ACADEMIA MILITAR

OS NÚCLEOS DE INVESTIGAÇÃO CRIMINAL DA GUARDA NACIONAL REPUBLICANA E O MANUSEAMENTO DA PROVA EM SUPORTE ELETRÓNICO

Autor: Aspirante de Cavalaria da GNR Vitor Manuel Seixas Teixeira

Orientadora: Professora Doutora Ana Maria Carapelho Romão Leston Bandeira
Coorientador: Major de Infantaria da GNR Tiago Lourenço Lopes

Mestrado Integrado em Ciências Militares, na especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, setembro de 2019

ACADEMIA MILITAR

OS NÚCLEOS DE INVESTIGAÇÃO CRIMINAL DA GUARDA NACIONAL REPUBLICANA E O MANUSEAMENTO DA PROVA EM SUPORTE ELETRÓNICO

Autor: Aspirante de Cavalaria da GNR Vitor Manuel Seixas Teixeira

Orientadora: Professora Doutora Ana Maria Carapelho Romão Leston Bandeira
Coorientador: Major de Infantaria da GNR Tiago Lourenço Lopes

Mestrado Integrado em Ciências Militares, na especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, setembro de 2019

EPÍGRAFE

"A humanidade tem adquirido toda a tecnologia certa para todas as razões erradas".

R. Buckminster Fuller

DEDICATÓRIA

Aos meus pais e ao meu irmão.

AGRADECIMENTOS

O presente Relatório Científico Final do Trabalho de Investigação Aplicada apenas foi exequível pelo suporte dado por parte de várias pessoas que, não só acompanharam a evolução deste trabalho, mas também contribuíram de forma essencial nas conclusões a que chegamos.

Em primeiro lugar, agradecer à Sr.ª Professora Ana Maria Carapelho Romão Leston Bandeira, minha orientadora, pela incansável disponibilidade e, sobretudo, celeridade em esclarecer todas as dúvidas que foram surgindo. Em segundo lugar, um obrigado muito especial ao Sr. Major Tiago Lourenço Lopes pela forma prática, profissional e exaustiva com que me ensinou a lidar com este tema e cujos ensinamentos espero transportar para outras situações da minha vida, no futuro. A sua forma de ser Oficial da Guarda Nacional Republicana constituí para mim um grande exemplo.

A todos os entrevistados quer da GNR, quer do Ministério Público pelo seu contributo, o qual caracterizo por uma abertura, transparência e rigor nas respostas às entrevistas concedidas.

Aos militares do Núcleos de Investigação Criminal da GNR pela participação nesta investigação através das respostas aos inquéritos por questionário apesar das suas ocupações profissionais fruto do forte empenhamento operacional.

À Direção dos cursos da GNR, pela preocupação demonstrada e pela disponibilidade em atender às necessidades relacionadas com a realização desta investigação.

À Academia Militar e à Escola da Guarda que, ao longo destes cinco anos me proporcionaram as dificuldades necessárias para me fazer crescer enquanto Homem e Soldado.

A todos os meus camaradas do XXIV Curso de Oficiais da Academia Militar, pelos laços que criamos. Afigura-se impossível traduzir o que ultrapassamos em palavras.

Por último, um agradecimento muito emocionado aos meus pais. Ao meu pai, Cabo da Guarda Nacional Republicana, João Filipe Teixeira, que criou em mim o desejo de contribuir para solução dos problemas dos outros mesmo com o sacrifício dos nossos interesses pessoais. Um conhecedor ímpar da Investigação Criminal, em particular na GNR, e que muito me aconselhou durante a realização desta investigação científica. À

melhor mãe do mundo, Maria de Deus Seixas Teixeira, por toda a preocupação, carinho e por acreditar sempre em mim.

RESUMO

O presente Relatório Científico Final do Trabalho de Investigação Aplicada, subordinado ao tema "Os Núcleos de Investigação Criminal da Guarda Nacional Republicana e o manuseamento da Prova em Suporte Eletrónico", visa caracterizar as capacidades destes militares na execução de diligências processuais no âmbito da Investigação Criminal respeitantes a este tipo de prova.

A metodologia empregue é de tipo qualitativo e quantitativo, com recurso, respetivamente, ao inquérito por entrevista e inquérito por questionário.

A investigação encontra-se dividida em duas partes, designadamente a Parte I – Enquadramento teórico e a Parte II – Prática. Na parte I, são apresentados os conceitos teóricos fundamentais para compreender o fenómeno estudado. Para além disto, apresentamos a estrutura de investigação criminal da GNR, assim como, as competências para o manuseamento da prova em suporte eletrónico por parte dos investigadores. Na Parte II são expostos os métodos e procedimentos utilizados, a análise e discussão dos resultados obtidos e as conclusões alcançadas.

Como principais conclusões destacamos que existem algumas necessidades ao nível da formação e do apoio técnico especializado para que seja possível alcançar uma maior eficácia nos processos crime confiados a esta força de segurança. Em segundo lugar verificamos a falta de um quadro de competências relativamente ao manuseamento da prova em suporte eletrónico dentro da estrutura de investigação criminal da GNR. Por ultimo, notamos existir uma limitação, por parte dos NIC, no que concerne à análise deste tipo de prova e que pode dificultar capacidade de interpretar os relatórios que são feitos após a aquisição dos dados.

Palavras chave: Guarda Nacional Republicana; Prova em suporte eletrónico; Prova digital; Investigação Criminal.

ABSTRACT

This Final scientific report on the work of applied research, subordinated to the theme "The Criminal investigation nuclei of the Republican National Guard and the handling of the test in Electronic support", aims to characterize the capacities of these In carrying out procedural steps in the context of Criminal investigations relating to this type of evidence.

