INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

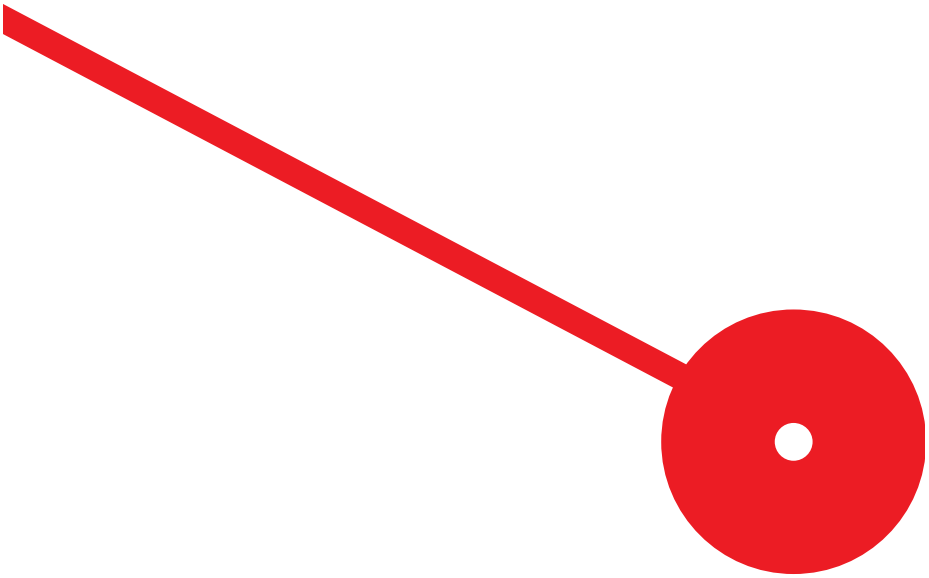
M MESTRADO
AUDITORIA

A Auditoria no Combate à Fraude Eletrónica: instrumentos de apoio

Ana Rafaela Santos de Jesus

Esta versão contém as críticas e sugestões dos elementos do júri

12/2022



Ana Rafaela Santos de Jesus. A Auditoria no Combate à Fraude Eletrónica: instrumentosde apoio. 12/2022

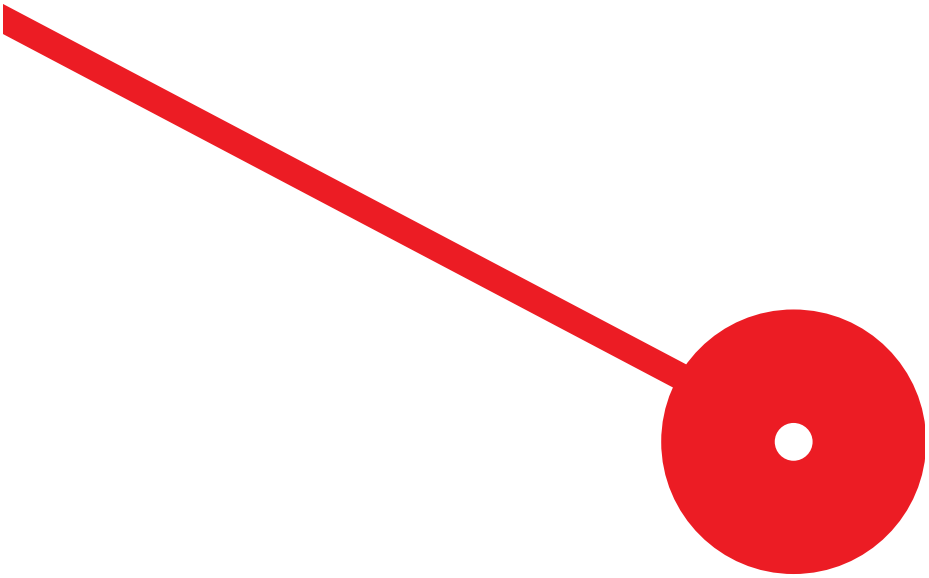
INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

M MESTRADO
AUDITORIA

A Auditoria no Combate à FraudeEletrónica: instrumentos de apoio

Ana Rafaela Santos de Jesus

Dissertação de Mestrado apresentado ao Instituto Superior de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Auditoria, sob orientação da Professora Doutora Susana Adelina Moreira Carvalho Bastos.



Ana Rafaela Santos de Jesus. A Auditoria no Combate à Fraude Eletrónica: instrumentosde apoio.
12/2022

Agradecimentos

O desenvolvimento desta dissertação de Mestrado foi possível devido à participação e influência de várias pessoas, que estiveram ao meu lado e me apoiaram incondicionalmente e a quem devo um especial reconhecimento:

À minha orientadora, Professora Doutora Susana Bastos por ter aceite este desafio, por todo o apoio, disponibilidade e suporte prestado ao longo deste projeto;

A todas as pessoas que estiveram envolvidas nesta investigação, nomeadamente, ao Diretor da Unidade de Perícia Financeira e Contabilística da Polícia Judiciária, Dr. Orlando Mascarenhas, por ter partilhado os seus sábios conhecimentos e também, aos utentes do Centro de Dia de Mafamude, pela vossa simpatia e boa vontade.

Aos meus amigos e colegas de curso, que me acompanharam ao longo do meu percurso académico e nunca me deixaram desistir.

À minha família por ser o meu suporte em todos os desafios da minha vida.

A todos, um enorme obrigada.

Resumo

Com a crescente utilização das tecnologias de informação e comunicação (TIC), a fraude eletrónica tem vindo a aumentar de forma expressiva. O facto de termos vivido recentemente uma pandemia mundial, potenciou ainda mais, a utilização da internet e dos meios de comunicação e, consequentemente, levou ao aumento dos casos de fraude eletrónica em Portugal.

O objetivo desta dissertação é o de analisar a ocorrência da fraude eletrónica no contexto social e demográfico em Portugal, compreender as medidas já implementadas pelos organismos especializados e perceber que práticas podem ser adotadas além das que existem, de modo a aumentar a segurança dos utilizadores tecnológicos.

A escolha da metodologia de investigação a utilizar recaiu no método misto, ou seja, na combinação dos métodos quantitativo e qualitativo, uma vez que foram utilizados questionários e entrevistas como instrumentos de recolha de dados. Estes instrumentos mostraram-se mais pertinentes para o estudo.

Para colmatar o crescimento do crime eletrónico é imprescindível a atuação dos diversos organismos especializados na investigação, no combate e no apoio às vítimas de fraudes eletrónicas. Contudo, estes organismos não são suficientes, é necessário agir socialmente, através da educação e formação de todos os cidadãos, para que estes sejam capazes de adotar comportamentos ciber-resilientes, de modo a garantir ao utilizador uma maior capacidade para identificar e atuar perante situações em que a sua segurança online possa estar em risco.

Palavras-chave: Burlas, Educação, Fraude Eletrónica, Prevenção e Deteção

Abstract

With the growing use of information and communication technologies (ICT), electronic fraud has been increasing significantly. The fact that we have recently experienced a worldwide pandemic has further boosted the use of the Internet and the means of communication and, consequently, led to an increase in cases of electronic fraud in Portugal.

The aim of this dissertation is to analyze the occurrence of electronic fraud in the social and demographic context in Portugal, to understand the measures already implemented by specialized bodies and to understand what practices can be adopted in addition to those that exist, to increase the security of technological users.

The choice of the research methodology to be used fell into the mixed method, i.e., the combination of quantitative and qualitative methods, as surveys and interviews were used as data collection tools. These instruments proved to be more pertinent to the study.

In order to counteract the growth of electronic crime, it is essential that the various specialized bodies act to investigate, combat and support the victims of electronic fraud. However, these bodies are not enough, it is necessary to act socially, through education and training of all citizens, so that they are able to adopt cyber-resilient behaviors, in order to ensure that users are better able to identify and act in situations where their online security may be at risk.

Key words: Fraud, Education, Electronic Fraud, Prevention and Detection

Índice

Índice de Figuras

Índice de Tabelas

Índice de Gráficos

Lista de Abreviaturas

APAV – Associação Portuguesa de Apoio à Vítima

ATM - *Automated Teller Machine*

CEO - *Chief Executive Officer*

DESI - *Digital Economy & Society Index*

DF's – Demonstrações Financeiras

DNS - Sistema de Nomes de Domínio ou *Domain Name System*

DS-PQA – Direção de Serviços de Planeamento, Qualidade e Avaliação

FCT- Fundação para Ciência e a Tecnologia

ISA – *International Standard on Auditing*

PJ – Polícia Judiciária

RASI - Relatório Anual de Segurança Interna

SIAD - Sistema Integrado de Apoio à Distância

SMS – *Short Message Service*

TIC – Tecnologias de Informação e Inovação

UE – União Europeia

UPFC – Unidade de Perícia Financeira e Contabilística

URL - *Uniform Resource Locator* ou Localizador Uniforme de Recurso

CAPÍTULO – INTRODUÇÃO

Introdução

Fruto da evolução e massificação no uso das Tecnologias de Informação e Comunicação e da crescente globalização económica, o mundo está conectado em tempo real e o acesso a todo o tipo de transaçõesde comércio internacional encontra-se à distância de um simples *"click"*.

Esta realidade apresenta vantagens significativas, mas também desvantagens no que à tecnologia e à informação eletrónica concerne. Nos últimos anos, as fraudes eletrónicas têm vindo a subir drasticamente.

A população mais jovem apresenta índices elevados de utilização intensiva das TIC e da Internet, mais concretamente das redes sociais, o que resulta numa maior vulnerabilidade à cibervitimação, em comparação com utilizadores mais velhos e com utilizadores menos frequentes.

Todos os cidadãos deveriam estar devidamente instruídos relativamente à utilização segura das TIC e do seu suporte às compras eletrónicas para não serem potenciais vítimas de burlas e, tal não acontece, registando-se cada vez mais um aumento dos roubos eletrónicos.

Para combater este tipo de fraude, é necessária a atuação de diversos organismos especializados, que procuram não só detetar, mas essencialmente, prevenir qualquer tipo de fraude que possa ocorrer no seio organizacional, bem como a título singular.

Este trabalho procura analisar a ocorrência da fraude eletrónica no contexto social e demográfico em Portugal, compreender as medidas já implementadas pelos organismos especializados e perceber que práticas podem ser adotadas além das que existem, de modo a aumentar a segurança dos utilizadores tecnológicos.

No que concerne à estruturação da dissertação, no capítulo I será apresentada a revisão da literatura, onde serão abordadas as diversas perspetivas nas temáticas de auditoria forense, de fraude e de burlas eletrónicas. No capítulo II, irão ser abordadas as metodologias de investigação, em que se apresenta a linha de investigação para este estudo, tendo por base as questões de investigação apresentadas na revisão da literatura. Ainda, neste capítulo é realizada uma contextualização ao nível da população no sentido de perceber a atual estrutura populacional no nosso país.

No decorrer deste estudo foi possível perceber qual a faixa etária que apresenta uma

maior vulnerabilidade às burlas eletrónicas, quais as modalidades de crime eletrónico mais frequentes, a relação entre o nível de literacia tecnológica e a fraude eletrónica (a uma elevada literacia digital está associado o aumento de comportamentos ciber-resilientes) e, por fim, a importância da Auditoria Forense no combate a este tipo de fraude, pela sua deteção e prevenção.

CAPÍTULO I – REVISÃO DA LITERATURA

Revisão da Literatura

1 Auditoria

1.1 Conceito de Auditoria

A Auditoria consiste num exame cuidadoso e sistemático das atividades desenvolvidas em determinada organização, cujo objetivo é averiguar se estas estão de acordo com o planeamento estabelecido previamente, se foram implementadas com eficácia e se são adequadas à consecução dos objetivos.

Segundo Crepaldi (2020), pode-se definir auditoria como o levantamento, estudo e avaliação sistemática das transações, procedimentos, operações, rotinas e das demonstrações financeiras de uma entidade.

1.2 Tipos de Auditoria

A auditoria apresenta várias classificações, para este estudo, importa a auditoria externa e auditoria interna.

