implementar canais de denúncia de forma similar e correta	- Implementação de forma similar: rejeitar hipótese; - Implementação de forma correta: não rejeitar hipótese.
Q2. De que forma os canais de denúncia estão a ser utilizados pelos cidadãos;	H2. Os cidadãos utilizam de forma limitada os canais de denúncia devido a falta de confiança e desconhecimento dos mesmos	Não rejeitar
Q3. De que forma o recurso a novas tecnologias, como a IA e iAP podem melhorar a qualidade dos atuais canais de denúncia.	H3. A aplicação de IA e iAP em canais de denúncia é vista como útil na melhoria da sua eficiência	Não rejeitar

Conclusões

No presente capítulo apresentam-se as principais conclusões obtidas com este trabalho, recomendações e oportunidades de investigação futura.

6.1. Conclusões

Nos dias de hoje, os canais de denúncia são ferramentas cruciais no combate à fraude e corrupção. Funcionam como meios de comunicação de irregularidades dentro das organizações, mas também são frequentemente utilizados para reclamações, o que leva a gastos desnecessários de tempo e recursos. A análise, tratamento e encaminhamento de denúncias são processos exigentes em termos de recursos humanos e de tempo, sendo atualmente pouco automatizados.

A literatura sobre corrupção, canais de denúncia, inteligência artificial e interoperabilidade é relativamente recente e dispersa. A corrupção é vista como uma área de estudo interdisciplinar, sendo de extrema importância a sua análise e compreensão no sentido da prevenção de futuros casos. Os canais de denúncia estão a presenciar um desenvolvimento tecnológico sem precedentes, que inclui, em alguns casos, a incorporação de IA para melhorar o seu desempenho. A iAP assume-se como uma ferramenta capaz de promover a eficiência na troca de dados entre entidades, sem comprometer a sua segurança.

Existem várias vantagens na utilização de IA e iAP aplicada aos canais de denúncia, quer do ponto de vista do denunciante aquando do reporte das denúncias, quer do ponto de vista das entidades responsáveis pelo seu tratamento. Essas vantagens traduzem-se em maior eficiência nos processos, perspetivando-se menor gasto de recursos humanos, financeiros e de tempo, na análise e tratamento das denúncias.

A implementação dos canais de denúncia na AP levou à existência de múltiplos procedimentos de contratação pública, de vários tipos, com o mesmo fim, o que denota alguma ineficiência por parte das entidades adjudicantes. Os cidadãos apresentaram um nível médio de conhecimento positivo relativamente a IA e iAP, embora não muito elevado. Não obstante, estas tecnologias foram consideradas confiáveis e úteis para serem aplicadas aos canais de denúncia, o que constitui um importante ponto de partida para a implementação generalizada das mesmas num canal de denúncias único na Administração Pública. Note-se que este resultado está em linha com a proposta que consta na Agenda Anticorrupção, de operacionalizar

um canal de denúncias comum a todo o Governo. Contudo, a implementação de um canal deste tipo poderá posteriormente ir além do Governo e estender-se a toda a Administração Pública.

6.2. Recomendações

Face aos resultados obtidos, poderá ser útil reunir esforços no sentido de uniformizar a contratação de canais de denúncia, uma vez que no presente assistimos a uma multiplicidade de aquisições com a mesma finalidade por parte das entidades. Será também importante aumentar a formação dos cidadãos sobre temas como a prevenção da corrupção e infrações conexas, de modo a melhorar a qualidade do reporte.

Adicionalmente, considera-se útil desenhar um canal de denúncias único para a Administração Pública Portuguesa, dotado de IA e iAP, de modo a evitar gastos na contratação de soluções distintas que não favorecem a uniformização do reporte de irregularidades e a troca de dados entre entidades.

6.3. Oportunidades de investigação futura

Com base nos resultados alcançados, que indicam que a IA e iAP são tecnologias consideradas úteis no âmbito dos canais de denúncia, poderá ser importante analisar outros fatores que influenciem a utilidade percebida, como por exemplo a experiência de utilização dos canais que contemplam esta tecnologia comparativamente aos canais tradicionais.

Existindo dados sobre a utilização destas tecnologias, poderão ser efetuados estudos longitudinais sobre a aplicação de IA e iAP nos canais de denúncia, assim como estudos comparativos entre diferentes sectores (ex. público *vs.* privado, saúde *vs.* educação) e analisar em que casos existem maiores ganhos em termos de utilidade.

Outra área de investigação que poderá surgir reside na análise da redução da carga de trabalho, que atualmente é realizado por funcionários e no futuro será realizado por AI, ao nível da classificação das denúncias, identificação de falsas denúncias, priorização com base na gravidade das denúncias, entre outras tarefas.

Por fim seria importante analisar a utilidade que teria um canal de denúncias único na Administração Pública, dotado de IA e iAP, como forma de obter sinergias ao nível da poupança de recursos financeiros e humanos, eficiência na troca de informação e melhoria da celeridade dos processos.

Referências bibliográficas

- ACFE. (2024). *The Nations ® Occupational Fraud 2024: 2 Foreword Occupational Fraud 2024: A Report to the Nations*.
- Almeida Prado Cestari, J. M., Loures, E. de F. R., Santos, E. A. P., & Panetto, H. (2020). A capability model for public administration interoperability. *Enterprise Information Systems*, 14(8), 1071–1101. <https://doi.org/10.1080/17517575.2018.1564154>
- AMA. (2022). *Guia para a Inteligência Artificial - Guia Para Uma Inteligência Artificial Ética, Transparente E Responsável Na Administração Pública*.
- Bardhan, P. K. (1997). Corruption and Development: A Review of Issues. *Journal of Economic Literature*, 35, 1320–1346.
<https://api.semanticscholar.org/CorpusID:142624977>
- Bazart, C., Beaud, M., & Dubois, D. (2019). *Whistleblowing vs. Random Audit: An Experimental Test of Relative Efficiency*.
- Bloch-Wehba, H., Carroll, J., Casado Perez, V., Crootof, R., Douek, E., Green, M. Z., Kadri, T., Morten, C., Mulligan, S., Racabi, G., Richards, N., Solow-Niederman, A., Tiku, N., & Welsh, N. (2024). The promise and perils of tech whistleblowing. In *Printed in U.S.A* (Vol. 118, Issue 6). <https://www.theguardian.com/news/2018/mar/17/data-war->
- Citizens attitudes towards corruption in the EU in 2024*. (2024).
<https://doi.org/10.2837/237452>
- Džino, J., Džino, S., & Injac, D. (2023). Analysis of public administration, effects and impact of digitalization and interoperability in public administration. *JITA*, 13, 48–53.
<https://doi.org/10.7251/JIT2301048D>
- Gao, L. (2020). *Technology Advancements for Whistleblowing Reporting Platforms and Employees' Decision to Blow the Whistle*. <https://doi.org/10.2308/API-2020-001>
- Transparência e Integridade - Transparency International Portugal. (2019). *Glossário Anti-Corrupção*.