For the pursuit of the investigation, the inductive model was used. In this way, the study aims to answer the questions derived and has as final answer to the starting question.

The methodology explained by Quivy and Campenhoudt (2008), Fortin (2009) and Guerra (2006) was employed in conducting the present research work. The data collection instruments used were the questionnaire survey and the interview.

The research is divided into two parts, namely Part I – Theoretical framework and part II – Practice. In part I, the fundamental theoretical concepts are presented to understand the phenomenon studied. In addition, we present the criminal investigation structure of GNR, as well as the competences necessary for the handling of evidences in electronic support by criminal investigators. In part II are exposed the methods and procedures used, the analysis and discussion of the results obtained and the conclusions reached.

As main conclusions we highlight that there are some needs in training and specialized technical support so that it is possible to achieve greater effectiveness in the crime processes entrusted to this security force. Secondly, there is a lack of a core competence description for handling digital evidence within the GNR criminal investigation structure. Lastly, we note that there is a limitation by the criminal investigators regarding the analysis of this type of evidence and that it may hinder the ability to interpret the reports that are made after the acquisition of the data.

Keywords: *Guarda Nacional Republicana*; electronic supported evidence; digital evidence; Criminal Investigation.

ÍNDICE GERAL

ÍNDICE DE FIGURAS

ÍNDICE DE QUADROS

LISTA DE APÊNDICES

APÊNDICES

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AJ	Autoridade Judiciária
AM	Academia Militar
APA	*American Psychological Association*
Artigo	Art.
CDF	Comando de Doutrina e Formação
Cfr.	Conforme
CTer	Comando Territorial
DEFR	Digital Evidence First Responder
E	Entrevistado
et al.	*"et aliae"* - E outros (para pessoas)
GNR	Guarda Nacional Republicana
H	Hipótese
MP	Ministério Público
n.º	Número
NEP	Norma de Execução Permanente
NIC	Núcleo de Investigação Criminal
NTP	Núcleo Técnico-Pericial
OE	Objetivo Específico
OG	Objetivo Geral
OPC	Órgão de Polícia Criminal

PD	Pergunta Derivada
PP	Pergunta de Partida
PQ	Pergunta do questionário
PSE	Prova em Suporte Eletrónico
RCFTIA	Relatório Científico Final do Trabalho de Investigação Aplicada

INTRODUÇÃO

O recurso a meios tecnológicos ou redes é feito de forma constante por parte da maioria das pessoas na nossa sociedade. Estes, por sua vez, podem ser utilizados como meio de cometimento de ilícitos criminais e abarcar praticamente toda a tipologia de crimes existentes. Neste âmbito podemos incluir um largo espectro de situações relevantes, como por exemplo, comunicações entre suspeitos, suspeitos e vítimas, fotografias, ou vídeos.

De acordo com as competências de investigação da Guarda Nacional Republicana (GNR), o nosso trabalho incide sobre uma particular ramificação do conceito de cibercrime. Este fenómeno pode ser dividido em três: crimes nos quais os dispositivos eletrónicos ou as redes são os alvos da atividade criminosa; crimes onde o computador é uma ferramenta utilizada para a sua prática, como por exemplo pornografia infantil e fraude informática; e os crimes em que a utilização de um dispositivo tecnológico é uma ferramenta secundária para o seu cometimento, contudo pode fornecer provas relacionadas com a prática do mesmo (Clough, 2010, p. 10). Posto isto, é nesta última parte que pretendemos focar a nossa abordagem.

Uma das orientações estratégicas para o ano 2017, mencionadas no Relatório Anual de Segurança Interna (RASI), no âmbito da segurança no ciberespaço é "reforçar a área da prevenção e repressão do cibercrime e reforçar a capacidade de aquisição da prova digital" (2016, p. 231). Esta preocupação decorre do acréscimo generalizado da prática de condutas criminosa através do uso de meios informáticos ou contra um bem informático, e ainda, crimes comuns onde é cada vez mais relevante a prova eletrónica armazenada em dispositivos e nas redes (2016, p. 31).

No RASI (2016, p. 31) pode ler-se que o sucesso da prevenção e da investigação criminal nesta tipologia de crimes passa pela "formação profissional continuada". Esta determinação encontra-se igualmente patente no *Scientific working groups on Digital Evidence and Imaging Technology* (2010, p. 3) onde consta que todo o pessoal encarregue de adquirir, preservar, analisar e/ou examinar provas digitais ou multimédia deve estar a par dos procedimentos comummente seguidos pela comunidade forense e devem seguir as recomendações que os próprios emanam.

O autor Armando Dias Ramos (2017, p. 194) reforça esta ideia escrevendo que o "investigador criminal que proceda à apreensão de prova informático-digital, para além dos conhecimentos técnicos informáticos que lhe são requeridos, também terá que saber lidar convenientemente com este tipo de prova, quer na sua apreensão, manuseamento e transporte, quer na análise/exame que posteriormente irá recair sobre a mesma".

No âmbito da sua estratégia organizacional, a GNR procura a edificação e melhoria das suas capacidades operacionais através da prevenção, predição e repressão, de forma cada vez mais eficaz, das atividades criminais que decorrem de atos preparatórios com origem no ciberespaço (GNR, 2016, p. 66).