A auditoria interna é o exame de investigação dos processos empresariais realizadas por um profissional próprio da organização, enquanto a auditoria externa é realizada por um profissional que não possui vínculos com a empresa.

Existem vários tipos de auditoria, nomeadamente, auditoria financeira, fiscal, tributária, ambiental, de qualidade, forense, entre outros. Iremos e para efeitos da presente investigação aprofundar o conceito de auditoria forense.

2 Auditoria Forense

2.1 Conceito de Auditoria Forense

Existem várias definições de Auditoria Forense segundo estudos realizados por diversos autores.

Tapia (2010), defende que a Auditoria Forense consiste numa técnica executada através da investigação de atos conscientes e voluntários de contornar a legislação aplicável e, consequentemente, adotar práticas de fraude.

Geralmente, neste ramo existem equipas multidisciplinares integradas por especialistas nas áreas da contabilidade, direito, caligrafia e engenharia da computação.

Este tipo de auditoria é muito relevante no que respeita à obtenção de provas de suporte para os departamentos de investigação policial, fiscal e esclarecimento judicial acerca de

quaisquer atos ilícitos ou crimes praticados por terceiros.

A Auditoria Forense ganhou força em Portugal, quando o diretor do Banco de Portugal anunciou em 2014, que tinha solicitado a realização de uma Auditoria Forense ao Banco Espírito Santo. Até essa altura, era um ramo da auditoria desconhecido da população em geral.

A Auditoria Forense é definida pelo Banco de Portugal como *"um instrumento complementar de supervisão que visa confirmar o cumprimento rigoroso das matérias que se inscrevam nas competências do Banco de Portugal"* (Jornal de Negócios, 2014)

2.2 Objetivos de Auditoria Forense

Segundo Tapia (2010), a Auditoria Forense apresenta como objetivos:

- Identificar e demonstrar a fraude cometida pelo criminoso;
- Prevenir e reduzir a fraude através da implementação de recomendações para o reforço das medidas de controlo interno propostas pelo auditor;
- Participar no desenvolvimento de programas de prevenção de perdas e fraude;
- Participar na avaliação dos sistemas e estruturas de controlo interno;
- Reunir provas utilizando as técnicas de investigação forenses;
- No caso de organizações não governamentais, fornecer apoio técnico através das evidências de suporte aos órgãos do Ministério Público e judiciais, para investigação de crimes e aplicação das respetivas punições, entre outros.

2.3 Tipos de Auditoria Forense

Tapia (2010), diferencia a Auditoria Forense em dois tipos: Auditoria Forense Preventiva e Auditoria Forense Detetiva.

A primeira, tal como a própria palavra indica, preocupa-se em prevenir, impedir, detetar e implementar ações contra a fraude, através de avaliações e pareceres emitidos às organizações, que lhes permite tomar medidas e decisões no presente para evitar fraudes no futuro. São exemplos de medidas preventivas, os sistemas de alerta quando ocorrem irregularidades e os programas de controlo antifraude.

A segunda consiste em identificar, numa situação concreta, a ocorrência de fraude através de uma investigação minuciosa de forma a identificar a quantidade dos efeitos (diretos e indiretos) das fraudes efetuadas, os presumíveis criminosos e a cumplicidade

que poderá estar por detrás do ato criminoso. A Auditoria Forense serve de auxílio à justiça, que é o órgão incumbido da análise, julgamento e condenação dos atos criminais.

3 Fraude

3.1 Conceito de Fraude

De acordo com o Direito Penal, podemos classificar a palavra "fraude" como sendo o crime ou ofensa de deliberadamente enganar outros com o propósito de os prejudicar, normalmente, para obter propriedade ou serviços injustamente.

Segundo a *International Standard on Auditing* (ISA) 240 (p. 260), a fraude é definida como *"Um ato intencional praticado por um ou mais indivíduos de entre a gerência, encarregados da governação, empregados ou terceiros, envolvendo o uso propositado de falsidades para obter uma vantagem injusta ou ilegal"*. Refere ainda, que a fraude se distingue do erro se a ação subjacente, que resulta na distorção das demonstrações financeiras, foi intencional ou não intencional. A grande preocupação do auditor é se essa distorção intencional dá origem a uma distorção material nas Demonstrações Financeiras (DF's). A ISA 240 refere que existem dois tipos de distorções materiais intencionais quando detetadas pelo auditor: distorções resultantes de relato financeiro fraudulento e distorções resultantes de apropriação.

A fraude assume várias formas, nomeadamente fraude de correspondência, através dos meios das tecnologias de informação, fraude por telefone e fraude por internet. De seguida, apresentamos alguns exemplos de fraude:

- **Roubo de identidade:** furto de identidade online, quer os dados pessoais da vítima sejam obtidos através da Internet, ou por outro meio, mas transferidos através da Internet ou usados para cometer um crime pela Internet.

- **Falsificação de documentos ou assinaturas:** *"Quem, com intenção de causar prejuízo a outra pessoa ou ao Estado, de obter para si ou para outra pessoa benefício ilegítimo, ou de preparar, facilitar, executar ou encobrir outro crime: fabricar ou elaborar documento falso, ou qualquer dos componentes destinados a corporizá-lo; falsificar ou alterar documento ou qualquer dos componentes que o integram; abusar da assinatura de outra pessoa para falsificar ou contrafazer documento; fizer constar falsamente de documento ou de qualquer dos seus componentes facto juridicamente relevante; usar documento a que se referem as alíneas anteriores; ou por qualquer meio, facultar ou detiver*

documento falsificado ou contrafeito…" (Artigo 256.º Código Penal).

- **Publicidade enganosa**: crime ou má conduta de publicar, transmitir ou de outra forma fazer circular publicamente um anúncio com declarações falsas, errôneas ou enganosas, feita de forma intencional ou imprudente para promovera venda de propriedades, bens ou serviços ao público.

- **Fraude nigeriana:** realizada principalmente por correio eletrónico, onde o fraudador tenta convencer o fraudado a pagar quantias cada vez mais elevadas na tentativa de obter um ganho superior.

- **Esquemas em pirâmide:** operações fraudulentas de investimento, baseadas na promessa de pagamentos de lucros anormalmente elevados aos investidores, com recurso, exclusiva ou maioritariamente, aos capitais dos investidores subsequentes e não a fundos gerados pela atividade.

3.2 Árvore da Fraude

A Árvore da Fraude consiste num estudo desenvolvido por Wells (2007) que tem como objetivo identificar as fraudes e os abusos ocupacionais.

Este autor agrupa a fraude em 3 categorias:

1. **Apropriação indevida de ativos:** envolve mais do que o furto ou o desfalque, envolve o uso indevido de qualquer bem da empresa para benefício pessoal. Pode-se verificar através de duas formas de apropriação: dinheiro, que se subdivide em três meios (furto, desembolsos fraudulentos e sonegação) e inventários e os outros ativos.
2. **Corrupção:** consiste na utilização do poder para favorecer o próprio ou terceiros. Este tipo de fraude divide-se em quatro subcategorias: conflito de interesses, suborno, gratificações ilegais e extorsão económica. O conflito de interesses fomenta o favorecimento pessoal ou de um terceiro, através do desenvolvimento de esquemas de compras ou de vendas. Relativamente ao suborno, este representa a prática de oferecer dinheiro ou benefícios a um ou mais indivíduos, em troca de um ato ilícito de modo a obter vantagens. No caso das gratificações ilegais, estas constituem uma recompensa paga, de forma ilícita, pela realização de um determinado serviço. Por fim, a extorsão económica corresponde à obtenção de vantagens por parte de outrem, com recurso à chantagem, coação ou violência.
3. **Relatórios de contas fraudulentos:** caracterizam-se pelo facto de as informações financeiras divulgadas apresentarem distorções, com a finalidade de induzir os

seus utilizadores financeiros em erro. Estes relatórios podem ser financeiros e não financeiros. Caso se trate de relatórios financeiros, poderão estar evidenciadas, por exemplo, sobrevalorizações ou subvalorizações de ativos e receitas. A nível dos relatórios não financeiros verifica-se a possibilidade de falsificação de documentos organizacionais, quer internos quer externos.

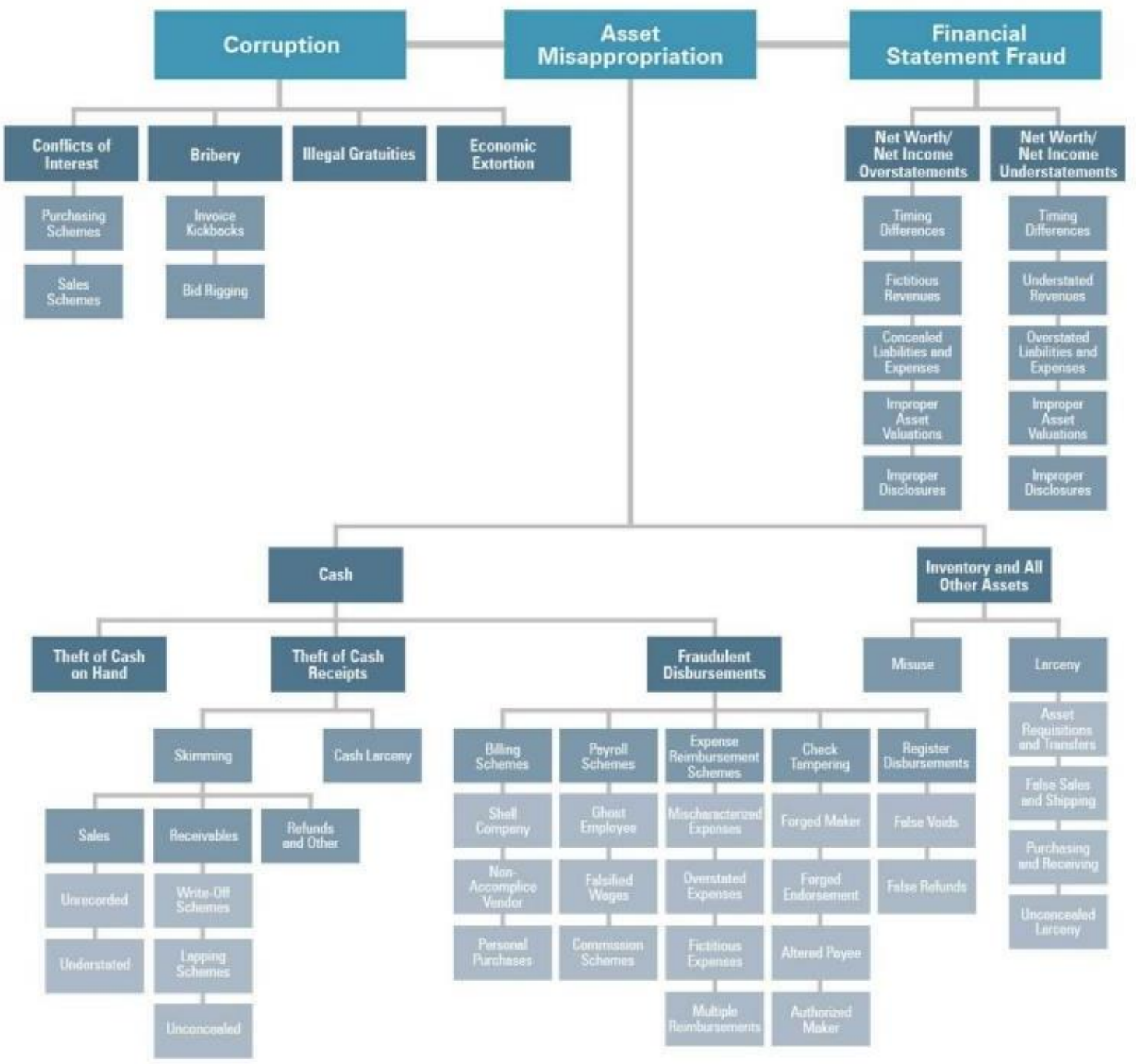


Figura 1: Árvore da Fraude

Fonte: ACFE (2014); *Report to the Nation on Occupational Fraude & Abuse*

3.3 Pentágono da Fraude

Renato Santos (2016) criou o modelo designado por "Pentágono da Fraude" com base no Triângulo da Fraude de Cressey (1953) e no Diamante da Fraude de Wolfe e Hermanson (2004).