- Hellberg, A. S., & Grönlund, Å. (2013). Conflicts in implementing interoperability: Re-operationalizing basic values. *Government Information Quarterly*, 30(2), 154–162. <https://doi.org/10.1016/j.giq.2012.10.006>
- Kagias, P., Garefalakis, A., Passas, I., Kyriakogkonas, P., & Sariannidis, N. (2024). Whistleblowing Based on the Three Lines Model. *Administrative Sciences*, 14(5). <https://doi.org/10.3390/admsci14050083>
- Kagias, P., Sariannidis, N., Garefalakis, A., Passas, I., & Kyriakogkonas, P. (2023). Validating the Whistleblowing Maturity Model Using the Delphi Method. *Administrative Sciences*, 13(5). <https://doi.org/10.3390/admsci13050120>
- Kang, M. M. (2023). Whistleblowing in the Public Sector: A Systematic Literature Review. *Review of Public Personnel Administration*, 43(2), 381–406. <https://doi.org/10.1177/0734371X221078784>
- Landman, T. (2008). *Issues and Methods in Comparative Politics: An Introduction, Third Edition*. Routledge.
- Maia, A., & Simões, P. (2022). *O Whistleblowing em Portugal - Proteção do Denunciante nas Organizações*. Almedina.
- Mauro, P. (1995). Corruption and growth. *Trends in Organized Crime*, 2, 67. <https://api.semanticscholar.org/CorpusID:146778066>
- Mrowiec, D. (2022). Factors influencing internal whistleblowing. A systematic review of the literature. *Journal of Economics and Management*. <https://doi.org/10.22367/JEM.2022.44.07>
- Noor, N. R. A. M., & Mansor, N. (2019). Exploring the Adaptation of Artificial Intelligence in Whistleblowing Practice of the Internal Auditors in Malaysia. *Procedia Computer Science*. <https://doi.org/10.1016/J.PROCS.2019.12.126>
- Previtali, P., & Cerchiello, P. (2022). Organizational Determinants of Whistleblowing. A Study of Italian Municipalities. *Public Organization Review*, 22(4), 903–918. <https://doi.org/10.1007/s11115-021-00554-0>
- Putra, I., Sulistiyo, U., Diah, E., Rahayu, S., & Hidayat, S. (2022). The influence of internal audit, risk management, whistleblowing system and big data analytics on the financial

- crime behavior prevention. *Cogent Economics & Finance*.
<https://doi.org/10.1080/23322039.2022.2148363>
- Silva, G. R. da, & Sousa, R. G. de. (2017). A influência do canal de denúncia anônima na detecção de fraudes contábeis em organizações. *Revista de Contabilidade e Organizações*, 11(30), 46. <https://doi.org/10.11606/rco.v11i30.134372>
- Simões, P. (2019). *O Whistleblowing em Portugal Será que pode ser praticado pelo auditor?* <http://hdl.handle.net/10400.21/11354>
- Simões, P. (2023a). *Proteção de Denunciantes e Canais de Denúncias - Whistleblowing*. Almedina.
- Simões, P. (2023b). *Regime Geral de Prevenção da Corrupção, Regime Geral de Proteção de Denunciantes de Infrações e Legislação Complementar*. Almedina.
- Tanzi, V. L. (1998). Corruption Around the World: Causes, Consequences, Scope, and Cures. *Sustainability & Economics EJournal*.
<https://api.semanticscholar.org/CorpusID:154535201>
- Teodocio, H. T., & Morales, F. N. (2024). Fear, Anger and Reporting: Emotional Antecedents of Reporting Acts of Corruption in Public Organizations. *Politica y Gobierno*, 33(1), 35–68. <https://doi.org/10.60583/gypp.v33i1.8187>
- Zheng, Y., & Liao, X. (2019). Corruption governance and its dynamic stability based on a three-party evolutionary game with the government, the public, and public officials. *Applied Economics*, 51(49), 5411–5419.
<https://doi.org/10.1080/00036846.2019.1613508>
- Zouvia, K., Investigator, S., & Ombudsman, G. (2020). *Artificial Intelligence and Whistleblowing: Can A.I. be useful for Whistleblowing processes?* WAIEL2020.
<http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=12302>

Anexo 1

RGPC, RGPDI e legislação complementar

- Estratégia Nacional Anticorrupção 2020-2024
- Regime Geral da Prevenção da Corrupção
- Regime Geral de Proteção de Denunciantes de Infrações

- Legislação Complementar:
 - Mecanismo Nacional Anticorrupção
 - Instalação do Mecanismo Nacional anticorrupção
 - Conselho de Prevenção da Corrupção
 - Estatuto da Entidade para a Transparência
 - Constituição da República Portuguesa
 - Regime do Segredo de Estado
 - Código Penal
 - Código de Processo Penal
 - Medidas de Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo
 - Lei de Combate ao Terrorismo
 - Medidas de Combate à Criminalidade Organizada
 - Medidas de Combate à Corrupção
 - Regime Penal de Corrupção no Comércio Internacional e no Sector Privado
 - Lei Geral do Trabalho em Funções Públicas
 - Código do Trabalho
 - Regime Jurídico da Prevenção, da Proibição e do Combate à Discriminação
 - Estatuto da vítima
 - Lei de Proteção de Testemunhas
 - Regulamento da Lei de Proteção de Testemunhas
 - Estatuto do Provedor de Justiça
 - Código do Procedimento Administrativo
 - Código dos Contratos Públicos
 - Regime Jurídico da Urbanização e Edificação
 - Regime Jurídico das Autarquias Locais
 - Estatuto do Pessoal Dirigente dos Serviços e Organismos da administração Pública
 - Regime do Exercício de Funções por Titulares de Cargos Políticos e Altos Cargos Públicos
 - Crimes da Responsabilidade de Titulares de Cargos Políticos
 - Estatuto do Gestor Público
 - Responsabilidade Civil Extracontratual do Estado e Pessoas Colectivas de Direito Público

- Regime Jurídico da Actividade de Inspeção da Administração Direta e Indireta do Estado
- Regime da Carreira Especial de Inspeção
- Ilícito de mera ordenação social
- Código de Justiça Militar
- Código das Sociedades Comerciais
- Práticas Comerciais Desleais
- Medidas de combate à corrupção e criminalidade económica e financeira
- Infrações Antieconómicas e Contra a Saúde Pública
- Estatuto do Serviço Nacional de Saúde
- Regime de Responsabilidade Penal por Comportamentos antidesportivos
- Estatuto do Jornalista
- Acções Encobertas
- Lei do Cibercrime
- Lei de Organização da Investigação Criminal
- Lei Quadro da Política Criminal