Dois dos constrangimentos apresentados no relatório de atividades da GNR, em 2017, foram a desterritorialização, mobilidade e sofisticação da criminalidade, assim como fenómenos de criminalidade associados às novas tecnologias (GNR, 2017, p. 68). Na prossecução da atividade diária foram apreendidos 3.265 telemóveis e material eletrónico (GNR, 2017, p. 12) e foram feitas 5.868 inspeções técnicas e judiciárias das quais se recolheram 1.881 vestígios de natureza tecnológica (GNR, 2017, p. 176). No âmbito da Criminalística, foram efetuadas, 1.586 pesquisas de dados informáticos em dispositivos tecnológicos, em 2017.

No âmbito da presente investigação restringimo-nos ao regime processual da lei 109/2009 de 15 de setembro (Lei do Cibercrime) que legisla sobre o conjunto de provas de comunicações preservadas ou conservadas em sistemas informáticos excluindo, por outro lado, os restantes regimes processuais como é o caso das escutas telefónicas. Pois, é este o regime processual que os militares dos Núcleos de Investigação Criminal (NIC) devem adotar no manuseamento da Prova em suporte eletrónico (PSE), juntamente, com o Código de Processo Penal[1]. Com vista a obtermos uma concordância com o ordenamento jurídico português preferimos adotar o conceito de prova em suporte eletrónico, em vez de prova digital, apesar de na presente investigação consideramos uma correspondência direta entre ambos no que concerne aos seus significados.

Desta forma, consideramos pertinente estudar as capacidades de manuseamento de prova em suporte eletrónico por parte dos investigadores operativos da GNR – os NIC.

Este trabalho foi elaborado no âmbito da estrutura curricular dos cursos ministrados e no término de cinco anos do Mestrado Integrado em Ciências Militares na Especialidade de Segurança da Academia Militar (AM). Desta forma, o tema deste Trabalho de

[1] Decreto-Lei n.º78/87, de 17 de fevereiro

Investigação Cientifica (TIA) é: "Os Núcleos de Investigação Criminal da Guarda Nacional Republicana e o manuseamento da prova em suporte eletrónico".

Considerando que a pergunta de partida (PP) é o meio "através do qual o investigador tenta exprimir o mais exatamente possível o que procura saber, elucidar, compreender melhor" (Quivy & Campenhoudt, 2008, p. 32), formulou-se então a seguinte PP: Os militares dos Núcleos de Investigação Criminal (NIC) têm capacidade para executar as diligências processuais adequadas e necessárias para manusear prova em suporte eletrónico (PSE)?

Por sua vez, surgem as PD da investigação, com o intuito de delimitarem e operacionalizem a PP:

PD_1: Quais as disposições processuais que legitimam a atividade dos militares dos Núcleos de Investigação Criminal para manusear PSE?

PD_2: Quais os conhecimentos técnicos adquiridos em formação ou trabalho em equipa para identificar, adquirir e preservar PSE?

PD_3: Quais capacidades técnicas de que os militares dos Núcleos de Investigação Criminal, enquanto *first responders*, dispõem para identificar, adquirir e preservar PSE?

PD_4: Quais as capacidade dos Núcleos de Investigação Criminal, ao nível do suporte técnico, para garantir o manuseamento da PSE, em testemunhas e vítimas, de forma manual e lógica em sede de processos crime?

A PP de investigação e as PD constituem o fio condutor do trabalho. A par com as perguntas foram formulados os objetivos de investigação, nomeadamente o objetivo geral (OG) e os objetivos específicos (OE). O objetivo geral torna explícito o problema, aumentando os conhecimentos sobre determinado assunto (Marconi & Lakatos, 2003, p. 156). Assim sendo, enuncia-se o objetivo geral da presente investigação como sendo: "Caracterizar a capacidade dos militares dos NIC da GNR no manuseamento da prova em suporte eletrónico".

Por forma a atingir o objetivo geral, surgem os objetivos específicos, que possuem um carácter mais concreto e que permitem aplicar o estudo a situações particulares (Marconi & Lakatos, 2003, p. 219). Assim, elencam-se os OE da investigação.

OE_1: Determinar se os militares dos Núcleos de Investigação Criminal têm um conhecimento atual das disposições processuais no âmbito da PSE.

OE_2: Determinar se os militares dos Núcleos de Investigação Criminal têm a formação técnica adequada para identificar, adquirir e preservar PSE.

OE_3: Analisar as capacidades técnicas (consciência/suporte técnico / formação) que os NIC têm, enquanto *first responder*, para identificar, adquirir e preservar PSE relevante em diligências processuais (no âmbito das medidas cautelares ou em buscas) em sede de processos crime.

OE_4: Analisar as capacidades técnicas que os NIC têm para adquirir e analisar PSE em testemunhas e vítimas, de forma manual e lógica em sede de processos crime.

O RCFTIA encontra-se dividido em duas partes interligadas entre si que se complementam, designadamente a Parte I – Enquadramento Teórico e a Parte II – Prática. O Enquadramento Teórico tem dois Capítulos sendo no primeiro apresentados alguns conceitos e definições relacionados com a PSE, passando pela caracterização dos crimes com recurso a meios eletrónicos. De seguida abordamos os princípios, características e fontes da PSE, terminando com as disposições processuais constantes no ordenamento jurídico português e que afetam a atividade dos NIC. No segundo capítulo analisamos a estrutura de Investigação Criminal presente na GNR; apresentamos os níveis de análise de conteúdos que se podem efetuar em termos de PSE; posteriormente, expomos o conceito de *first responder em prova digital* (DEFR), e a possibilidade de o mesmo se aplicar, em determinadas situações, aos NIC. Por fim, elencam-se dois níveis de DEFR tendo por base aquelas que são as competências dos investigadores da GNR, e que são, peça chave do nosso estudo.