O Triângulo da Fraude baseia-se em três pilares: pressão, oportunidade e racionalização. O "Diamante da Fraude" baseia-se nos três pilares referidos anteriormente e, ainda no da capacidade.

O Pentágono da Fraude decompõe-se nos quatro pilares acima referidas do Diamante da Fraude, onde acresce mais uma, a disposição ao risco.

Este modelo assenta em cinco aspetos que levam os indivíduos a cometerem atos fraudulentos.

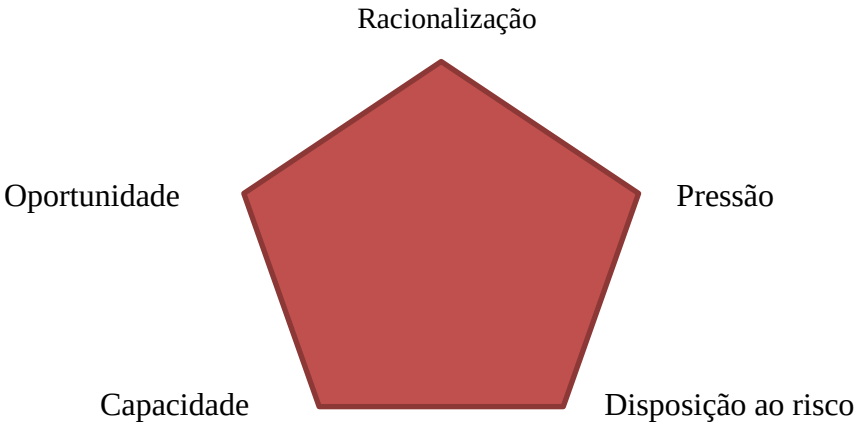


Figura 2: Pentágono da Fraude

Fonte: Elaboração própria, 2022

1. **Oportunidade:** para cometer uma fraude, é necessário que o indivíduo tenha uma oportunidade de estar envolvido em alguma situação no interior da organização, da qual consiga tirar benefícios através da adoção do ato de fraude.
2. **Pressão:** o indivíduo encontra-se sob pressão, seja esta exercida pela empresa ou pelo próprio, o que o leva a considerar o caminho da fraude como a solução mais imediata.
3. **Racionalização:** o fraudulento procura justificar o seu ato criminoso e racionalizar que vai cometer efetivamente um crime, abdicando dos seus valores pessoais e organizacionais.

4. **Capacidade:** é necessário existir um certo conhecimento organizacional, nomeadamente dos controlos, para pensar em executar fraude, e que esta seja realizada com sucesso.
5. **Disposição ao risco:** é preciso estar disposto a correr o risco de cometer a fraude e ser descoberto. Embora reconheça essa possibilidade, o fraudador aceita e assume esse risco, apesar de saber que pode ser descoberto a qualquer momento.

4 Burlas Eletrónicas

4.1 Conceito de Burlar

Burlar significa enganar ou praticar fraude em qualquer sistema, ou ainda lesar ou ludibriar alguém. Uma das burlas mais frequentes são as burlas eletrónicas, devido ao grande avanço das tecnologias e à consequente utilização das mesmas.

4.2 Burlas Eletrónicas

De acordo com a Associação Portuguesa de Apoio à Vítima (APAV), em contexto online e a título singular, as burlas com maior expressão em termos estatísticos e aquelas que causam um maior dano patrimonial às suas vítimas são: burlas no comércio eletrónico, burlas bancárias e as burlas nos relacionamentos amorosos **(***romance scams***)**.

Entre 2020 e 2024, são esperadas perdas de cerca de 200 mil milhões de euros por burlas realizadas no comércio eletrónico, de acordo com um estudo realizado pela APAV.

4.2.1 Burlas no Comércio Eletrónico (e-commerce)

De acordo com a APAV, as burlas no comércio eletrónico apresentam diferentes graus de complexidade: desde esquemas mais simples, nos quais é prometido ao comprador o envio de certo artigo pelo correio mediante transferência bancária, o qual acaba por não ser recebido; até esquemas mais elaborados, que muitas vezes envolvem a falsificação de documentos, como comprovativos de transferências bancárias, exploração de vulnerabilidades em *websites* de compras *online* que armazenam dados bancários dos utilizadores (cartões de crédito ou débito), sendo estes depois usados pelos criminosos para colocar à venda na *darkweb* ou para fazer transações bancárias com desconhecimento das vítimas *(card not present fraud)*, ou o s*kimming*, que consiste na cópia da banda magnética de um cartão de pagamento, sem o conhecimento ou consentimento do titular do cartão, o que geralmente ocorre quando o cartão de pagamento está a ser utilizado pelo titular numa caixa multibanco ou num terminal de ponto de venda.

4.2.2 Burlas Bancárias

A burla bancária centra-se sobretudo nos ataques de *phishing*, de que podem ser alvo tanto particulares como empresas. Nestes casos é importante referir que, regra geral, nos e-mails ou *Short Message Service* (SMS) de *phishing* a pessoa é levada a clicar num *link* que pensa ser da sua entidade bancária, sendo conduzida a um *website* que está desenhado para parecer o da entidade bancária. O desenho deste *website* é realizado com o recurso a uma técnica denominada de *pharming*, que em informática é o termo atribuído ao ataque baseado na técnica *Domain Name System* (DNS) *cache poisoning* (envenenamento de cache DNS), que consiste em corromper o DNS numa rede de computadores, fazendo com que o *Uniform Resource Locator* (URL) de um site passe a apontar para um servidor diferente do original.

Recentemente têm vindo a verificar-se outro tipo de ataques a sistemas bancários, nomeadamente a máquinas *Automated Teller Machine* (ATM), através de um processo denominado de *jackpotting*, que pode ocorrer de duas formas distintas: seja através da introdução de *malware* no sistema informático da máquina ATM ou então através da ligação de um *hardware* denominado de "*Black-Box*", que é ligado diretamente ao ATM. O objetivo do *jackpotting* é levar as máquinas multibanco a emitirdinheiro que têm em caixa, através do comando do criminoso.

4.2.3 Burlas nos Relacionamentos Amorosos *(Romance Scams)*

As burlas nos relacionamentos amorosos acontecem quando o criminoso consegue, de uma forma eficaz, fingir estabelecer uma relação de confiança e de intimidade com a vítima, como forma de a burlar. Os atos fraudulentos podem envolver acesso ao dinheiro da vítima, contas bancárias, cartões de crédito, passaportes, contas de e-mail ou números de identificação nacional, ou, ainda, forçando as vítimas a cometer crimes em nome do agressor.

4.3 Organismos de Combate às Burlas

4.3.1 Unidade de Perícia Financeira e Contabilística (UPFC)

A Polícia Judiciária (PJ) procura desenvolver e promover as ações de prevenção, deteção e investigação criminal da sua competência ou que lhe sejam cometidas pela Lei de Segurança Interna, pela Lei-Quadro da Política Criminal e pelas estratégias nacionais que definem os objetivos, as prioridades e as orientações de política criminal e realizar, enquanto entidade oficial, perícias e exames.

Dentro da PJ existe a UPFC que se dedica à análise das fraudes eletrónicas.

Compete à UPFC:

- Realizar perícias, exames e análises de natureza financeira, contabilística, fiscal e bancárias, ordenadas pelas autoridades judiciárias e de polícia criminal;
- Prestar assessoria técnica aos serviços de investigação criminal e às autoridades judiciárias nas ações de recolha e análise de documentos e outros meios de prova;
- Coadjuvar as autoridades judiciárias nas fases de questionário, instrução e julgamento, no âmbito das suas competências;
- Manter, em articulação com a Direção de Serviços de Planeamento, Qualidade e Avaliação (DS-PQA), um sistema de gestão de qualidade, visando a acreditação junto das respetivas autoridades oficiais competentes.

4.3.2. Associação Portuguesa de Apoio à Vítima (APAV)

A Associação Portuguesa de Apoio à Vítima (APAV) é uma instituição particular de solidariedade social, pessoa coletiva de utilidade pública, que tem como objetivo estatutário promover e contribuir para a informação, proteção e apoio aos cidadãos vítimas de infrações penais.

É, em suma, uma organização sem fins lucrativos e de voluntariado, que apoia, de forma individualizada, qualificada e humanizada, vítimas de crimes, através da prestação de serviços gratuitos e confidenciais.

Fundada em 25 de junho de 1990, é uma instituição de âmbito nacional, localizando-se a sua sede em Lisboa.

Para a realização do seu objetivo, a APAV propõe-se, nomeadamente: promover a proteção e o apoio a vítimas de infrações penais, em particular às mais carenciadas, designadamente através da informação, do atendimento personalizado e encaminhamento, do apoio moral, social, jurídico, psicológico e económico; colaborar com as competentes entidades da administração da justiça, polícias, de segurança social, da saúde, bem como as autarquias locais, regiões autónomas e outras entidades públicas ou particulares; incentivar e promover a solidariedade social, designadamente através da formação e gestão de redes de cooperadores voluntários e do mecenato social, bem como da mediação vítima-infrator e outras práticas de justiça restaurativa; fomentar e patrocinar a realização de investigação e estudos sobre os problemas da vítima, para a mais adequada satisfação dos seus interesses; promover e participar em programas, projetos e ações de informação e sensibilização da opinião pública; contribuir para a adoção de medidas legislativas, regulamentares e

administrativas, facilitadoras da defesa, proteção e apoio à vítima de infrações penais, com vista à prevenção dos riscos de vitimização e atenuação dos seus efeitos e estabelecer contactos com organismos internacionais e colaborar com entidades que em outros países prosseguem fins análogos.

O *Data Detox Kit*, ou *Data Detox x Youth*, é um livro de atividades para ajudar os jovens acontrolar a sua tecnologia. Este é um *kit* de ferramentas interativo que pretende incentivar os jovens a pensarem sobre diferentes aspetos das suas vidas digitais, desde os seus perfis nas redes sociais às *passwords*, com atividades simples para reflexão e diversão.

Este *kit* está dividido em quatro secções: Privacidade Digital, Segurança Digital, Bem-estar digital e Desinformação, e tem como principais destinatários jovens que já possuem os seus próprios dispositivos, mas pode ser utilizado por pessoas de todas as idades.

Este mecanismo foi criado pela *Tactical Tech*, e foi traduzido para português pela APAV, estando disponível o seu *download* no site da APAV. Integra o Projeto Internet Segura, cujas entidades parceiras são o Centro Nacional de Cibersegurança, a Direção Geral da Educação, o Instituto Português do Desporto e da Juventude, a Fundação para a Ciência e Tecnologia, a Associação Portuguesa de Apoio à Vítima, a Fundação Altice Portugal e a Microsoft. O projeto é cofinanciado pela União Europeia (UE), pelo Mecanismo Interligar a Europa.

A APAV dispõe de um serviço de atendimento telefónico e *online* sobre questões relacionadas com o uso de plataformas e tecnologias *online*. A Linha Internet Segura, passa assim a ser um apoio específico do *Integrated Distance Support* System (L) da APAV, que irá assegurar o apoio anónimo e confidencial, ao uso das tecnologias *online* cobrindo todos os assuntos relativos à utilização das mesmas. A integração da Linha Internet Segura no SIAD assegura ainda uma resposta articulada com os serviços de proximidade da APAV.

Os objetivos da Linha Internet Segura são:

- Prestar apoio telefónico ou *online*, de forma anónima e confidencial, dispondo de um sistema para remeter ocorrências graves às autoridades competentes quando uma criança parecer estar em perigo;
- Analisar, discutir e fornecer resultados que contribuam para as estratégias de sensibilização na área da Internet Segura.

Na prossecução de um atendimento de melhor qualidade e maior abrangência, a Linha Internet Segura conta com o apoio de várias entidades para encaminhamento e seguimento de contactos cuja resposta integrada no SIAD, permite que a cada situação seja dada uma resposta conjugada tanto com os serviços de proximidade da APAV, comocom os sistemas de referenciação protocolados entre a APAV e as entidades parceiras.