Fonte: Simões, Regime Geral de Prevenção da Corrupção, Regime Geral de Protecção de Denunciantes de Infrações e Legislação Complementar (2023a)

Anexo 2

Quadro A2.1 Questionário utilizado

Secção	Questão	Hipótese de resposta
Secção 1 - Dados sobre o respondente	1 - Identifique a sua faixa etária:	<input type="radio"/> Menor de 17 anos <input type="radio"/> Entre 18 e 29 anos <input type="radio"/> Entre 30 e 54 anos <input type="radio"/> Maior de 55 anos
	2 - Identifique o seu género:	<input type="radio"/> Homem <input type="radio"/> Mulher <input type="radio"/> Outro / Prefiro não responder
	3 - Qual a sua formação académica mais elevada?	<input type="radio"/> Qualificação técnica <input type="radio"/> Licenciatura <input type="radio"/> Pós-graduação <input type="radio"/> Mestrado <input type="radio"/> Doutoramento <input type="radio"/> Outro
	4 – Região onde vive	<input type="radio"/> Norte <input type="radio"/> Centro <input type="radio"/> Lisboa e Vale do Tejo <input type="radio"/> Alentejo <input type="radio"/> Algarve <input type="radio"/> Açores <input type="radio"/> Madeira <input type="radio"/> Nenhum dos anteriores
	5 - Exerce funções de chefia ou de coordenação?	<input type="radio"/> Sim <input type="radio"/> Não <input type="radio"/> Outro
	6 - Indique o sector no qual trabalha:	<input type="radio"/> Público <input type="radio"/> Privado <input type="radio"/> Terceiro setor (ex: Organizações sem Fins Lucrativos)
	6.1 - Se trabalhador do sector público, indique a área administrativa a que pertence a sua entidade. Se trabalhador do sector privado e terceiro sector, passar para a questão seguinte.	<input type="radio"/> Negócios Estrangeiros <input type="radio"/> Finanças <input type="radio"/> Presidência <input type="radio"/> Ministro Adjunto e da Coesão Territorial <input type="radio"/> Assuntos Parlamentares <input type="radio"/> Defesa Nacional <input type="radio"/> Justiça <input type="radio"/> Administração Interna <input type="radio"/> Educação, Ciência e Inovação <input type="radio"/> Saúde <input type="radio"/> Infraestruturas e Habitação <input type="radio"/> Economia <input type="radio"/> Trabalho, Solidariedade e Segurança Social <input type="radio"/> Ambiente e Energia <input type="radio"/> Juventude e Modernização <input type="radio"/> Agricultura e Pescas <input type="radio"/> Cultura

Secção	Questão	Hipótese de resposta
		<ul style="list-style-type: none"> ○ Administração Autárquica ○ Administração Regional – RAA (Açores) ○ Administração Regional – RAM (Madeira) ○ Outro
	7 - Qual o número total de funcionários da entidade onde trabalha?	<ul style="list-style-type: none"> ○ Menos de 50 ○ 50-100 ○ 101-500 ○ 501-1000 ○ Mais de 1000
Secção 2 - Grau de conhecimento sobre prevenção da corrupção e canais de denúncia	8 - Como avalia o seu grau de conhecimento sobre:	<ul style="list-style-type: none"> ○ RGPC ○ RGPDI ○ Plano de Prevenção de Riscos de Corrupção e Infrações Conexas ○ Código de conduta ○ Funcionamento dos canais de denúncia ○ Distinguir uma denúncia de uma reclamação ○ Funções do responsável pelo cumprimento normativo ○ Instrumentos que fazem parte do programa de cumprimento normativo da minha entidade ○ Políticas e procedimentos de prevenção da corrupção e infrações conexas implementados na sua entidade
	9 - Alguma vez teve formação sobre prevenção da corrupção e infrações conexas?	<ul style="list-style-type: none"> ○ Sim ○ Não
	9.1 – Se respondeu “sim” à questão anterior, nos últimos dois anos, quantas horas de formação teve sobre prevenção da corrupção e infrações conexas?	<ul style="list-style-type: none"> ○ Nenhuma ○ até 2 horas ○ entre 2 e 8 horas ○ entre 8 e 14 horas ○ mais de 14 horas
	10 - Para as seguintes situações, identifique o seu grau de concordância relativamente às que poderão ser objeto de denúncia: <ul style="list-style-type: none"> • Demora excessiva, num determinado dia, na prestação de um serviço público; • Suspeita de favorecimento na prestação de serviço público; • Antipatia na prestação de serviço público; • Indícios de concessão de vantagem a determinada entidade no âmbito de um 	<ul style="list-style-type: none"> ○ Discordo totalmente ○ Discordo parcialmente ○ Indiferente ○ Concordo parcialmente ○ Concordo totalmente

Secção	Questão	Hipótese de resposta
	<p>procedimento de contratação pública;</p> <ul style="list-style-type: none"> • Suspeita de enviesamento da avaliação de um procedimento concursal; • Obtenção de informação incompleta por parte de funcionários público 	
	11 - Qual o seu grau de confiança relativamente aos canais de denúncia atualmente em vigor?	<ul style="list-style-type: none"> ○ 0 – Nada confiante ○ 10 – Extremamente confiante
Secção 3 - Experiência em denunciar irregularidades	12 - Alguma vez apresentou uma denúncia sobre uma irregularidade praticada numa organização:	<ul style="list-style-type: none"> ○ Nunca ○ 1 vez ○ 2 a 5 vezes ○ Mais de 6 vezes
	12.1 – Case tenha apresentado pelo menos uma denúncia, é questionado relativamente à última denúncia que apresentou: Qual foi o tipo de entidade?	<ul style="list-style-type: none"> ○ Pública ○ Privada ○ Terceiro sector
	12.2 - Qual a nacionalidade da entidade?	<ul style="list-style-type: none"> ○ Nacional ○ Estrangeira
	12.3 - Qual foi o tipo de irregularidade denunciada?	<ul style="list-style-type: none"> ○ Contratação pública; ○ Serviços, produtos e mercados financeiros e prevenção do branqueamento de capitais e do financiamento do terrorismo; ○ Segurança e conformidade dos produtos; ○ Segurança dos transportes; ○ Proteção do ambiente; ○ Proteção contra radiações e segurança nuclear; ○ Segurança dos alimentos para consumo humano e animal, saúde animal e bem-estar animal; ○ Saúde pública; ○ Defesa do consumidor; ○ Proteção da privacidade e dos dados pessoais e segurança da rede e dos sistemas de informação; ○ Assédio sexual ○ Outro
	12.5 - Qual foi o modo de apresentação da denúncia:	<ul style="list-style-type: none"> ○ Por escrito através de plataforma eletrónica ○ Verbal através de plataforma eletrónica ○ Por escrito, através de carta ○ Por escrito, através de email ○ Verbal, através de reunião presencial ○ Outro