A Parte II divide-se entre capítulo relativo à metodologia e procedimentos e a análise e discussão dos resultados. No primeiro apresentamos o modelo de análise, as hipóteses em estudo, a discussão e análise da fase metodológica da investigação a que recorremos, referem-se as questões relacionadas com a amostra e procedimentos de amostragem, bem como com as técnicas estatísticas utilizadas na análise dos dados. No segundo apresentados os dados recolhidos quer das entrevistas realizadas, quer dos inquéritos por questionário que foram endereçados aos militares dos NIC e que visaram contribuir para que pudessem ser dada a resposta à PP e se tecerem as devidas conclusões.

As normas utilizadas para a elaboração deste trabalho científico foram, sempre que possível, as normas da AM, redigidas na Norma de Execução Permanente (NEP) número (n.º) 520/4ª (AM - Direção de Ensino, 2015), "Normas para a Redação de Trabalhos de Investigação", e nas NEP 522/1ª (AM - Direção de Ensino, 2016), que regem a formatação do Relatório. Para a elaboração das referências bibliográficas do trabalho de investigação, optou-se pela 6ª edição das normas APA (2012) nos pontos em que a NEP 522/1ª fosse omissa.

PARTE I – ENQUADRAMENTO TEÓRICO

CAPÍTULO 1.
A PROVA EM SUPORTE ELETRÓNICO

O objetivo geral desta investigação é caracterizar as capacidades dos militares dos NIC no manuseamento da PSE. Para isso, iremos percorrer, neste capítulo, um caminho que se inicia pela apresentação de alguns conceitos e definições relacionados com esta investigação, passando pela caracterização dos crimes com recurso a meios eletrónicos. De seguida abordaremos os princípios, características e fontes da PSE, terminando com as disposições processuais constantes no ordenamento jurídico português e que afetam a atividade dos NIC.

1.1. Conceptualização de prova em suporte eletrónico

Na obra *Digital Evidence and Computer Crime*, Eoghan Casey menciona dois aspetos que influenciam a dificuldade em definir PSE. Por um lado, "as definições apresentadas focam-se demasiado na prova e negligenciam dados que podem promover uma investigação. Por outro, algumas definições restringem os dados binários aos únicos dados possíveis de ser representados informaticamente (Casey, 2011, p. 7) . Como exemplo destas incorreções apresentamos o conceito de PSE proposto pelo *Scientific Working Group on Digital Evidence: "*informação com valor probatório que é armazenada ou transmitida na forma binária[2]" (Scientific Working Group on Digital Evidence, 2016, p. 7).

A prova eletrónica pode englobar tanto a vertente digital como a analógica, como por exemplo, as fotografias em rolo fotográfico (formato analógico) que podem ser transferidas para um formato digital através de uma digitalização (Ramalho, 2017, p. 100).

Deste modo, adotamos uma definição abrangente do conceito de suporte eletrónico considerando aplicar-se a "qualquer dado guardado ou transmitido através da utilização de um computador que suporte ou refute as circunstâncias de como um crime ocorreu ou que possam provar uma intenção ou um álibi". Os dados referidos na definição apresentada

[2] Tradução nossa para: *"information stored or transmitted on binary form that may be relied upon in court*".

dizem respeito a uma combinação de números que, por sua vez, representam informação de vários tipos, incluindo, textos, imagens, áudio e vídeo (Casey, 2011, p. 7).

No que toca às comunicações efetuadas pelos utilizadores de uma rede, como por exemplo a Internet, existem três tipos de dados, conforme nos elucida o Acórdão n.º 241/2002 emitido pelo Tribunal Constitucional:

> "Os dados relativos à conexão à rede, ditos dados de base; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego; dados relativos ao conteúdo da comunicação ou da mensagem, dados de conteúdo.
>
> Os dados de base consistem nos elementos necessários ao acesso à rede por parte do utilizador, pelo que estão aqui necessariamente em causa o número e os dados através dos quais o utilizador acede ao serviço. Ora, esses elementos, de que se destacam a identificação e a morada do utilizador, são fornecidos ao explorador (operador) do serviço para efeito de ligação à rede (assinatura do contrato ou protocolo) ou são atribuídos por este ao utilizador (atribuição do respetivo número de acesso)" (Acórdão n.º 241/2002/T. Constitucional, 2002).

De acordo com Benjamim Silva Rodrigues (2009, p. 39) "a prova electrónico-digital pode definir-se como qualquer tipo de informação, com valor probatório, armazenada [em repositório electrónico-digitais de armazenamento] ou transmitida [em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital".

Segundo Ramos (2017, p. 174) , a prova em suporte eletrónico "conjuga em si vários fatores que a tornam diferente, vulnerável e especial. Por isso, a mesma assume caráter temporário, é fungível e de grande volatilidade. Destas características, que aprofundaremos o seu estudo no subcapítulo seguinte, resulta que a rapidez na sua obtenção, aliada a uma correta recolha de prova, são essenciais para o êxito da investigação e imputação dos factos ao suspeito do crime" (Ramos, 2017, p. 197). Renato Lopes Militão (s.d., p. 261) adianta que, "em face de tudo isto, as ações de investigação criminal relativas à prova digital exigem aprofundados conhecimentos informáticos e, muitas vezes, meios técnicos e tecnológicos de ponta".

1.2. A investigação de crimes com recurso a meios tecnológicos

Apesar do enorme aumento da utilização de diferentes tipos de tecnologias ter possibilitado cometer crimes de maneiras muito diferentes do que se apenas existisse um mundo físico, surgiu, pelo menos, um aspeto positivo a isto relacionado. O envolvimento de tantos instrumentos contribui para uma forte abundância de prova que pode ser apreendida e utilizada contra os seus autores, em tribunal (Casey, 2011, p. 5).