A Linha Internet Segura integra também um serviço de denúncia de conteúdos ilegais *online* onde são disponibilizados um conjunto de meios através dos quais, e de forma totalmente anónima, é possível apresentar denúncias de conteúdos eventualmente ilegais. As denúncias recebidas são triadas e analisadas por operadores especializados que lhes dão o devido seguimento: autoridade policial nacional ou congénere internacional.

5 Monitorização da Segurança Interna em Portugal

5.1 Conselho Superior de Segurança Interna

O Conselho Superior de Segurança Interna é o órgão interministerial de audição e consulta em matéria de segurança interna.

De acordo com o Artigo 12.º da Lei nº 53/2008, *"o Conselho Superior de Segurança Interna é presidido pelo Primeiro-Ministro e dele fazem parte: os Vice-Primeiros-Ministros, se os houver; os Ministros de Estado e da Presidência, se os houver; os Ministros da Administração Interna, da Justiça, da Defesa Nacional, das Finanças e das Obras Públicas, Transportes e Comunicações; os Presidentes dos Governos Regionais dos Açores e da Madeira; os Secretários-Gerais do Sistema de Segurança Interna e do Sistema de Informações da República Portuguesa; o Chefe do Estado-Maior-General das Forças Armadas; dois deputados designados pela Assembleia da República por maioria de dois terços dos deputados presentes, desde que superior à maioria absoluta dos deputados em efetividade de funções; os comandantes-gerais da Guarda Nacional Republicana e da Polícia Marítima, os diretores nacionais da Polícia de Segurança Pública, da Polícia Judiciária e do Serviço de Estrangeiros e Fronteiras e os diretores do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança; a Autoridade Marítima Nacional; a Autoridade Aeronáutica Nacional; a Autoridade Nacional de Aviação Civil; o presidente da Autoridade Nacional de Proteção Civil; o diretor-geral de Reinserção e Serviços Prisionais; o coordenador do Centro Nacional de Cibersegurança; o diretor-geral da Autoridade Tributária e Aduaneira."*

Todos os anos é publicado no Diário da República, o Relatório Anual de Segurança Interna (RASI) que sistematiza a informação sobre a criminalidade e é de facto um instrumento essencial à avaliação e acompanhamento do estado da segurança interna em Portugal.

O RASI apresenta uma visão integrada da realidade e é um instrumento de trabalho para a política criminal e da atuação das forças e serviços de segurança na prevenção e repressão da mesma.

5.2 Principais Crimes Eletrónicos

O crescente número de computadores pessoais (portáteis) e a maior permanência de ligação na web, associados ao confinamento, contribuíram para uma maior exposição ao crime de base tecnológica.

Os principais crimes ciberdependentes e ciberinstrumentais estão associados ao crime de branqueamento resultante de fraudes por falsos investimentos, burlas por *Chief Executive Officer* (CEO), fraudes online (associadas a transação de bens ou serviços), *phishing*, em particular o bancário.

O *phishing* bancário com recurso à modalidade de *smishing* (envio de SMS com um link – bit.ly) e o *vishing* (chamada telefónica para validar dados ou transferência bancária ilicitamente efetuada) e as burlas online, quer seja em investimentos em moeda virtual, quer através da transação de bens ou serviços continuam a predominar.

O objetivo destas fraudes são, principalmente, a recolha de credenciais de acesso ao *homebanking* e serviços financeiros, a recolha de dados de cartão de crédito ou débito e a recolha de credenciais de acesso ao correio eletrónico (para exfiltração de informação e/ou a disseminação de campanhas de fraude, tendo como origem um e-mail fidedigno).

Relativamente ao número de abertura de incidentes em 2021, estes totalizaram 1.781 casos, sendo 803 deles referentes a fraude (mais 23,7% face a 2020) e a constituir a classe com maior peso dentro dos incidentes.

5.3 Fraude Eletrónica

A fraude eletrónica consiste no uso da tecnologia da informação para cometer fraude.

O fenómeno da fraude através de meios de pagamento eletrónico tem registado um contínuo aumento, fruto da proliferação do uso de tecnologias digitais, do comércio eletrónico e de aplicações fáceis de usar (permitem pagamentos simples e rápidos), mas nem sempre acompanhadas por procedimentos seguros, como o caso da dupla validação, ou com "falhas de segurança"/ausência de procedimentos de validação segura por parte das entidades bancárias, processadores de pagamentos e comerciantes, que permitem facilmente, e a qualquer pessoa, usar dados de pagamento de outrem.

Esta nova realidade produz e concentra um elevado número de questionários para investigação. Segundo a PJ e a análise de questionários, foram constituídos 743 arguidos (mais 86,7% do que o ano anterior da publicação relatório), 88foram detidos (registando um aumento significativo de 266,7% face a 2020) e 11elementos ficaram em prisão preventiva (mais 5,7 pontos percentuais em relação a 2020).

Por outro lado, face ao surgimento de fenómenos criminosos como o caso das fraudes através da aplicação MB *Way*, a situação configurou-se de forma mais séria. Pese embora o impacto do crime (baixo valor e pouca relevância criminal e penal), o fenómeno atingiu milhares de vítimas que ficaram em sérias dificuldades financeiras.

No caso concreto da fraude com meios de pagamento eletrónico, a concretização tende a não se revestir de elevada complexidade, podendo qualquer cidadão com conhecimentos médios do meio digital ser autor de fraude, mesmo quando se trata de casos de *skimming* (clonagem de cartões) ou ataques lógicos, porque o processo complexo não é a concretização, mas sim a construção de "dispositivos" e/ou programas informáticos/*malware,* que são ações planeadas e executadas por experts.

6 Questões de Investigação

Ao longo da revisão de literatura foram colocadas questões de investigação, tendo em consideração as afirmações de vários autores, que estão evidenciadas na seguinte tabela e que serão respondidas posteriormente, na apresentação de resultados:

Questão de Investigação	Fundamentação Teórica
Q1 – Quem são as principais vítimas das burlas eletrónicas?	APAV
Q2 – Quais são as fraudes eletrónicas mais frequentes?	RNSI (2021)
Q3 – Haverá alguma relação entre o nível de literacia tecnológica e a fraude eletrónica?	APAV
Q4 – Qual é o procedimento a seguir em caso de denúncia de fraude eletrónica?	UPFC
Q5 – A Auditoria Forense é uma ferramenta valiosa para combater e suprimir os atos fraudulentos?	Tapia (2010)
Q6 – Qual seria a forma mais proativa e eficaz de lutar contra a fraude?	UPFC

Tabela 1: Questões de Investigação
Fonte: Elaboração própria, 2022

A escolha da metodologia de investigação a utilizar recaiu no método quantitativo, uma vez que foram utilizados questionários como instrumento de recolha de dados. Foram delineados dois questionários distintos uma vez que pretendemos perceber a atitude de faixas etárias distintas quanto à burla/fraude eletrónica.

CAPÍTULO II – METODOLOGIAS DE INVESTIGAÇÃO

Metodologias de Investigação

Neste capítulo descrevem-se os aspetos relacionados com a investigação realizada, entre os quais os objetivos e questões que incitaram a realização do estudo, a metodologia escolhida, o instrumento privilegiado para a recolha da informação, as técnicas de tratamento da informação e, por fim, a caraterização dos participantes envolvidos na indagação da temática.

1. Métodos de Investigação

A palavra "método" é proveniente da palavra grega "methodos", que significa meio para atingir o fim.

Lakatos (1985) define "método" como sendo o conjunto de procedimentossistemáticos e racionais que permite alcançar os objetivos da pesquisa, tendo em consideração aspetos de segurança, economia e validez.

Por sua vez, Sousa e Baptista (2011), defende que a metodologia de investigação é um processo de seleção da estratégia de investigação, que por si só, condiciona a seleção das técnicas de recolha de dados, que devem ser adequadas aos objetivos a atingir.

Coutinho (2013), explica que a metodologia se centra em técnicas e princípios, designadas de métodos. As generalidades destas técnicas possibilitam a aplicação às diferentes ciências ou a uma parte significativa delas, incluindo procedimentos de formar conceitos e hipóteses, fazer observações e medidas, descrever protocolos experimentais e construir modelos e teorias.

A escolha do tipo de pesquisa a efetuar é feita através da seleção das questões de investigação, onde questões iniciadas por "porquê" e "como" se podem revelar mais adequadas à utilização de estudos de caso como estratégia preferencial de investigação (Yin, 2003).

A pesquisa de um determinado tema pode ser vista como um processo de reflexão que deriva de várias etapas, que passam por: reunir evidências, percecionar resultados que até então não estavam explícitos, bem como gerar novos resultados para além daqueles que se pretendiam com o estudo (Mack, Woodsong, MacQueen, Guest & Namey, 2005; Melo, 2013).

Existem métodos de investigação distintos, nomeadamente, métodos de investigação

quantitativa, e métodos de investigação qualitativa, que serão desenvolvidos de seguida, e existem também métodos mistos, que conjugam os dois métodos, qualitativo e quantitativo (Sousa e Baptista, 2011). Deverá ser selecionado o método mais pertinente e adequado para o estudo em causa.

1.1 Métodos de Investigação Qualitativa

Para Yin (2013), a análise qualitativa é mais significativa que o estudo do caso empírico, pois foca-se na recolha e armazenamento dos dados e na hipótese de os mesmos serem depois alvo de nova análise.

Segundo Fortin, (1999), a investigação qualitativa procura compreender e explicar o objeto de estudo, considerando o seu contexto histórico, tecnológico, socioeconómico e cultural.

A investigação qualitativa foca-se na compreensão dos problemas, analisando os comportamentos, as atitudes ou os valores. Este tipo de investigação é descritivo e indutivo, pois o investigador desenvolve ideias, conceitos, entendimentos e chega à compreensão dos fenómenos a partir de padrões encontrados na recolha de dados (Sousa e Baptista, 2011).

Os recursos mais utilizados para estes métodos são as entrevistas, a observação, os questionários abertos, a interpretação de formas de expressão visual, como fotografias e pinturas, e os estudos de caso (Fonseca R., 2009).

1.2 Métodos de Investigação Quantitativa

Segundo Sousa e Baptista (2011), a investigação quantitativa procura descrever, contextualizar ou elucidar com técnicas estatísticas o objeto de estudo. A técnica de mensuração mais utilizada nesta investigação são os questionários de escolha múltipla.

Neste método, as opiniões e informações, são traduzidas em números, para as analisar e classificar, recorrendo a técnicas estatísticas tais como: percentagem, média, moda, mediana, coeficiente de correlação, entre outras (Fonseca R., 2009).

Aquando do desenvolvimento de uma pesquisa desta natureza devem-se formular hipóteses e classificar a relação entre as variáveis, de modo a garantir a precisão dos resultados e a evitar contradições na análise e interpretação dos dados (Prodanov C. e Freitas E., 2013).

2. Estudo Empírico

O estudo apresentado irá focar-se no método quantitativo na sua essência, dado que, foi realizada apenas uma entrevista no sentido de perceber de que forma a Polícia Judiciária atua em casos de deteção de fraudes. Os questionários realizados procuram analisar a ocorrência da fraude eletrónica no contexto social e demográfico em Portugal.

2.1 População em Portugal

Pretende-se, neste ponto, apresentar uma breve contextualização da população em Portugal, uma vez que se pretende analisar o risco à burla/fraude eletrónica na população portuguesa em geral e, em particular perceber quais as faixas etárias mais propensas a este tipo de fraude.

Segundo os Censos de 2021, a população residente em Portugal, em 31 de dezembro de 2021, foi estimada em 10.343.066 pessoas.

A população residente apresenta um total de homens de 4.920.220 e de mulheres um total de 5.422.846. A faixa etária mais representativa é a dos 15 aos 64 anos, designada por população adulta, pelo INE, com um valor de 5.500.152, cerca de 53% do total da população, o que indica o envelhecimento da população portuguesa se, consideramos que a população acima dos 65 anos e mais é superior em 1.100.000 à da faixa etária dos 0 aos 14 anos (estes dados tiveram por base os valores presentes no site do INE relativos aos Censos de 2021).