Secção	Questão	Hipótese de resposta
	12.5 - Relativamente à denúncia que apresentou, considera que foram cumpridos os seguintes prazos:	<ul style="list-style-type: none"> ○ Prazo de notificação da receção da denúncia e informação sobre os requisitos, autoridades competentes e forma de admissibilidade da denúncia externa (7 dias); ○ Prazo de comunicação das medidas previstas ou adotadas para dar seguimento à denúncia a respetiva fundamentação (3 meses a contar da data de receção da denúncia) ○ Não sabe/ não responde
	12.6 - Teve alguma dificuldade durante o reporte da denúncia?	<ul style="list-style-type: none"> ○ Não; ○ Sim, dificuldade técnica relacionada com o canal usado ○ Sim, dificuldade técnica relacionada com a explicitação do conteúdo da denúncia ○ Sim, outro tipo de dificuldade
	12.6.1 – Se a resposta anterior foi “sim”, conseguiu ultrapassar a dificuldade sentida durante o reporte da denúncia?	<ul style="list-style-type: none"> ○ Não; ○ Sim, através de ajuda prestada pela entidade; ○ Sim, através de consulta na internet; ○ Sim, através de um familiar ou amigo; ○ Outro.
	12.7 - Após ter apresentado a denúncia, sentiu-se protegido de represálias?	<ul style="list-style-type: none"> ○ 0 – Desprotegido; ○ 10 – Muito protegido
	12.8 - Qual o seu grau de confiança relativamente ao canal de denúncias utilizado?	<ul style="list-style-type: none"> ○ 0 – Nada confiante; ○ 10 – Extremamente confiante
	12.9 - Qual o seu grau de confiança relativamente ao desfecho da denúncia efetuada?	<ul style="list-style-type: none"> ○ 0 – Nada confiante; ○ 10 – Extremamente confiante
Secção 4 - Inteligência Artificial e Interoperabilidade	13 - Qual o seu nível de conhecimento relativamente à Inteligência Artificial (IA)?	<ul style="list-style-type: none"> ○ 0 – Inexistente; ○ 10 - Elevado
	14 - Qual o seu nível de conhecimento relativamente à Interoperabilidade na Administração Pública (iAP)?	<ul style="list-style-type: none"> ○ 0 – Inexistente; ○ 10 - Elevado
	15 - Considera útil a integração de IA num canal de denúncias, de forma a auxiliar o denunciante no reporte da denúncia, por exemplo, através de um assistente virtual?	<ul style="list-style-type: none"> ○ 0 – Nada útil; ○ 10 – Extremamente útil.
	16 - Considera útil a integração de IA num canal de denúncias, de forma a auxiliar o tratamento de cada denúncia	<ul style="list-style-type: none"> ○ 0 – Nada útil; ○ 10 – Extremamente útil.

Secção	Questão	Hipótese de resposta
	(por exemplo, na fase de triagem)?	
	17 - Considera útil a integração de interoperabilidade de dados num canal de denúncias, como forma de melhorar a transferência de dados entre entidades?	<ul style="list-style-type: none"> ○ 0 – Nada útil; ○ 10 – Extremamente útil.
	18 - Qual o nível de confiança que teria ao utilizar um canal de denúncias dotado de interoperabilidade?	<ul style="list-style-type: none"> ○ 0 – Nada confiante; ○ 10 – Extremamente confiante.
	19 - Qual o nível de confiança que teria ao utilizar um canal de denúncias dotado de inteligência artificial?	<ul style="list-style-type: none"> ○ 0 – Nada confiante; ○ 10 – Extremamente confiante.
	20 - Considera útil a eventual existência de um canal de denúncias único na Administração Pública, dotado de Inteligência Artificial e Interoperabilidade?	<ul style="list-style-type: none"> ○ 0 – Nada útil; ○ 10 – Extremamente útil.

Anexo 3

Resultados do inquérito

1. Identifique a sua faixa etária:

[Mais Detalhes](#)

Menor de 17 anos	0
Entre 18 e 29 anos	2
Entre 30 e 54 anos	40
Maior de 55 anos	8



Figura A3.1 Faixa etária dos inquiridos

2. Identifique o seu género:

[Mais Detalhes](#)

Homem	22
Mulher	28
Outro / Prefiro não responder	0

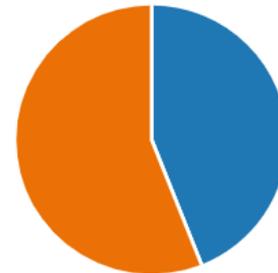


Figura A3.2 Género dos inquiridos

3. Qual a sua formação académica mais elevada?

[Mais Detalhes](#)

Qualificação técnica	2
Licenciatura	10
Pós-graduação	20
Mestrado	15
Doutoramento	3
Outro	0

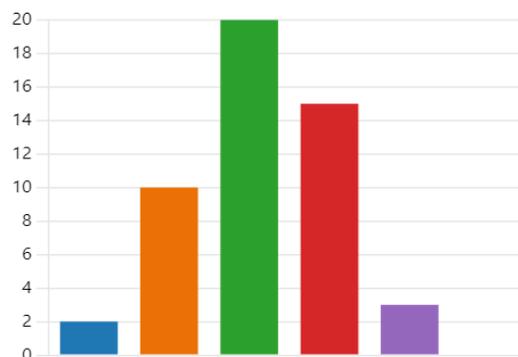


Figura A3.3 Formação académica dos inquiridos

4. Região onde vive:

[Mais Detalhes](#)

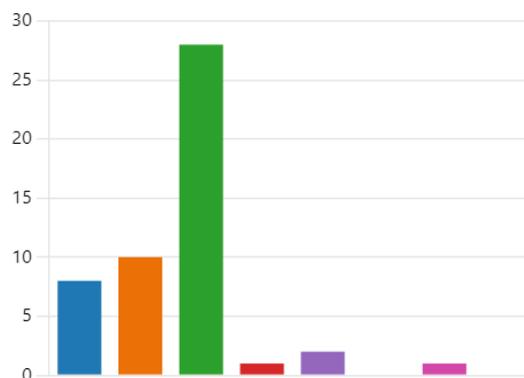


Figura A3.4 Região onde vive

5. Exerce funções de chefia ou de coordenação?

[Mais Detalhes](#)

[Informações](#)

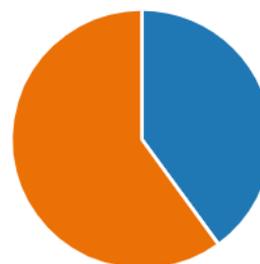


Figura A3.5 Exerce funções de chefia ou de coordenação

6. Indique o sector no qual trabalha:

[Mais Detalhes](#)