Os processos crime dependem de provas que permitam a decisão sobre a culpa ou a inocência de alguém e que podem levar, em primeiro lugar, à acusação e, posteriormente, à sua condenação[3]. As formas tradicionais da prova podem ser denominadas por provas físicas, como os documentos, fotografias, testemunhos, impressões digitais ou amostras biológicas. Por sua vez, a prova em suporte eletrónico deriva de dispositivos eletrónicos como melhor se explica no subcapítulo 1.3.2. A informação aqui contida não possui, *per si*, uma forma física (CyberCrime@IPA, 2014, p. 11).

A prova em suporte eletrónico pode ser usada na investigação e resolução de um largo espectro de crimes como o homicídio, ofensas à integridade física, violência domestica, sequestro, abusos sexuais incluindo crianças, furtos e roubos, tráfico de droga, entre outros. Importa acrescentar o facto de que o tipo de dados que incluídos neste conceito de prova pode ajudar a estabelecer o momento em que os factos ocorreram, o local onde as vitimas e os suspeitos se encontraram, com quem comunicaram e, possivelmente, a intenção do cometimento de um tipo de crime (Casey, 2011, p. 6).

Neste sentido afirma, Militão (s.d., p. 266) que, a problemática da PSE não se esgota nos crimes afetos à criminalidade informática. Num sentido amplo, este tipo de prova pode contribuir para a investigação de todos os tipos criminais. "Basta que pensemos, a título meramente ilustrativo, nas mensagens de correio electrónico ou registos de comunicações de natureza semelhante cujo conteúdo se reporte à prática de qualquer tipo criminal" (s.d., p. 267).

Contudo, existem circunstâncias em que a PSE não é diferente das provas tradicionais, na medida em que, os procedimentos legais para o seu manuseamento devem ser capazes de demonstrar as circunstâncias e informações factuais do que ocorreu na altura da prática dos atos ilícitos. Isto significa que os dados não podem ser alterados, apagados ou adicionados. A natureza intangível, *supra* descrita, de qualquer dado ou informação armazenada de forma eletrónica faz com que seja mais fácil verificarem-se

[3] Cfr. Art.º 124º do CPP

alterações ou manipulações (CyberCrime@IPA, 2014, p. 11). Desta forma, revela-se essencial que sejam conhecidas as suas características particulares e que visem a integridade da prova.

1.2.1 Caracteristicas da PSE

De seguida, apresentaremos algumas características da PSE que consideramos essenciais para a nossa investigação, segundo o Guia de Prova Eletrónica (2014):

- *Invisibilidade a olho nu*: a PSE muitas vezes encontra-se localizada em locais onde apenas pessoal especializado consegue aceder e com recurso a ferramentas específicas;
- *Altamente volátil*: existem dados que podem ser perdidos se o dispositivo for desligado como por exemplo aqueles que se encontram armazenados na memoria RAM;
- *Deve ser manuseada por pessoal certificado*: cada tipo de dispositivo eletrónico tem características específicas pelo que é necessário adaptar os procedimentos. Um dos riscos decorrentes é a alteração dos dados que podem levar à violação da integridade da prova;
- *Evolução constante das fontes de PSE*: as novas tecnologias são criadas e desenvolvidas de uma forma muito rápida. Consequentemente, torna-se necessário um acompanhamento da formação e treino de quem lida com este tipo de prova;
- *Utilização de procedimentos, técnicas e ferramentas de suporte apropriados*;
- *Admissibilidade em tribunal*: a aquisição da PSE deve ser feita em conformidade com a legislação em vigor.

1.2.2 Princípios da PSE

Como foi mencionado anteriormente, a PSE deve ser manuseada de maneira a que se mantenha uma completa e exata preservação dos dados originais e seja possível validar a admissibilidade e integridade dos mesmos (Casey, 2011, p. 232). Para isso, a Agência da União Europeia para a Segurança das Redes e da Informação (ENISA, 2014, p. 5) descreve a existência de cinco fundamentos principais para o manuseamento da PSE:

- *Integridade dos dados*: as ações dos investigadores não devem alterar nenhum dado que possa vir a ser utilizado como prova. O responsável pela aquisição de prova deve garantir a sua cadeia de custódia (Casey, 2011, p. 21). Como forma de garantir esta integridade, alguns autores defendem como essencial o registo de valores *hash*. Estes valores são considerados impressões digitais dos ficheiros pois cada um possuí um número irrepetível. Desta forma é possível perceber se aquele determinado ficheiro se mantém igual ao original ou se, pelo contrário, foi modificado. Outro método que pode ser aplicado para garantir a integridade dos dados consiste em aceder ao dispositivo no modo "somente leitura". Este processo é efetuado usando um dispositivo denominado por bloqueadores de escrita (CyberCrime@IPA, 2014) ;
- *Registos de controlo*: todas as ações no manuseamento da PSE como a pesquisa, apreensão, armazenamento ou transferências, devem ser devidamente documentadas, preservadas, assim como, manterem-se disponíveis;
- *Treino e formação apropriado*: os *first responders* devem ter a formação adequada para efetuarem a pesquisa e apreensão da PSE no caso de não existirem especialistas no local;
- *Legalidade*: o investigador é responsável por assegurar que todos os procedimentos se encontram de acordo com a lei.