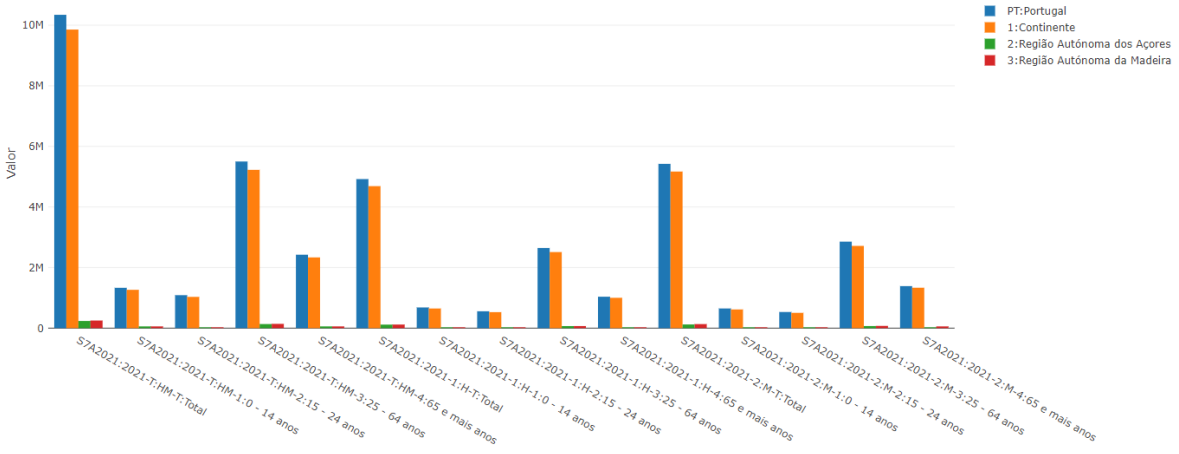


Figura 3: População Residente por Local de Residência, Sexo e Grupo Etário

Fonte: INE, Censos 2021

Sistematizando a informação apresentada no gráfico anterior, apresenta-se a mesma pelos 3 grupos etários a composição da população portuguesa no ano em análise.

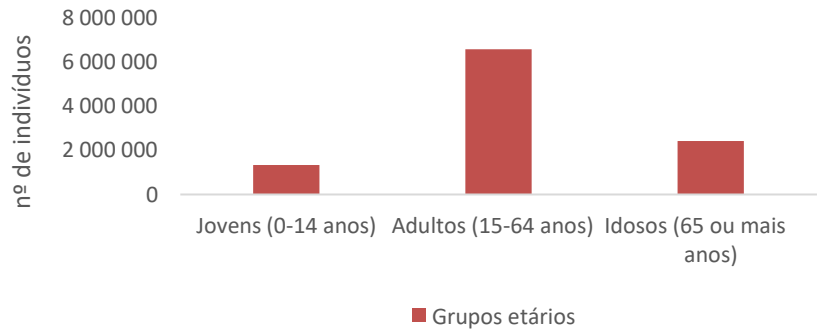


Gráfico 1: População Residente em Portugal por Grupo Etário

Fonte: Elaboração própria, 2022

2.2 Índice de Envelhecimento

De acordo com a PORDATA (Estatísticas sobre Portugal e Europa), em 2020, Portugal ocupava o 2.º lugar no ranking dos países com a população mais envelhecida da UE, apresentando, assim, um índice de envelhecimento de 165,1 idosos por cada 100 jovens. Em 2021, este índice aumentou para 182,70, conforme se pode verificar pela figura apresentada a seguir.

PERÍODO DE REFERÊNCIA DOS DADOS	2021		
SEXO	HM	H	M
LOCAL DE RESIDÊNCIA (À DATA DOS CENSOS 2021)			
Portugal	182,07	151,97	213,71
Continente	184,59	154,40	216,33
Região Autónoma dos Açores	113,19	93,73	133,72
Região Autónoma da Madeira	156,74	118,87	196,39

Figura 4: Índice de Envelhecimento por Local de Residência e Sexo

Fonte: INE, Censos 2021

Ao longo dos anos, o índice de envelhecimento tem vindo a aumentar cada vez mais, como podemos analisar no seguinte gráfico:

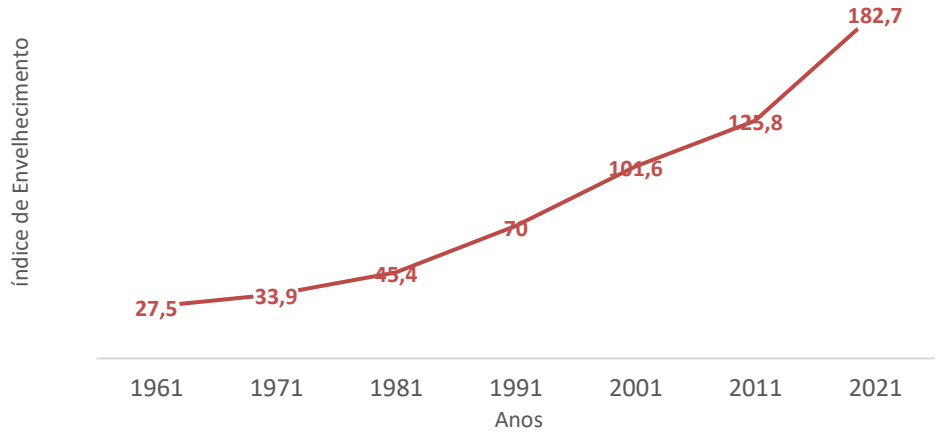


Gráfico 2: Índice de Envelhecimento em Portugal

Fonte: Elaboração própria, 2022

2.3 Literacia Digital/Tecnológica

O conceito de literacia digital/tecnológica diz respeito à consciência, conhecimento e competências que permitem a uma determinada pessoa a utilização eficaz da Internet, das TIC e dos equipamentos e ferramentas associadas e à movimentação em ambientes digitais. Constitui, por isso mesmo, um importante fator na determinação dos níveis de risco e de proteção face à cibervitimação.

As competências e conhecimentos de utilização da Internet e das TIC parecem reduzir o risco de cibervitimação pelo facto de garantirem ao utilizador uma maior capacidade para identificar e atuar perante situações em que a sua segurança online possa estar em risco.

Assim, a uma elevada literacia digital está associada o aumento de comportamentos ciber-resilientes. A ciber-resiliência, por sua vez, é a capacidade de continuar a atividade online, pese embora a ocorrência de incidentes adversos, como ataques cibernéticos. Uma pessoa ciber-resiliente consegue evitar e/ou recuperar de um ataque cibernético com a mínima ocorrência de danos possível.

Em termos genéricos e de acordo a APAV, a população mais jovem apresenta índices elevados de utilização intensiva das TIC e da Internet, concretamente das redes sociais, o que resultará numa maior vulnerabilidade à cibervitimação, em comparação com utilizadores mais velhos e com utilizadores menos frequentes.

2.4 Combate à Literacia Digital/Tecnológica

Todas as pessoas, independentemente da faixa etária a que pertencem, deveriam estar devidamente instruídas relativamente a este assunto, para não serem potenciais vítimas de burlas. Contudo, tal não acontece, verificando-se cada vez mais um aumento dos roubos eletrónicos.

A iniciativa Nacional em Competências Digitais e.2030, Portugal INCoDe.2030, pretende estimular e garantir o desenvolvimento de competências digitais como instrumento para a preparação de uma sociedade orientada para o futuro e para as novas oportunidades que surgem face à acelerada adoção das TIC.

Lançada no dia 3 de abril de 2017, esta iniciativa procura assegurar a generalização do acesso às tecnologias digitais a toda a população e a formação das camadas mais jovens através do estímulo e reforço das competências digitais. Pretende também capacitar profissionalmente a população ativa, promover a especialização em tecnologias digitais e garantir as condições para a produção de novos conhecimentos, potencializando a investigação na área das tecnologias/digital, a utilização da inteligência artificial e de linguagens de programação.

Neste contexto, o Portugal INCoDe.2030 está estruturado em torno de cinco eixos estratégicos: inclusão, educação, qualificação, especialização e investigação. Cada um destes eixos está associado a um conjunto de objetivos e medidas de políticas públicas, que são dinamizados por diversas instituições e entidades.

Até 2030, a iniciativa pretende dar resposta a três grandes desafios, nomeadamente:

- garantir a literacia e a inclusão digitais para o exercício da cidadania;
- estimular a especialização em tecnologias e aplicações digitais para a qualificação do emprego e uma economia de maior valor acrescentado;
- produzir novos conhecimentos em cooperação internacional.

Portugal INCoDe.2030 é uma iniciativa conjunta das áreas governativas da Modernização Administrativa; da Ciência, Tecnologia e Ensino Superior; da Educação; do Trabalho; do Planeamento e das Infraestruturas e da Economia, do XXI Governo de Portugal.

Enquadra-se no contexto internacional na área das TIC e visa melhorar e reforçar a posição de Portugal no Índice *Digital Economy & Society Index* (DESI) 2017 da Comissão Europeia, aumentando a competitividade do país através da promoção das competências digitais.

A Fundação para a Ciência e a Tecnologia (FCT) desempenha, ao longo de toda a iniciativa, o papel de entidade coordenadora de diferentes pontos associados aos cinco eixos estratégicos.

3. Método de Investigação Adotado

Tendo em consideração a revisão bibliográfica realizada e as respetivas questões de investigação formuladas, optou-se por utilizar o método de investigação quantitativo, uma vez que foram utilizados questionários como instrumento de recolha de dados. Foram delineados dois questionários distintos uma vez que pretendemos perceber a atitude de faixas etárias distintas quanto à burla/fraude eletrónica.

3.1 Construção de Hipóteses

Na tabela abaixo, podemos encontrar as hipóteses que servirão de suporte para a elaboração do modelo de análise misto:

QUESTÕES DE INVESTIGAÇÃO	HIPÓTESES
Q1. Quem são as principais vítimas de burlas eletrónicas? (APAV)	**H1.** Os jovens apresentam uma maior vulnerabilidade à cibervitimação.
Q2. Quais são as burlas eletrónicas mais frequentes? (APAV) **Q3.** Qual é o procedimento a seguir em caso de denúncia de fraude eletrónica?	**H2.** As burlas mais frequentes são as burlas no comércio eletrónico, burlas bancárias e burlas nos relacionamentos amorosos.
Q4. Haverá alguma relação entre o nível de literacia tecnológica e a fraude eletrónica? (APAV)	**H3.** A uma elevada literacia digital está associada o aumento de comportamentos ciber-resilientes.
Q5. A Auditoria Forense é uma ferramenta valiosa para combater e suprimir os atos fraudulentos? (Tapia, 2010) **Q6.** Qual seria a forma mais proativa e eficaz de lutar contra a fraude?	**H4.** A Auditoria Forense previne e deteta a fraude.

Tabela 2: Hipóteses
Fonte: Elaboração própria, 2022

3.2 O Modelo de Investigação Adotado

O Modelo de Análise Adotado reflete a interligação entre as questões de investigação formuladas, que associadas formam hipóteses. A articulação das questões de investigação conduziu à elaboração do seguinte modelo de análise:

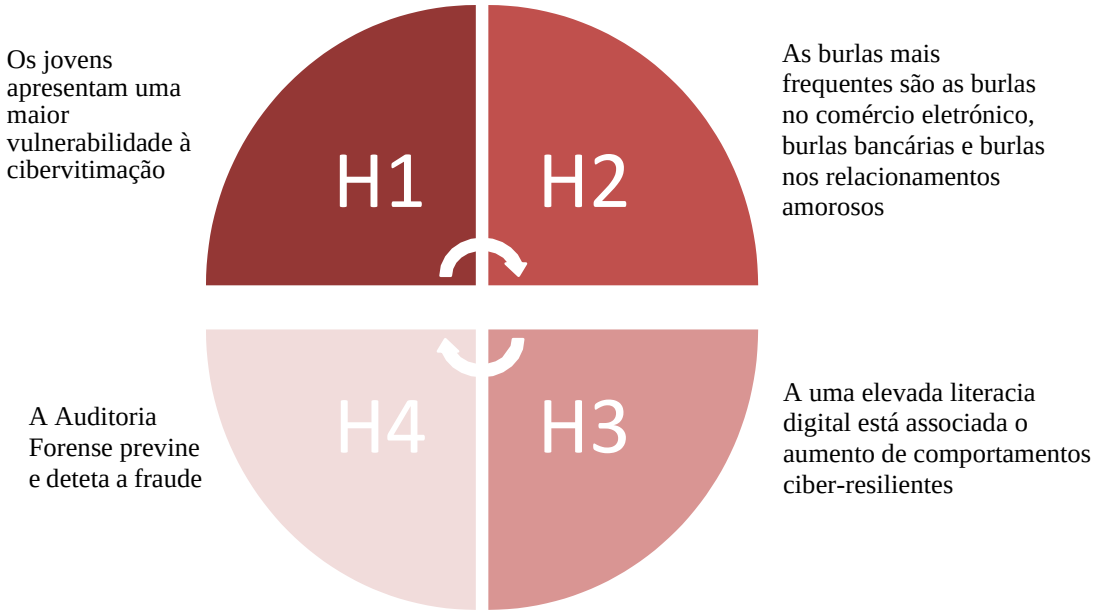


Figura 5: Modelo de Análise
Fonte: Elaboração Própria, 2022

Este modelo de análise assenta num ciclo.