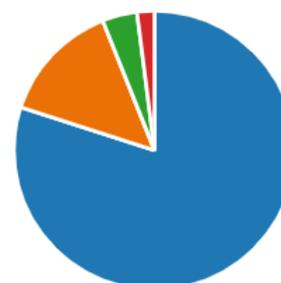
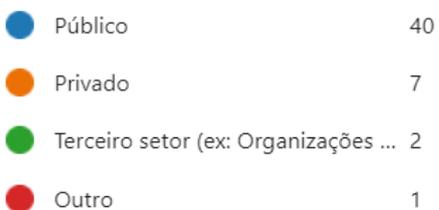


Figura A3.6 Sector no qual trabalha

7. Indique a área administrativa a que pertence a sua entidade:

[Mais Detalhes](#)

Negócios Estrangeiros	1
Finanças	5
Presidência	2
Ministro Adjunto e da Coesão T...	0
Assuntos Parlamentares	0
Defesa Nacional	0
Justiça	3
Administração Interna	0
Educação, Ciência e Inovação	5
Saúde	3
Infraestruturas e Habitação	9
Economia	1
Trabalho, Solidariedade e Segur...	1
Ambiente e Energia	0
Juventude e Modernização	2
Agricultura e Pescas	1
Cultura	1
Administração Autárquica	5
Administração Regional - RAA	0
Administração Regional - RAM	0
Outro	0

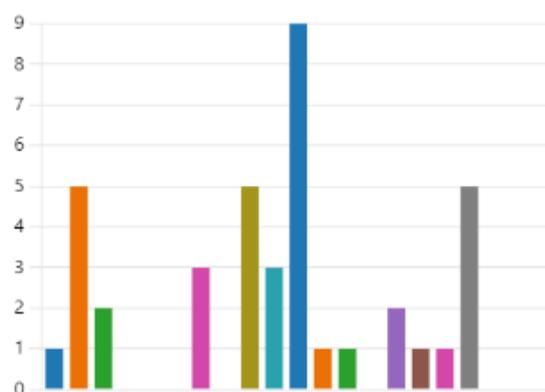


Figura A3.7 Área administrativa a que pertence a entidade em que trabalha

8. Qual o número total de funcionários da entidade onde trabalha?

[Mais Detalhes](#)

Menos de 50	9
50-100	4
101-500	16
501-1000	9
Mais de 1000	12



Figura A3.8 N.º de funcionários da entidade em que trabalha

9. Como avalia o seu grau de conhecimento sobre:

[Mais Detalhes](#)

■ Inexistente
 ■ Baixo
 ■ Médio
 ■ Alto
 ■ Muito alto
 ■ Não aplicável/ Não responde

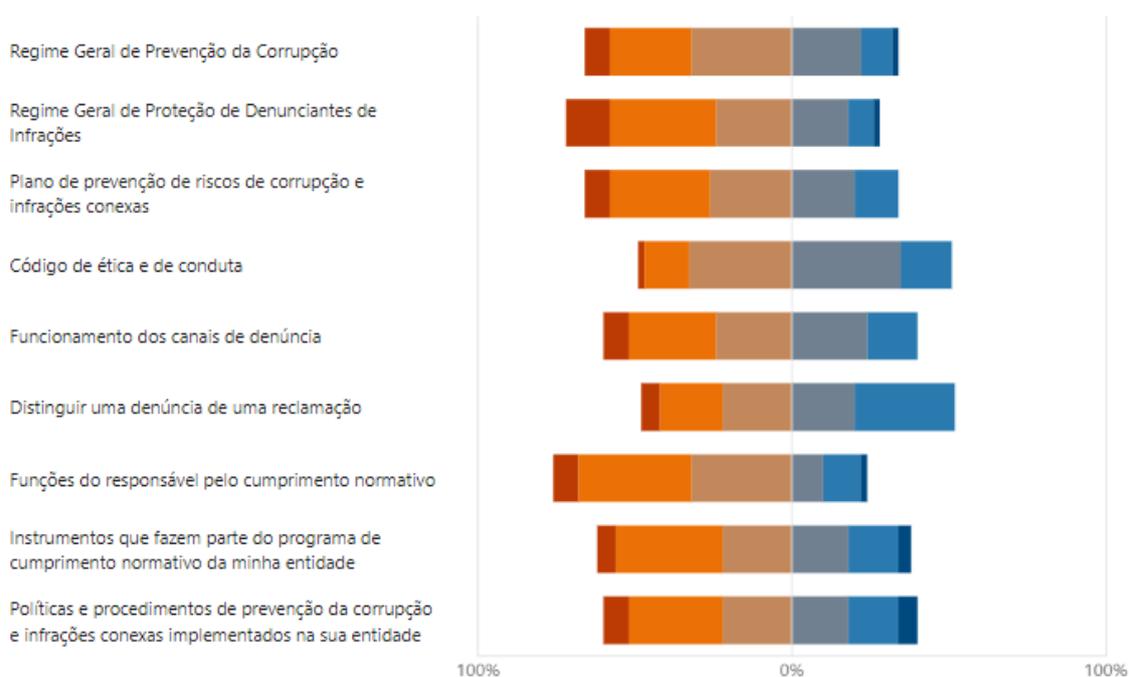


Figura A3.9 Avaliação do grau de conhecimento sobre matérias relacionadas com prevenção da corrupção e denúncias

10. Alguma vez teve formação sobre prevenção da corrupção e infrações conexas?

[Mais Detalhes](#)

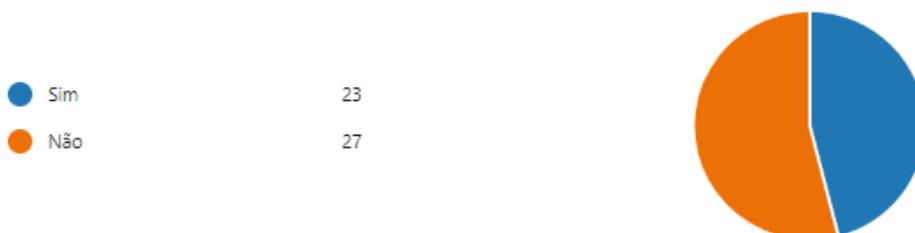


Figura A3.10 N.º de inquiridos com formação sobre prevenção da corrupção e infrações conexas

11. Nos últimos dois anos, quantas horas de formação teve sobre prevenção da corrupção e infrações conexas?

[Mais Detalhes](#)

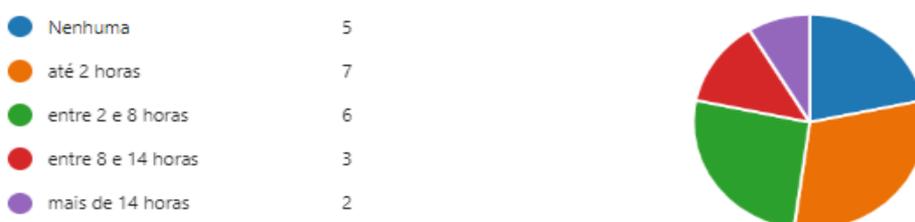


Figura A3.11 Distribuição da formação sobre prevenção da corrupção e infrações conexas