O autor português Benjamim Rodrigues Silva (2011, pp. 44-46) apresenta um conjunto de princípios que vão ao encontro daqueles mencionados em *supra*. Estes são: o *princípio da não alteração da prova no ato de recolha*, onde o investigador não deve tomar ações que contaminem os dados; *princípio da especialização ou qualificação do pessoal adstrito à investigação forense digital*, ressalvando a necessidade de todos os intervenientes serem dotados de conhecimentos técnicos de acordo com o seu nível de intervenção; *o princípio da garantia de documentação em todas as fases processuais* com vista a garantir a integridade da cadeia de controlo ou cadeia de custódia e; *o princípio da responsabilidade pessoal*, dado que todos os intervenientes no manuseamento da PSE são responsáveis por garantir a sua admissibilidade.

1.2.3 Fontes de PSE

A definição de sistema informático apresentada na Lei do Cibercrime abrange portáteis, tablets, smartphones e outros dispositivos eletrónicos:

> *a) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção*[4]*;*

Os investigadores devem considerar que qualquer equipamento eletrónico pode conter provas relevantes. Segundo o Electronic Evidence Guide (2014, p. 16) a presença desses equipamentos pode não ser óbvia do ponto de vista de um investigador com pouca formação ou experiência nesta área.

Eoghan Casey, no que toca às fontes de PSE, apresenta três grupos de sistemas informáticos nos quais podemos enquadrar todos os tipos de equipamentos apresentados. Em primeiro, os sistemas abertos, que compreendem os computadores sejam fixos ou portáteis, e os servidores, assim como todos os periféricos. Nestes sistemas podem ser armazenados grandes quantidades de documentos e os detalhes dos mesmos como, a data de criação, quem criou os dados, datas que podem ser importantes numa investigação (Casey, 2011, p. 36).

Em segundo, os sistemas de comunicações, onde se enquadram os sistemas de rede móvel, ligações *wireless*, a internet ou outras redes. Nestes casos pode ter-se conhecimento não apenas de dados relativos ao conteúdo das comunicações mas também a dados de base como a data do envio, quem enviou, quem recebeu e a localização dos dispositivos[5].

Por último, os sistemas *embedded*, incluem os equipamentos móveis como os smartphone, sistemas de navegação por satélite, camaras fotográficas ou de vídeo digitais que também podem incluir informações determinantes para uma investigação. Um GPS pode fornecer dados relativos ao percurso de um determinado veículo, por exemplo (Casey, 2011, p. 36).

Os dispositivos de armazenamento de dados podem ser de vários tipos pelo que apresentamos alguns:

[4] Cfr. Art. 2º, al. a) da Lei 109/2009 de 15 de setembro

- Hard discs drives (HDD) e Solid state disk (SSD);
- CD, DVD, Blue-ray Disc;
- Cartões de memória;
- Dispositivos USB;
- Periféricos – ex. scanners, impressoras, leitores de cartões;
- *Tablet*;
- *Smartphone*;
- Câmaras digitais;
- Câmaras CCTV;
- HUB, *Switch* e *router*;
- Servidores

1.3.4 Disposições processuais

Neste subcapítulo iremos analisar a Lei 109/2009 que aprova a Lei do Cibercrime (LCB). A mesma decorre da Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro e adapta o Direito Interno à convenção sobre o Cibercrime do Conselho da Europa. Este diploma legal surge pela "necessidade de harmonização das várias legislações europeias na matéria, propiciando e facilitando a cooperação internacional e as investigações de natureza criminal" (Verdelho, Bravo, Rocha, & Veiga, 2003, p. 10).

No Artigo 1º é estabelecido o objeto deste diploma sendo que, por um lado, do Art. 3º ao 10º estão catalogados um conjunto de disposições penais[6] e, por outro, no Capitulo III, encontram-se dois regimes processuais de PSE. O primeiro consta nos Arts. 12º a 17º e configura as disposições centrais para a nossa investigação, pois dizem respeito às situações em que está em causa a "pesquisa e recolha, para prova, de dados já produzidos mas preservados e armazenados"[7] . O segundo regime processual que consta no Art. 18º da LCB diz respeito "à interceção de comunicações eletrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático" [8].

[6] A Lei do Cibercrime engloba entre os Arts. 3º e 8º, os crimes de Falsidade Informática, Dano relativo a programa ou outros dados informáticos, Sabotagem Informática, Acesso Ilegítimo, Interceção Ilegítima, e Reprodução Ilegítima de programa protegido.

[7] Cfr. Acórdão do TRE, de 20 de Janeiro de 2015, proc. 648/14.6GCFAR-A.E, rel. João Gomes de Sousa, *in* http://www.dgsi.pt, acedido e consultado em 18 de Março de 2019.

[8] Cfr. Acórdão do TRE, de 20 de Janeiro de 2015, proc. 648/14.6GCFAR-A.E, rel. João Gomes de Sousa, *in* http://www.dgsi.pt, acedido e consultado em 18 de Março de 2019.

No âmbito deste TIA iremos, portanto, abordar os Arts. 12º, 15º e 16º (preservação, pesquisa e apreensão de dados, respetivamente), tendo como foco os crimes "em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico"[9], ou seja, procedimentos processuais que visem a obtenção de prova resultante de qualquer infração penal[10]. Assim, estas disposições afiguram-se "de aplicação geral (...) estando em causa criação de meios de obtenção de prova digitais para o combate da criminalidade, seja qual for a sua forma" (Venâncio, 2011, p. 90). Em análise a este diploma legal refere Paulo Dá Mesquita (2010, p. 98) que "as regras de direito probatório previstas não são assim meras normas processuais sobre *cibercrimes* ou sequer apenas relativas a crimes praticados em *sistemas informáticos*, mas correspondem a um regime consideravelmente mais abrangente sobre *prova electrónica* em processo penal aplicável a qualquer crime".