A população mais jovem apresenta índices elevados de utilização intensiva das TIC e da Internet, concretamente das redes sociais, o que pode resultar numa maior vulnerabilidade à cibervitimação, em comparação com utilizadores mais velhos e com utilizadores menos frequentes (H1).

Em contexto *online*, as burlas com maior expressão em termos estatísticos e aquelas que causam um maior dano patrimonial às suas vítimas são: burlas no comércio eletrónico, burlas bancárias e as burlas nos relacionamentos amorosos (H2). A Linha Internet Segura integra também um serviço de denúncia de conteúdos ilegais *online* onde são disponibilizados um conjunto de meios através dos quais, e de forma totalmente anónima, é possível apresentar denúncias de conteúdos eventualmente ilegais.

As competências e conhecimentos de utilização da Internet e das TIC parecem reduzir o risco de cibervitimação pelo facto de garantirem ao utilizador uma maior capacidade para identificar e atuar perante situações em que a sua segurança online possa estar em risco. Assim, a uma elevada literacia digital está associada o aumento de comportamentos ciber-resilientes (H3).

A iniciativa Nacional em Competências Digitais e.2030, Portugal INCoDe.2030, pretende estimular e garantir o desenvolvimento de competências digitais como instrumento para a preparação de uma sociedade orientada para o futuro e para as novas oportunidades que surgem face à acelerada adoção das TIC, sendo relevante demonstrar a importância da Auditoria Forense Preventiva, para que seja possível anteciparmos possíveis danos futuros associados à fraude, antes destes sequer acontecerem. A Auditoria Forense previne e deteta a fraude, uma vez que, deteta a ocorrência de fraude através de uma investigação minuciosa de forma a medir a quantidade dos efeitos (diretos eindiretos) das fraudes efetuadas, os presumíveis criminosos e a cumplicidade que poderáestar por detrás do ato criminoso (H4).

3.2.1 O Papel da UPFC na Deteção e Prevenção da Fraude Eletrónica

Tendo por objetivo conhecer o funcionamento interno da UPFC da PJ no que à deteção e prevenção da fraude eletrónica, foi dirigido um convite ao Diretor da UPFC da PJ, o Dr. Orlando Mascarenhas para ser entrevistado. A entrevista foi realizada no dia 19 de setembro de 2022, através da plataforma Zoom, tendo início às 18h02m, com a duração de 50 minutos. Esta foi gravada, após o consentimento do entrevistado. A gravação da entrevista possibilitou a sua transcrição na totalidade para possibilitar uma análise cuidada ao conteúdo da mesma.

O Diretor da UPFC exerce funções na PJ há cerca de 30 anos. Iniciou carreira inicialmente como agente, tendo, posteriormente, transitado para o cargo de inspetor. Quando iniciou as funções na PJ trabalhou na investigação do furto e de roubos, depois na investigação do tráfico de estupefacientes, na investigação dos homicídios, tendo mais tarde iniciado os seus trabalhos de investigação na área da corrupção. Quando ascendeu ao cargo de chefia, foi responsável pela brigada que investigava a corrupção. Mais tarde, quando entraram em vigor as leis e portarias que implementaram o Gabinete de Recuperação de Ativos em Portugal, fez parte da criação desse gabinete, ficando a chefiar a Delegação do Douro do Gabinete de Recuperação de Ativos até 2017. Em 2017, deixou este cargo e passou a ser Coordenador de InvestigaçãoCriminal, coordenando na região norte a investigação da corrupção, até que lhe foi dirigido um convite por parte da Direção da Polícia Judiciária para dirigir a UPFC e não só se mudou para Lisboa, como inclusive, para o cargo de Dirigente que atualmente ocupa.

3.2.1.1 Análise do Conteúdo à Entrevista

As primeiras questões efetuadas ao Diretor da UPFC da PJ incidiram sobre as quais as principais vítimas e modalidades das fraudes eletrónicas, ao que o entrevistado respondeu que não dispunha de dados estatísticos concretos sobre esta temática. Para uma melhor compreensãoda sua resposta explicou como é que a UPFC se articula e em que se insere a sua função.

"A UPFC é uma unidade de apoio técnico-científico especializado conjuntamente com mais duas outras unidades da Polícia Judiciária, como é o caso do Laboratório de Polícia Científica e a Unidade de Perícia Informática, portanto, tudo o que é técnico- científico especializado na Polícia Judiciária está concentrado nestas três áreas com todo o saber académico associado às mesmas. A área, no caso concreto das Perícias Financeiras ou Contabilísticas, pode exercer as funções de realização de perícias no âmbito de burlas informáticas como exerce no âmbito do crime de estupefacientes ou emqualquer outro tipo de crime, ou seja, não está centrado ou concentrado apenas numa tipificação criminal e por isso, o domínio de dados de algum tipo de crime, nós não possuímos. Eu não sei qual é a tendência ou a característica do crime A, B ou C porqueas solicitações que nos são remetidas, quer seja pela Polícia Judiciária, quer seja por outros órgãos de Polícia Criminal, quer seja mesmo pelo Ministério Público, ou já em última instância, pelos próprios tribunais para realização das perícias financeiras ou contabilísticas, é indiferente o tipo de crime que está associado ao mesmo. Aquilo que se visa é o conhecimento técnico-científico especializado, ou seja, de alguma forma abraça a componente económico-financeira de algum crime, portanto, aquela parte específica de um crime independentemente do tipo de crime. Responder em concreto e com dados concretos relativamente a essa pergunta que me fez, não tenho dados nem o consigo fazer".

O procedimento a seguir quando um indivíduo formaliza uma queixa, independentemente do tipo de crime, quer a queixa seja em termos eletrónicos quer em formato físico, obedece ao que está consagrado na lei processualpenal. Isto é, a denúncia é comunicada à PJ, é analisada pelas suas equipas no contexto da mesma, competência geográfica e tipificação no sentido de perceber de que tipo de crime se trata. De seguida, essa denúncia é remetida obrigatoriamente ao Ministério Público da comarca onde a competência geográfica da mesma está inserida. Como existe delegação de competências na PJ para os crimes de competência reservada da PJ, é remetida às comunidades de

competência de investigação desse tipo de crime. O procedimento é exatamente este, o Ministério Público delegou competência à PJ para a investigação desse crime, seja de competência reservada à PJ, de imediato a investigação passa a decorrer na unidade onde se insere aquela factualidade. Desenvolvida a investigação, chegando à conclusão de que a mesma tem matéria para acusação, é remetida no final para o Ministério Público e este, por sua vez, deduz a acusação e depois seguirão as instâncias em termos de tribunal, instâncias judiciais que irão dar seguimento ao julgamento.

O Diretor da UPFC da PJ considera que a Auditoria Forense é uma ferramenta valiosa para combater e suprimir os atos fraudulentos, mas não será a única. Acredita que todo o instrumento que assente em conhecimento especializado e que verse sobre um conjunto de factos que os torne mais transparentes, o mais credível possível e ao mesmo tempo, potencie o controlo dos mesmos, é sempre eficaz no combate à fraude. Acrescenta ainda, que quanto melhor for o tipo de ferramentas e instrumentos validados, acima de tudo cientificamente, para que a matéria-prima que está sujeita a essa avaliação em sede de auditoria, possa passar ou não, no crivo dessa mesma avaliação.

Quando questionado sobre o facto da PJ ter as ferramentas e os instrumentos necessários ao nível de Recursos Humanos e outros, como seria a forma ideal, mais proativa e eficaz, de lutar contra a fraude, o entrevistado respondeu que sobre os recursos, considera que a PJ tem os recursos que nos dias de hoje sãoos possíveis dentro dos que existem e, acrescenta que a PJ detém os recursos necessários.Em relação aos recursos humanos, afirma que "*é quase transversal a qualquer área da sociedade e não se refere à sociedade portuguesa, mas ao mundo ocidental, porque há a ideia de que os recursos humanos nunca são os necessários, mas todos sabemos que os recursos humanos são finitos e as necessidades é que são sempre infinitas e andamos sempre aqui a tentar encontrar um equilíbrio entre as necessidades e os recursos*". Importa referir que mais do que os recursos humanos serem os adequados ou serem o número suficiente, o Diretor da UPFC da PJ gosta de colocar a tónica de que por vezes, são mais eficazes se encontrarem modelos organizacionais que visem o fim pretendido com os recursos humanos que têm, do que propriamente *"dizer que não temos os recursos humanos que são necessários, sem fazer algo que mude os modelos organizacionais"*. Afirma que se nós temos os instrumentos tecnológicos que, nos dias de hoje, já conseguem substituir muitos dos recursos humanos, isto vai de encontro àquilo que disse previamente, que os modelos organizacionais possivelmente é que necessitam de ser mais adequados.

Quanto à segunda parte da questão, refere que o nível educacional é fulcral. *"Nós podemos ter todos os instrumentos de repressão ao nosso alcance, se em termos de prevenção nada funcionar e a prevenção começa como, e aqui estamos a falar num contexto eletrónico, ou seja, aquilo que nos dias de hoje é possível fazer. Se as pessoas são descuidadas, não têm formação, não têm cuidados comportamentais de navegar, por exemplo, na internet, fornecimento de dados, tudo aquilo que nos dias de hoje é possível fazer que é o tudo e que está ao alcance de um click. E se nós, previamente, não temos essa cultura educacional preventiva, de não partilha de dados, não termos por exemplo, equipamentos que estejam protegidos contra ataques maliciosos e spiderwares e malwares, tudo aquilo que é possível nos dias de hoje fazer, por muito que nós tenhamos em termos de recursos humanos e materiais na repressão, nunca será o suficiente. Nós vivemos numa sociedade, parece-me a mim, que caminha cada vez mais para, não vou dizer os 100%, mas quase o absoluto do digital, tudo se faz através do digital e o alcance da fraude através e com o digital também é de uma dimensão elevadíssima. Se não formos, todos como sociedade, suficientemente cuidadosos naquilo que fazemos na utilização digital é impossível, não há mecanismo coercivo que coloque fim àquilo que é possível fazer através da fraude com recurso a este tipo de instrumentos. E se nós olharmos para os últimos dados dos Relatórios Anuais de Segurança Interna e fizermos uma avaliação, creio que aqui é possível fazer, aquilo que é em termos de criminalidade ou comportamentos criminais associados a atividades digitais e eletrónicas, quer sejam as burlas ou todas as outras, nós vemos a constante crescente ano após ano e, a pandemia veio potenciar ainda mais até porque as pessoas passaram a utilizar mais, portanto o espetro possível de sermos vítimas ou de estarmos envolvidas numa situação fraudulenta, também aumentou, tendo um crescimento quase contínuo ao longo dos anos e parece-me a mim, enquanto cidadão, que não vai parar porque nós vamos utilizar sempre e cada vez mais. Se vamos utilizar sempre e cada vez mais, vamos ter obrigatoriamente, de estar dotados de informação e muitas vezes, muitas das fraudes acontecem porque a informação não é a mais adequada, portanto, é deficitária no nosso conhecimento de sociedade de uma forma geral, sobre quais são os mecanismos e os cuidados básicos na utilização do digital são muito reduzidos e isso potencia o acesso a quem vive e a quem se movimenta nestas áreas da fraude, seja a fraude crime ou não. A fraude através dos mecanismos eletrónicos e do digital é mais uma vez, quase o velho problema, normalmente o problema não são as armas, é o uso das mesmas, aqui o problema também não é o digital, mas sim o uso do mesmo que pode vir a ser um problema. Portanto, julgo*

eu que nos falta essa formação de base e, por isso é que eu disse que é educacional. Obviamente que deverá haver todo outro conjunto de medidas, mas julgo que passaria por aí, como eu sou um defensor do conhecimento e da formação, acho que a educação nos faria ganhar pontos no combate e acima de tudo na prevenção".