12. Para as seguintes situações, identifique o seu grau de concordância relativamente às que poderão ser objeto de **denúncia**:

[Mais Detalhes](#)

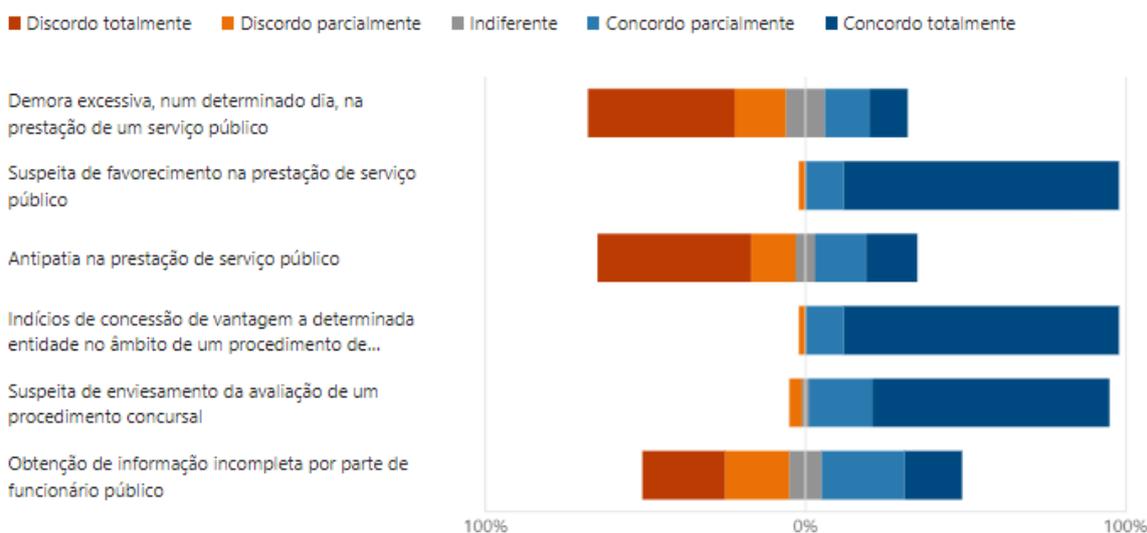


Figura A3.12 Avaliação de situações que podem ser objeto de denúncia

13. Qual o seu grau de confiança relativamente aos canais de denúncia atualmente em vigor?

[Mais Detalhes](#)

Promotores	2
Passivos	15
Detratores	32

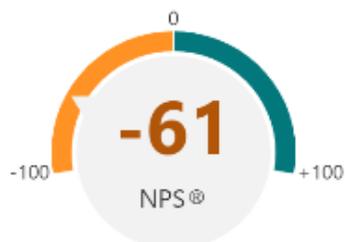


Figura A3.13 Grau de confiança relativamente aos canais de denúncia

14. Alguma vez apresentou uma denúncia sobre uma irregularidade praticada numa organização:

[Mais Detalhes](#)

● Nunca	40
● 1 vez	5
● 2 a 5 vezes	3
● Mais de 6 vezes	2



Figura A3.14 N.º de inquiridos que já apresentaram uma denúncia

15. Relativamente à última denúncia que apresentou:

[Mais Detalhes](#)

● Pública	7
● Privada	3
● Terceiro setor	0



Figura A3.15 Distribuição das entidades sobre as quais incidiu a denúncia

16. Relativamente à última denúncia que apresentou:

[Mais Detalhes](#)

● Nacional	10
● Estrangeira	0



Figura A3.16 Distribuição da nacionalidade das entidades sobre as quais incidiu a denúncia

17. Qual foi o tipo de irregularidade denunciada?

[Mais Detalhes](#)

● Contratação pública;	2
● Serviços, produtos e mercados f...	0
● Segurança e conformidade dos ...	1
● Segurança dos transportes;	0
● Proteção do ambiente;	0
● Proteção contra radiações e seg...	0
● Segurança dos alimentos para c...	0
● Saúde pública;	0
● Defesa do consumidor;	3
● Proteção da privacidade e dos d...	2
● Assédio sexual	0
● Outro	2

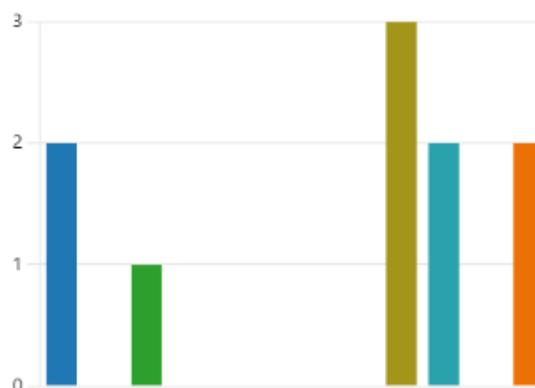


Figura A3.17 Distribuição do tipo de irregularidade denunciada

18. Qual foi o modo de apresentação da denúncia:

[Mais Detalhes](#)

● Por escrito através de plataform...	5
● Verbal através de plataforma ele...	0
● Por escrito, através de carta	1
● Por escrito, através de email	4
● Verbal, através de reunião prese...	0
● Outro	0

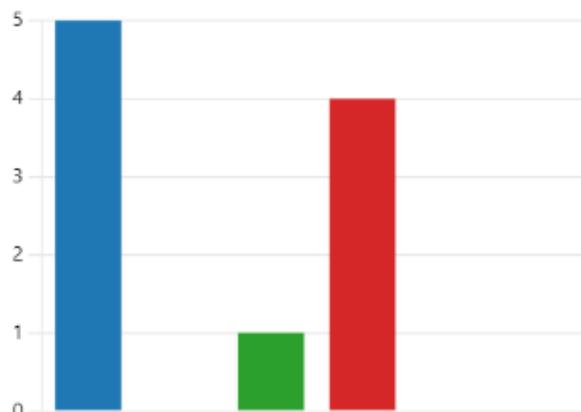


Figura A3.18 Distribuição do modo de apresentação da denúncia

19. Relativamente à denúncia que apresentou, considera que foram cumpridos os seguintes prazos:

[Mais Detalhes](#)

● Prazo de notificação da receção ...	3
● Prazo de comunicação das medi...	2
● Não sabe/ não responde	5



Figura A3.19 Cumprimento dos prazos relativamente à denúncia

20. Teve alguma dificuldade durante o reporte da denúncia?

[Mais Detalhes](#)

● Não	5
● Sim, dificuldade técnica relacion...	3
● Sim, dificuldade técnica relacion...	1
● Outro	1