O Art. 12º tem como epigrafe a "preservação expedita de dados e aplica-se nas situações em que se visa obter dados informáticos específicos armazenados num sistema informático incluindo dados de trafego". A aplicação deste Art. tem como requisitos o receio de os dados poderem perder-se, alterar-se ou deixarem de estar disponíveis[11] e, desta forma, consiste na sua preservação, por parte do fornecedor de serviço, de modo a permitir a sua obtenção por parte da AJ competente[12].

Por sua vez, a AJ deve ordenar a preservação[13], excetuando-se os casos de urgência ou perigo na demora em que esta ordem pode ser dada, ao fornecedor do serviço, pelo OPC[14]. Nestes casos deve a AJ ser imediatamente informada, através de um relatório previsto no Art. 254º do CPP. Na ordem da preservação deve constar: "a) a natureza dos dados; b) a sua origem e destino, se forem conhecidos; e c) o período de tempo pelo qual deve ser preservados, até ao máximo de três meses[15]. Estes podem ser renovados por iguais períodos de tempo até ao limite de um ano[16]".

O Art. 15º diz respeito à pesquisa de dados informáticos relativamente a situações em que decorra um processo com o intuito de serem obtidos "dados específicos e determinados, armazenados num sistema informático conhecido". De acordo com os mesmos trâmites que o Art. relativo à preservação, a AJ deve ordenar, através de despacho,

[9] Cfr. Art. 11º, n.º2, al. c).
[10] Cfr. Art. 14º, n.º2, al. c) da Convenção sobre o Cibercrime.
[11] Cfr. Art. 12º, n.º1.
[12] Cfr. Art. 12º, n.º4.
[13] Cfr. Art. 12º, n.º1.
[14] Cfr. Art. 12º, n.º2.
[15] Cfr. Art. 12º, n.º3, a), b) e c
[16] Cfr. Art. 12º, n.º5.

a pesquisa de dados[17]. Contudo, o OPC pode proceder à pesquisa sem prévia autorização. Estas situações verificam-se, admissíveis, quando exista consentimento voluntário de quem detenha os dados, devendo o mesmo ser documentado, assim como nos casos de terrorismo, criminalidade violenta ou altamente organizada, onde exista risco iminente para a vida ou situações de ofensa à integridade física graves[18].

Por sua vez, o Art. 16º estabelece as disposições processuais para a apreensão de dados informáticos. A aplicabilidade deste Art. diz respeito a situações onde no decurso de uma pesquisa informática sejam encontrados dados ou documentos informáticos necessários à produção de prova e, por isso, seja necessário proceder à apreensão dos mesmos[19]. A apreensão deve ser feita sob despacho da AJ apesar de poderem também ser efetuadas sem autorização prévia nos caso em que esteja a ser efetuada, pelo OPC, uma pesquisa de dados ou exista urgência ou perigo na demora[20].

Nos casos de o conteúdo apreendido ser suscetível de revelar dados pessoais íntimos, os mesmos devem ser apresentados ao juiz, que ponderará a sua junção aos autos. As apreensões devem ser sempre validadas, no prazo máximo de 72 horas pela AJ[21], como também faz referência o CPP no Art. 178º, n.º6.

Relativamente aos modos de apreensão pode ser realizada: "a) apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respetiva leitura; b) uma cópia dos dados, em suporte autónomo, que será junto ao processo; c) preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou d) a eliminação não reversível ou bloqueio do acesso aos dados".

No que concerne ao Art.17º, o mesmo visa legislar sobre a apreensão de correio eletrónico e registos de comunicação de natureza semelhante, onde se podem incluir as mensagens de SMS ou conversas em redes sociais. Neste âmbito vem esclarecer o Ac. do TRP de 12-09-2012 que a lei do Cibercrime e, particularmente, o Art. em apreço não vem distinguir correspondência fechada ou não lida daquela que tenha sido aberta ou lida. Posto isto, a leitura e apensão do conteúdo aqui tratado dependem da autorização do JIC "mesmo

[17]Cfr. Art. 15º, n.º1.
[18] Cfr. Art. 15º, n.º3.
[19] Cfr. Art. 16º, n.º1)
[20] Cfr. Art. 15º, n.º2)
[21] Cfr. Art. 15º, n.º3 e 4)

que esta resulte de uma pesquisa de dados validamente ordenada pelo MP[22]. Nestas situações pode ainda, segundo a jurisprudência, o MP autorizar a apreensão provisória dos dados de conteúdo das comunicações. Contudo, "deve depois ser o juiz a ordenar a apreensão definitiva"[23].

[22] Cfr. Acórdão do TRP, de 12 de setembro de 2012, proc. 787/11.5PWPRT.P1, rel. Alves Duarte, *in* http://www.dgsi.pt, acedido e consultado em 18 de março de 2019.

[23] Cfr. Acórdão do TRE, de 20 de março de 2011, proc. 735/10.0GAPTL – A.G1, rel. Maria José Nogueira, *in* http://www.dgsi.pt, acedido e consultado em 18 de março de 2019.