Os resultados obtidos nesta entrevista permitiram compreender o procedimento a seguir em caso de denúncia, a importância da Auditoria Forense e da UPFC da PJ no combate à fraude eletrónica e sobretudo, o quanto a educação é essencial no combate à fraude eletrónica como meio de prevenção.

3.2.2 Método Quantitativo

Relativamente ao método quantitativo, o instrumento de recolha de dados escolhido foi o questionário. O principal objetivo é o de investigar qual a classe etária mais vulnerávele mais propícia a ser vítima de burlas eletrónicas (adultos ou idosos) e, de que forma, isso se relaciona com aliteracia tecnológica.

Foi elaborado um questionário com recurso à plataforma *Google Forms.* O questionário eletrónico foi enviado por e-mail a 168 colaboradores da empresa Trindade das Viagens Abreu e, contou com a colaboração de 85 inquiridos.

De forma a que o questionário fosse respondido por um leque alargado ao maior número de faixas etárias, nomeadamente, a idosos, foi solicitada a colaboração dos utentes de Centros de dia da área de Vila Nova de Gaia. No entanto, apenas conseguimos a colaboração do Centro de Dia de Mafamude, que é frequentado por cerca de 30 utentes. Os questionários foram impressos e as questões foram colocadas a cada utente e as respostas recolhidas escritas na folha da entrevista. Esta atividade deu-se no dia 2 de setembro de 2022, pelas 11h00m, contou com a colaboração da Diretora do Centro e respetivos auxiliares, teve lugar no Centro de Dia de Mafamude, onde foram recolhidos dados de 23 utentes.

3.2.2.1 Apresentação de Resultados

No total, computamos uma população composta por 191 pessoas, sendo a nossa amostra constituída por 108 indivíduos.

Inicialmente, iremos proceder à caracterização da amostra, quanto à faixa etária e alfabetização. Cerca de 23% dos inquiridos encontram-se na faixa etária entre os 65 e mais anos de idade e 85% na faixa etária dos 15 aos 64 anos.

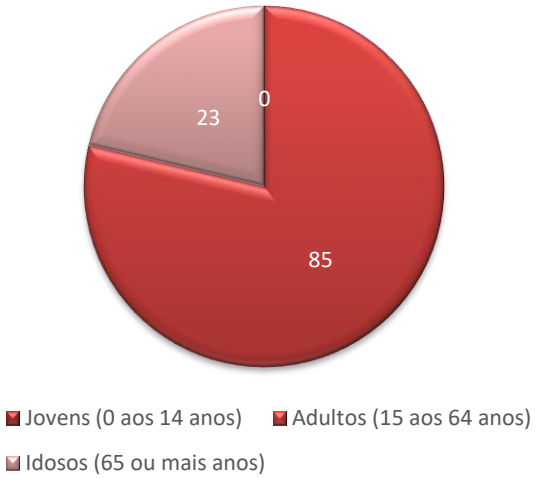


Gráfico 3: Faixa Etária
Fonte: Elaboração própria, 2022

A segunda questão da entrevista pretendia aferir se os inquiridos "sabem ler e escrever", os inquiridos compreendidos na faixa etárias dos 15 aos 64 anos de idade, na sua totalidade, responderam afirmativamente. Na faixa etária superior aos 65 anos de idade, 3 dos 23 inquiridos responderam "Não".

Dos 108 inquiridos, 97,22% sabem ler e escrever, enquanto 2,78 % não sabem ler nem escrever.

De seguida apresentamos as respostas obtidas no que ao escopo da investigação concerne, isto é, tentar perceber se os inquiridos utilizam a internet, em que casos e de que forma esta situação estará relacionada com a maior ou menor apetência para se tornarem potenciais vítimas de fraude eletrónica.

Só uma pessoa pertencente aos jovens e aos adultos, alega que apenas tem telemóvel, os restantes possuem telemóveis e computador.

Na faixa etária com mais de 65 anos de idade, duas pessoas possuem telemóvel e computador e 15 têm apenas o telemóvel, sendo que 6 dos idosos não têm telemóvel, nem computador.

Quando questionados "Costuma utilizar a internet? Se sim, em que situações?", apenas um dos inquiridos dentro da faixa etária entre os 15 e os 64 anos de idade refere que não utiliza a Internet, enquanto os restantes utilizam a internet no seu dia-a-dia. Este

uso diário da internet, por estes inquiridos, é necessário no seu trabalho, para lazer, estudar, comprar online, redes sociais, órgãos de informação, jogos, filmes, pesquisas, contas bancárias, entre outros.

Nenhum dos inquiridos com idade superior a 65 anos utiliza a internet.

À questão "Alguma vez foi burlado? Se sim, em que situação?" as respostas permitiram aferir que foram alvo de burla eletrónica 15 inquiridos na faixa etária entre os 15 e os 64 anos de idade. Estas burlas foram respetivas a casos de compras online, aluguer de casa de férias e chamadas telefónicas a pedir acesso às contas bancárias, feitas por indivíduos que se fazem passar por colaboradores do banco.

Dentro da faixa etária dos idosos, 9 foram roubadas, mas não eletronicamente, apenas se referiram a assaltos.

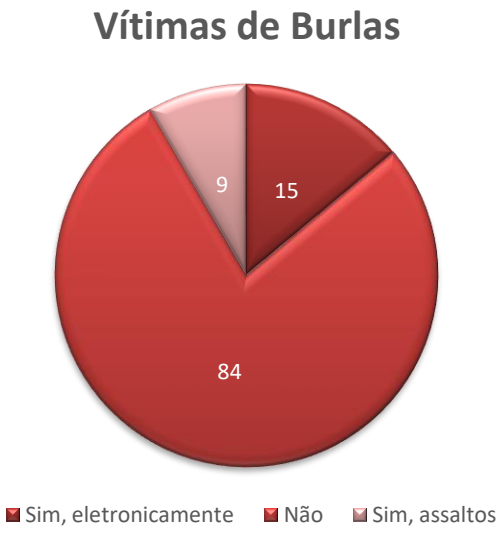


Gráfico 4: Vítimas de Burlas
Fonte: Elaboração própria, 2022

Assim sendo, estamos perante uma taxa de 13,89% de burlas eletrónicas.

Os resultados obtidos nesta entrevista permitiram identificar as principais vítimas de burlas eletrónicas de acordo com a sua faixa etária, neste caso são os adultos, analisar em que circunstâncias as pessoas utilizam a internet, que é praticamente em tudo da sua vida quotidiana e reconhecer quais são as modalidades da fraude eletrónica mais recorrentes.

3.2.3 Discussão de Resultados

Após a apresentação de resultados, recolhidos através das entrevistas e do questionário, é necessário estudar a veracidade dos mesmos, isto é, se estes respondem às questões de investigação criadas através da revisão da literatura, que posteriormente deram origem a hipóteses.

A primeira questão de investigação refere quem são as principais vítimas da fraude eletrónica. Em termos genéricos e de acordo a APAV, a população mais jovem apresenta índices elevados de utilização intensiva das TIC e da Internet, mais concretamente das redes sociais, o que resultará numa maior vulnerabilidade à cibervitimação, em comparação com utilizadores mais velhos e com utilizadores menos frequentes. Através dos resultados recolhidos nos questionários e nas entrevistas, verificamos que efetivamente os utilizadores mais velhos, os idosos, não apresentam casos em que foram vítimas de burlas eletrónicas, ao contrário dos adultos, que apresentam uma taxa de 13,89% de burlas eletrónicas.

A segunda questão de investigação procura saber quais são as burlas eletrónicas mais frequentes. Segundo a APAV, em contexto online, as burlas com maior expressão em termos estatísticos e aquelas que causam um maior dano patrimonial às suas vítimas são: burlas no comércio eletrónico, burlas bancárias e as burlas nos relacionamentos amorosos (*romance scams*). Os 15 adultos que foram vítimas de fraude eletrónica mencionam casos de compras online, aluguer de casa de férias e chamadas telefónicas a pedir acesso às contas bancárias, efetuadas por indivíduos que se fazem passar por colaboradores do banco. Não foram registados casos de burlas nos relacionamentos amorosos por parte da nossa amostra.

A terceira questão foca-se no procedimento a ser levado a cabo em caso de denúncia, do ponto de vista do cidadão, mas também das autoridades competentes para tratar do processo. A Linha Internet Segura integra um serviço de denúncia de conteúdos ilegais *online* onde são disponibilizados um conjunto de meios através dos quais, e de forma totalmente anónima, é possível apresentar denúncias de conteúdos eventualmente ilegais. As denúncias recebidas são triadas e analisadas por operadores especializados que lhes dão o devido seguimento: autoridade policial nacional ou congénere internacional. Tendo em conta a entrevista realizada ao Diretor da UPFC da PJ, o procedimento passa pelo

Ministério Público que delegou competência à PJ para a investigação desse crime, seja de competência reservada à PJ, de imediato a investigação passa a decorrer na unidade onde se insere aquela factualidade. Desenvolvida a investigação, chegando à conclusão de que a mesma tem matéria para acusação, é remetida no final para o Ministério Público e este, por sua vez, deduz a acusação e depois seguirão as instâncias em termos de tribunal, instâncias judiciais que irão dar seguimento ao julgamento.

A quarta questão de investigação pretende estudar a relação entre o nível de literacia tecnológica e a fraude eletrónica. De acordo com a APAV, as competências e conhecimentos de utilização da Internet e das TIC parecem reduzir o risco de cibervitimação pelo facto de garantirem ao utilizador uma maior capacidade para identificar e atuar perante situações em que a sua segurança online possa estar em risco. Assim, a uma elevada literacia digital está associada o aumento de comportamentos ciber-resilientes. Uma pessoa ciber-resiliente consegue evitar e/ou recuperar de um ataque cibernético com a mínima ocorrência de danos possível. Através da entrevista ao Diretor da UPCF, verificamos que a educação é fulcral nesta temática, uma vez que atua como meio de prevenção na fraude eletrónica e, consequentemente, gera pessoas ciber-resilientes, capazes de evitar um ataque cibernético.

A quinta e sexta questões prendem-se com a importância da Auditoria Forense no combate e na supressão aos atos fraudulentos e qual seria a forma mais proativa e eficaz de lutar contra a fraude. Tendo em conta a entrevista realizada ao Diretor da UPFC da PJ, este considera que a Auditoria Forense é uma ferramenta valiosa para combater e suprimir os atos fraudulentos, mas não será a única. O entrevistado acredita que todo o instrumento que assente em conhecimento especializado e que verse sobre um conjunto de factos que os torne mais transparentes, o mais credível possível e ao mesmo tempo, potencie o controlo dos mesmos, é sempre eficaz no combate à fraude. Menciona ainda, que o conhecimento a nível educacional e como formação base é muito importante como meio de prevenção e de combate à fraude eletrónica.

CAPÍTULO III – CONCLUSÃO

Conclusão

A presente dissertação teve como objetivo analisar a ocorrência da fraude eletrónica no contexto social e demográfico em Portugal, compreender as medidas já implementadas pelos organismos especializados e perceber que práticas podem ser adotadas além das que existem, de modo a aumentar a segurança dos utilizadores tecnológicos.