Figura A3.20 Dificuldades durante o reporte da denúncia

21. Conseguiu ultrapassar a dificuldade sentida durante o reporte da denúncia?

[Mais Detalhes](#)

● Não	4
● Sim, através de ajuda prestada ...	0
● Sim, através de consulta na inter...	1
● Sim, através de um familiar ou a...	0
● Outro	0



Figura A3.21 Conseguiu ultrapassar a dificuldade sentida durante o reporte da denúncia

22. Após ter apresentado a denúncia, sentiu-se protegido de represálias?

[Mais Detalhes](#)

Promotores	1
Passivos	3
Detratores	6

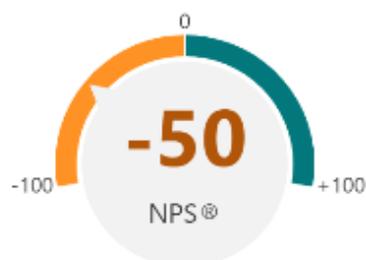


Figura A3.22 Sentimento relativamente a represálias após ter apresentado a denúncia

23. Qual o seu grau de confiança relativamente ao canal de denúncias utilizado?

[Mais Detalhes](#)

Promotores	0
Passivos	4
Detratores	6

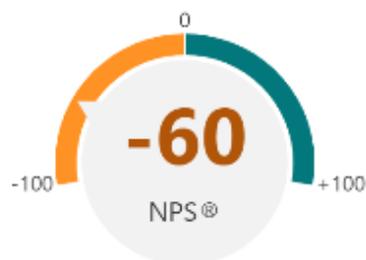


Figura A3.23 Confiança relativamente ao canal de denúncias utilizado

24. Qual o seu grau de confiança relativamente ao desfecho da denúncia efetuada?

[Mais Detalhes](#)

Promotores	1
Passivos	2
Detratores	7

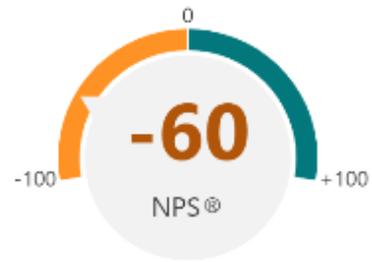


Figura A3.24 Grau de confiança relativamente ao desfecho da denúncia

25. Qual o seu nível de conhecimento relativamente à Inteligência Artificial (IA)?

[Mais Detalhes](#)

Promotores	5
Passivos	17
Detratores	27

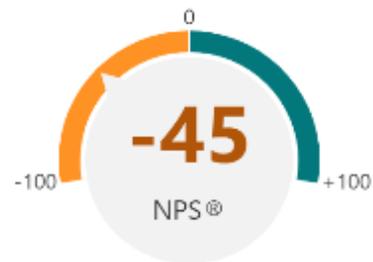


Figura A3.25 Nível de conhecimento relativamente à IA

26. Qual o seu nível de conhecimento relativamente à Interoperabilidade na Administração Pública (iAP)?

[Mais Detalhes](#)

Promotores	6
Passivos	17
Detratores	27

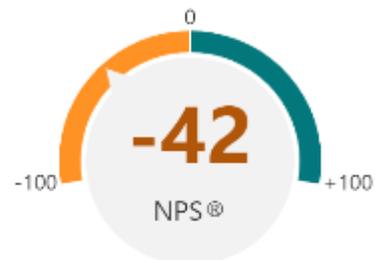


Figura A3.26 Nível de conhecimento relativamente à iAP

27. Considera útil a integração de IA num canal de denúncias, de forma a auxiliar o denunciante no reporte da denúncia, por exemplo, através de um assistente virtual?

[Mais Detalhes](#)



Figura A3.27 Nível de utilidade de IA para auxiliar o reporte da denúncia

28. Considera útil a integração de IA num canal de denúncias, de forma a auxiliar o tratamento de cada denúncia (por exemplo, na fase de triagem) ?

[Mais Detalhes](#)

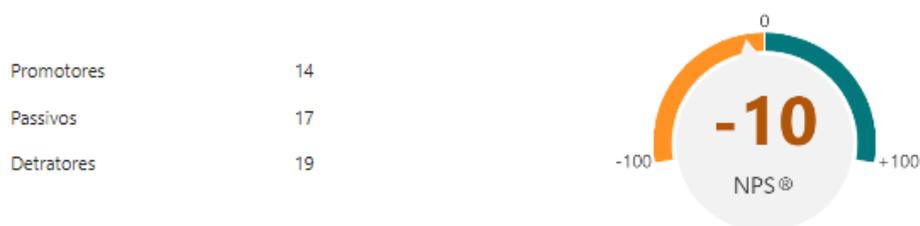


Figura A3.28 Nível de utilidade de IA para auxiliar o tratamento da denúncia

29. Considera útil a integração de interoperabilidade de dados num canal de denúncias, como forma de melhorar a transferência de dados entre entidades?

[Mais Detalhes](#)



Figura A3.29 Nível de utilidade de iAP para melhorar a transferência de dados entre entidades

30. Qual o nível de confiança que teria ao utilizar um canal de denúncias dotado de interoperabilidade?

[Mais Detalhes](#)



Figura A3.30 Nível de confiança relativamente à utilização de um canal de denúncias com iAP

31. Qual o nível de confiança que teria ao utilizar um canal de denúncias dotado de inteligência artificial?

[Mais Detalhes](#)



Figura A3.31 Nível de confiança relativamente à utilização de um canal de denúncias com IA

32. Considera útil a eventual existência de um canal de denúncias único na Administração Pública, dotado de Inteligência Artificial e Interoperabilidade?

[Mais Detalhes](#)



Figura A3.32 Nível de utilidade relativamente à utilização de um canal de denúncias único na AP com IA e iAP

Anexo 4

Quadro A4.1 Distribuição dos contratos por entidades adjudicatárias

Empresa	Nº de contratos	% Nº de contratos	Total PC	Total PC %
Fujitsu Technology Solutions, Lda	2	1,57%	422 170	21,52%
Closer - Consultoria, Lda.	18	14,17%	266 817	13,60%
WIREMAZE- Sistemas de Informação, S.A	19	14,96%	133 487	6,81%
Informa D& B (Serviços de gestão de empresas)	10	7,87%	110 153	5,62%
Wemake, Tecnologias de Informação, Lda	3	2,36%	95 418	4,86%
Link Consulting - Tecnologias de Informação, S.A.	5	3,94%	75 475	3,85%
Master Link - Sistemas de Informação, Lda	1	0,79%	60 900	3,10%
Dnxt Azores, Unipessoal Lda	1	0,79%	58 410	2,98%
CCR - Sociedade de Advogados, SP, RL	3	2,36%	57 440	2,93%
Whistleblower Software ApS	15	11,81%	49 244	2,51%
LCG Consultoria, S.A.	1	0,79%	46 250	2,36%
Deloitte Corporate Finance, S.A.	1	0,79%	43 750	2,23%
Gofox - Tecnologias de Informação, Unipessoal Lda.	4	3,15%	41 280	2,10%
XPAND SOLUTIONS - Informática e Novas Tecnologias Lda	1	0,79%	40 706	2,08%
Whispli SAS	1	0,79%	40 500	2,06%
7Log - Sistemas de Informação, Lda.	1	0,79%	39 348	2,01%
Just Like You, Unipessoal, Lda	3	2,36%	38 118	1,94%
Quidgest Consultores de Gestão S.A.	4	3,15%	34 980	1,78%
JRM - Gabinete de Estudos Técnicos e Informática, Lda.	1	0,79%	28 000	1,43%
HOLOS – Soluções Avançadas e Tecnologias de Informação, SA	1	0,79%	27 100	1,38%
VisionWare - Sistemas de Informação, SA	4	3,15%	25 760	1,31%
WNPC - World Network Projects Campus - Unipessoal, Lda	2	1,57%	22 540	1,15%
PRICEWATERHOUSECOOPERS /AG - ASSESS DE GESTÃO, LDA	1	0,79%	19 800	1,01%
ACIN-ICLOUD SOLUTIONS, LDA	2	1,57%	18 499	0,94%
Dower CMNS - Sociedade de Advogados, SP, RL	1	0,79%	18 000	0,92%
Edilocal Consultores Técnicos, Lda	1	0,79%	16 000	0,82%
Best Privacy Consulting Unipessoal, Lda	1	0,79%	14 800	0,75%
F3M - Information Systems, SA	1	0,79%	14 372	0,73%
Neves Ferreira Rocha Alves & Associados Sociedade de Advogados, SP RL	2	1,57%	13 840	0,71%
JÚDICE GLÓRIA, TABORDA DA GAMA - SOCIEDADE DE ADVOGADOS, SP, RL	1	0,79%	12 500	0,64%
ESTRATEGOR- CONSULTORES DE GESTAO, LDA	2	1,57%	10 380	0,53%
APROVARELATÓRIO - CONSULTORIA E FORMAÇÃO, UNIPESSOAL, LDA	1	0,79%	10 080	0,51%
António Danado, Rita henriques e Associados-Sociedade de Advogados, RL	1	0,79%	9 600	0,49%
CYBERSEC UNIPESSOAL LDA	2	1,57%	9 560	0,49%
SEGI-Engineering Consulting	1	0,79%	6 180	0,32%

Empresa	Nº de contratos	% Nº de contratos	Total PC	Total PC %
Waymotion, Lda	1	0,79%	5 971	0,30%
Direct Hit - Serviços de Apoio a Empresas, Unipessoal, Lda	1	0,79%	5 000	0,25%
CTT SOLUÇÕES EMPRESARIAIS, S.A.	1	0,79%	4 536	0,23%
ALPIBRE, LDA	1	0,79%	4 500	0,23%
Nooperation, Lda	1	0,79%	3 240	0,17%
Codeffect	1	0,79%	2 125	0,11%
ADYTA, LDA.	1	0,79%	2 000	0,10%
Whistleblower Software Aps	1	0,79%	1 398	0,07%
CPS CONSULTORES INFORMATICA, LDA	1	0,79%	1 197	0,06%
Total Geral	127	100,00%	1 961 422	100,00%

Anexo 5

Quadro A5.1 Preço contratual total por CPV

Empresa	Preço contratual total	%
Serviços técnicos	291 870	14,88%
Serviços de TI: consultoria, desenvolvimento de software, Internet e apoio	282 187	14,39%
Serviços de fornecimento de software	158 854	8,10%
Serviços de assistência técnica informática	158 300	8,07%
Pacotes de software e sistemas de informação	142 262	7,25%
Serviços de consultoria em matéria de sistemas	74 580	3,80%
Plataformas informáticas	70 886	3,61%
Pacote de software para sectores específicos	63 712	3,25%
Serviços de desenvolvimento de software para bases de dados	60 900	3,10%
Serviços relacionados com software	51 393	2,62%
Pacote de software e sistemas informáticos diversos	49 600	2,53%
Serviços a empresas: direito, comercialização, consultoria, recrutamento, impressão e segurança	49 235	2,51%
Serviços de desenvolvimento de software à medida	37 030	1,89%
Serviços relacionados com a gestão	34 940	1,78%
Serviços de assessoria jurídica	33 100	1,69%
Pacote de software para criação de documentos	27 720	1,41%
Serviços de manutenção de sistemas	25 380	1,29%
Serviços de implementação de software	22 728	1,16%
Pacote de software para edição de páginas Web	22 540	1,15%
Serviços relacionados com a informática	21 250	1,08%
Serviços de actualização informática	19 800	1,01%
Serviços de investigação e desenvolvimento e serviços de consultoria conexos	18 000	0,92%
Outros serviços	17 480	0,89%
Serviços de hospedagem para operação de sítios da World Wide Web (WWW)	16 967	0,87%
Serviços de manutenção e reparação de software	16 252	0,83%
Serviços técnicos de análise ou consultoria	16 231	0,83%
Serviços públicos	14 372	0,73%
Serviços de formação	14 099	0,72%
Pacote de software para gestão de sistemas, de armazenamento e de conteúdos	13 991	0,71%
Pacote de software de segurança	13 948	0,71%
Serviços de desenvolvimento de software para interconectividade de plataformas	10 869	0,55%
Serviços de gestão de dados	10 080	0,51%
Serviços de apoio a sistemas	9 955	0,51%
Serviços relacionados com a administração pública	9 600	0,49%
Serviços de Internet	8 494	0,43%
Serviços de consultoria em matéria comercial e de gestão e serviços conexos	7 628	0,39%
Serviços de consultoria em matéria de concepção	6 520	0,33%
Serviços de consultoria e de programação de software	6 040	0,31%
Sistema de gestão de documentos	6 000	0,31%
Serviços de desenvolvimento de software para melhoria de sistemas operativos	5 971	0,30%
Serviços de transferência eletrónica de dados	5 820	0,30%
Serviços de informática prestados por profissionais	4 995	0,25%

Empresa	Preço contratual total	%
Serviços relacionados com dados	4 800	0,24%
Serviços de fornecimento	4 500	0,23%
Serviços de desenvolvimento de aplicações para clientes de Internet ou intranet	4 350	0,22%
Pacote de software para sistemas operativos em rede	4 300	0,22%
Serviços de consultoria financeira	3 860	0,20%
Manutenção de software para as tecnologias da informação	2 360	0,12%
Pacote de software para segurança de dados	2 125	0,11%
Serviços de informação eletrónica	1 867	0,10%
Licenças	1 680	0,09%
Total	1 961 422	100,00%