Fruto da revisão de literatura realizada obtivemos a base teórica que sustentou a investigação prática. Tendo sido escolhida uma metodologia de investigação mista, em que o instrumento de recolha de resultados foi a entrevista e o questionário, revelando-seo mais pertinente para o estudo.

No decorrer da revisão de literatura realizada foi possível perceber a faixa etária que apresenta mais vulnerabilidade às burlas eletrónicas, as modalidades de crime eletrónico mais frequentes, a relação entre o nível de literacia tecnológica e a fraude eletrónica e por fim, a importância da Auditoria Forense no combate a este tipo de fraude.

O desenvolvimento dos objetivos de investigação, permitiu-nos estabelecer hipóteses que nos levaram a analisar de forma mais profunda as questões de investigação suscitadas na revisão da literatura:

- **Hipótese 1:** Os jovens apresentam uma maior vulnerabilidade à cibervitimação.
- **Hipótese 2:** As burlas mais frequentes são as burlas no comércio eletrónico, burlas bancárias e burlas nos relacionamentos amorosos.
- **Hipótese 3:** A uma elevada literacia digital está associada o aumento de comportamentos ciber-resilientes.
- **Hipótese 4:** A Auditoria Forense previne e deteta a fraude.

Tendo por base o estudo desenvolvido podemos concluir que a hipótese 1 se encontra validada. AAPAV defende que as principais vítimas da fraude eletrónica são a população mais jovemcomparativamente com os utilizadores mais velhos, que utilizam menos a tecnologia. Osresultados analisados das respostas aos questionários e às entrevistas confirmam que os utilizadores mais velhos, não apresentam casos em que foram vítimas

de burlas

eletrónicas.

A hipótese 2 é validada, porque segundo a APAV, em contexto online, as burlas com maior expressão em termos estatísticos são as burlas no comércio eletrónico, burlas bancárias e as burlas nos relacionamentos amorosos (*romance scams*). Os questionários referem nomeadamente, casos de burlas no comércio eletrónico e burlas bancárias. A Linha Internet Segura integra um serviço de denúncia de conteúdos ilegais *online* onde são disponibilizados um conjunto de meios através dos quais, é possível apresentar denúncias de conteúdos eventualmente ilegais. Através da entrevista realizada ao Diretor da UPFC da PJ, foi possível compreender todo o procedimento a efetuar em caso de denúncia: o procedimento passa pelo Ministério Público que delegou competência à PJ para a investigação desse crime, seja de competência reservada à PJ, de imediato a investigação passa a decorrer na unidade onde se insere aquela factualidade.Desenvolvida a investigação, chegando à conclusão de que a mesma tem matéria para acusação, é remetida no final para o Ministério Público e este, por sua vez, deduz a acusação e depois seguirão as instâncias em termos de tribunal, instâncias judiciais que irão dar seguimento ao julgamento.

De acordo com a APAV, as competências e conhecimentos de utilização da Internet e das TIC parecem reduzir o risco de cibervitimação pelo facto de garantirem ao utilizador uma maior capacidade para identificar e atuar perante situações em que a sua segurança online possa estar em risco. Na entrevista realizada ao Diretor da UPCF, este defende que a educação é fulcral nesta temática, uma vez que as fraudes acontecem muitas vezes, porque a informação que os utilizadores possuem não é a mais adequada, os mecanismos e os cuidados básicos na utilização do digital são muito reduzidos e isso potencia a que a segurança do utilizador fique comprometida. Pelo que a hipótese 3 se encontra validada.

Tendo em conta a entrevista realizada ao Diretor daUPFC da PJ, este considera que a Auditoria Forense é uma ferramenta valiosa para combater e suprimir os atos fraudulentos, mas não será a única. O conhecimento a nível educacional e como formação base é muito importante como meio de prevenção e de combate à fraude eletrónica. A hipótese 4 encontra-se validada.

Podemos concluir que é necessário apostar na educação desde cedo para que os indivíduos possuam conhecimentos tecnológicos mais aprimorados e, consequentemente,

exista uma diminuição dos casos das burlas eletrónicas. Uma sugestão para implementar esse conhecimento seria apostar em ações de formação nas escolas, faculdades seniores, lares e centros de dia de idosos, para que a informação chegue não só aos mais novos como também aos mais velhos.

Como referiu o Diretor da UPFC da PJ, na sua entrevista, *"o problema não são as armas, mas sim o uso das mesmas. Vivemos na era da tecnologia e por isso, é essencial termos uma educação que nos ensine a manusear a tecnologia da forma mais correta possível, antecipando possíveis fraudes que possam ocorrer".*

Limitações de Estudo

Uma das limitações identificadas no presente estudo foi o facto de estarmos perante um estudo em que a amostra é reduzida face ao tamanho da população, apenas abrange 108 inquiridos pelo que, a generalização está limitada nesse aspeto.

O facto de termos vivido uma pandemia recentemente, tornou-se um entrave a que conseguisse facilmente a colaboração dos centros de dia para o meu estudo de caso, uma vez que os idosos representam uma faixa etária de grande risco e por isso, existiu uma grande resistência quanto à colaboração dos utentes, pois nem todos os centros de dia se mostraram interessados em participar no projeto.

O facto de ter sido possível realizar apenas uma entrevista também resulta por si só numa limitação, dado que não temos um elo de comparação com as respostas de outro indivíduo que opera no mesmo ramo. É importante salientar que parte deste estudo foi realizado com base em opiniões e informação obtida do entrevistado, não havendo observação direta ou verificação da realidade das respostas obtidas, pelo que, este estudo está limitado nesse sentido.

Sugestões para Investigações Futuras

Como aspetos a melhorar pode-se referir o tamanho da amostra, poderia ter sido maior de forma a dar uma ideia mais realista do seu todo na globalidade.

Teria sido interessante abordar a temática da fraude eletrónica em contexto organizacional e, consequentemente, ter a opinião da área no setor privado, com a finalidade de apurar as diferenças dos procedimentos a seguir em caso de fraude eletrónico no setor público versus setor privado.

Referências Bibliográficas

ACFE (2014); *Árvore da Fraude*. https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/-/media/51FB0E7892E24FC392ED325FE0A42C2A.ashx

ACFE (2014); *Report to the Nation on Occupational Fraude & Abuse.* https://www.acfe.com/-/media/files/acfe/pdfs/2014-report-to-nations.ashx

ACFE (2014); *Triângulo da Fraude.* https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud

APAV. https://apav.pt/apav_v3/index.php/pt/

Araújo, A. (2016); *Responsabilidade Social e Ética dos Auditores na Deteção ePrevenção de Fraude.* Dissertação de Mestrado, ISCAP.

Azevedo, A. (2016); *Burlas Informáticas: Modos de Manifestação*. Dissertação EDUM.

Banco de Portugal (2014); *Esclarecimento sobre a Auditoria Forense em curso ao grupo Banco Espírito Santo.* https://www.bportugal.pt/comunicado/esclarecimento-sobre-auditoria-forense-em-curso-ao-grupo-banco-espirito-santo

CNCS (2022); *Relatório de Cibersegurança em Portugal.* https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

Código Penal. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1995-34437675

Coutinho, C. (2013); Metodologia de investigação em ciências sociais e humanas: Teoria e prática (2ª ed.). Porto: Almedina.

Crepaldi, S. (2000); *Auditoria Contábil: Teoria e Prática.* Brasil: Atlas.

Dave Ramos (2021); *Pentágono da Fraude: a geometria de suborno e corrupção.* https://fabricadequalidade.com.br/pentagono-da-fraude-suborno-corrupcao/

Esteves, I. (2012); *A Responsabilidade Social do Auditor Perante a Fraude.* Dissertação de Mestrado, ISCAL.

Fernandes, M. (2016); *Relação entre a Auditoria Forense e a Ética das Organizações*. Dissertação de Mestrado, ISCAP.

Fonseca (2015); *A Prevenção da Fraude e a Afirmação da Auditoria Forense.* OCC.

Fonseca, R. (2009); *Metodologia do Trabalho Científico*. Brasil: IESDE Brasil S.A.

Fortin, M. (1999); *O Processo de Investigação: da Concepção à Realização* (2ª edição). Loures: Lusociência.

ISA 240 – International Standard on Auditing 204. https://ifrs.ocpcangola.org/ifrs/wp-content/uploads/2017/07/A013-2012-IAASB-Handbook-ISA-240-PT.pdf

Instituto Nacional de Estatística (2021). https://tabulador.ine.pt/censos2021/?r=PALAVRAPT%7Ec%7E%23P958

Jornal de Negócios (2014); *O que é uma Auditoria Forense? https://www.jornaldenegocios.pt/empresas/banca---%20financas/detalhe/o_que_e_uma_auditoria_forense*

Lei de Segurança Interna. https://dre.pt/dre/legislacao-consolidada/lei/2008-34501675-67578006

Linha Internet Segura. https://www.internetsegura.pt/lis/sobre-a-lis

Mendes, A. (2021); *A Importância da Auditoria no Combate à Corrupção*. Dissertação de Mestrado, ISCAC.

Ministério Público (2022); Cibercrime: Denúncias Recebidas. https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/2022_07_13_denu ncias_recebidas.pdf

Pordata.https://www.pordata.pt/Europa/%c3%8dndice+de+envelhecimento-1609

https://www.pordata.pt/portugal/populacao+residente+total+e+por+grandes+grupos+etarios-513

Relatório Anual de Segurança Interna (2021) https://www.portugal.gov.pt/pt/gc23/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2021

Sousa, J., & Baptista, S. (2011); *Como fazer Investigação Dissertações, Teses e Relatórios Segundo Bolonha*, (1ª edição). Lisboa: Pactor.

Sousa, N. (2016); *A importância da Auditoria na deteção e prevenção da fraude.* Dissertação de Mestrado, ISCAP.

Tapia (2010); A integração de conhecimentos forenses, contábil, jurídica, processual e de recursos financeiros para a luta contra a fraude. http://www.forodeseguridad.com/artic/pt/9005.htm

Unidade de Perícia Financeira e Contabilística da Polícia Judiciária. https://www.policiajudiciaria.pt/upfc/

Prodanov C., & Freitas, E. (2013); *Metodologia do Trabalho Científico: Métodos eTécnicas de Pesquisa e do Trabalho Acadêmico* (2ª Edição). Brasil: Editora Feevale.

Wells, Joseph T. (2007); *Manual da fraude na empresa, prevenção e deteção.* New Jersey: Association of Certified Fraud Examiners.

Yin, K. (2003); *Case study research: Design and methods* (3ª Edição). London. Sage Publication.

Apêndices

Apêndice I – Guião de Entrevista ao Diretor da UPFC da PJ

1) Gostaria que fizesse inicialmente uma pequena contextualização sobre o percurso da sua carreira profissional na Polícia Judiciária, salientando os cargos e as funções que já desempenhou e que atualmente desempenha.
2) A minha dissertação está mais direcionada para as burlas eletrónicas e por isso, as próximas questões irão incidir sobre esse ramo. Quem são as principais vítimas de burlas eletrónicas, tendo em conta a sua faixa etária?
3) Quais são as modalidades de burlas eletrónicas mais frequentes que recebem queixa?
4) Qual é o procedimento que executam quando um indivíduo formaliza uma queixa em que alega que foi burlado eletronicamente, desde a formalização da queixa até ao arquivo do caso?
5) Quais são as suas recomendações para combater este tipo de fraude?
6) Considera que a Auditoria Forense é uma ferramenta valiosa para combater e suprimir os atos fraudulentos? Porquê?
7) Da sua longa experiência de 30 anos na Polícia Judiciária e tendo em conta esta questão da fraude que está cada vez mais aprimorada quer eletronicamente ou não, o Dr. Orlando encara que vocês têm as ferramentas e os instrumentos necessários ao nível de Recursos Humanos e outros, e como é que na sua perspetiva seria a forma ideal de lutar contra a fraude de uma forma mais proativa e eficaz?

Apêndice II – Questões do Questionário aos Idosos

1) Que idade tem?
2) Sabe ler e escrever?
3) Possui telemóvel, computador ou ambos?
4) Costuma utilizar a Internet? Se sim, em que casos?
5) Alguma vez foi burlado? Se sim, em que situação?