CAPÍTULO 2.
A PROVA EM SUPORTE ELETRÓNICO NA INVESTIGAÇÃO CRIMINAL DA GUARDA NACIONAL REPUBLICANA

Em 2012 a polícia metropolitana de Londres via implementado, em 16 postos policiais, um sistema que permitia extrair dados dos dispositivos móveis, como *smartphones*, dos suspeitos detidos. Esta informação incluía registos de chamadas, mensagens e contactos. Até àquela data, os polícias desta força de segurança enviavam os dispositivos para análise forense demorando este processo várias semanas. Com implementação deste sistema, os dados passaram a ser extraídos, no momento. Foram também criadas linhas orientadoras acerca da extração desses dados, onde entre outras coisas, se esclarecia que apenas se poderia realizar a extração quando existissem suficientes suspeitas de que aquele equipamento havia sido utilizado para a prossecução de uma atividade criminosa. Por outro lado foram treinados cerca de 300 polícias na área da aquisição de dados dos equipamentos tecnológicos, para que pudessem operar com esse sistema [24].

Neste capítulo iremos, primeiramente, analisar a estrutura de Investigação Criminal presente na GNR. De seguida, iremos apresentar os níveis de análise de dados que se podem efetuar em termos de PSE. Posteriormente, apresentaremos o conceito de *first responder em prova digital* (DEFR), e a possibilidade de o mesmo se aplicar, em determinadas situações, aos NIC. Por fim, pretendemos elencar dois níveis de DEFR tendo por base as competências dos investigadores da GNR, e que são peça chave do nosso estudo.

2.1. Investigação criminal na GNR

O conceito de Investigação criminal encontra-se previsto na Lei de Organização da Investigação Criminal[25], doravante designado por LOIC, e "compreende o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as

[24] Lee, D. (2012). *Met Police to extract suspects' mobile phone data.* Obtido em 26 de 04 de 2019, de BBC: https://www.bbc.com/news/technology-18102793

[25] Lei 49/2009 de 27 de agosto (Assembleia da República, 2007)

provas, no âmbito do processo"[26]. A notícia dos crimes pode ser dada a conhecer ao Ministério Público pelos Órgãos de Polícia Criminal (OPC), nos casos em que estes presenciem os mesmos ou quando destes tenham conhecimento levantando sempre auto de notícia[27] .

A Lei Orgânica da GNR aprovada em 6 de novembro de 2007 define no seu Título I que a "GNR é uma força de segurança de natureza militar" com uma missão geral de "assegurar a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos". Para a prossecução desta missão executa, entre outras tarefas, o "desenvolvimento de ações de investigação criminal que lhe sejam atribuídas por lei, delegadas por autoridades judiciárias ou solicitadas por autoridades administrativas". A competência da Guarda para a "investigação dos crimes cuja competência não esteja reservada a outros OPC's é considerada genérica[28].

Para além disto, a GNR pode iniciar de imediato a investigação e praticar os atos cautelares e necessários para garantir a inviolabilidade dos meios de prova que decorram do conhecimento de qualquer crime[29].

Quer estejamos no âmbito dos meios de obtenção de prova ou das medidas cautelares e de polícia, os atos processuais podem ser efetuados através dos diferentes níveis de intervenção processual penal que compõem o dispositivo da GNR, nomeadamente, o OPC genérico, as secções de inquérito dos Postos Territoriais e pela estrutura de IC. Esta última "é caraterizada pela sua tripla valência: operativa, criminalística e de análise de informação" (Branco, 2010 cit in Mateus, 2016, p. 4).

Tendo por base o Despacho 18/14, que estabelece a organização da estrutura de IC da GNR, Mateus (2016) refere que "na vertente operativa a GNR é composta por vários tipos de núcleos IC que estão distribuídos pelos Comandos Territoriais (CTer) sendo que os NIC encontram-se fisicamente sediados nos Destacamentos Territoriais (DTer), embora dependam funcionalmente das Secções de Informações e Investigação Criminal (SIIC) dos CTer. Por sua vez, a vertente de criminalística é composta pelos Núcleos de Apoio Técnico (NAT), sediados em cada CTer, e pelos Núcleos Técnico-Periciais (NTP). No que toca à digital forense a estrutura está disseminada por um NTP em Coimbra, e duas equipas em Faro e no Porto e uma Secção de Recolha de Prova Digital no órgão técnico sediada na

[26] Cfr. Art. 1º da Lei n.º 49/2008 de 27 de agosto;
[27] Cfr. Art. 241º e 242º, n.º 1, al. a), Art.º 243º, n.º 1 e Art.º 248º, n.º1, todos do DL 78/87 de 17 de fevereiro;
[28] Cfr. Art. 6º da Lei no 49/2008 de 27 de agosto;
[29] Cfr. Art. 249º n.º 1, 2 e 3 do DL 78/87 de 17 de fevereiro;

Divisão de Investigação Criminal (DIC) em Lisboa. Por último, a vertente de análise de informação é composta pelos Núcleos de Análise de Informações e Informação Criminal (NAIIC) (Mateus, 2016, p. 5).

2.2. First responders de PSE

Benjamin Silva Rodrigues (2011, p. 31) alertava para a necessidade de os responsáveis pela investigação criminal estarem capacitados de recursos humanos e mecanismos técnicos e tecnológicos adequados e eficazes nas respostas às já mencionadas características e princípios próprios da PSE. Neste sentido é fundamentado, por um lado, a criação de unidades especializadas, dentro das Forças e Serviços de Segurança e, por outro o desenvolvimento da ciência digital forense que visa encaminhar a investigação criminal, dentro do âmbito da criminalidade informático-digital, para as diligências processuais específicas. Incluem-se aqui a preservação, recolha, gravação, validação, identificação, análise, interpretação, documentação e apresentação desta tipologia de prova.

Um órgão de polícia criminal deve ter conhecimento de todos os procedimentos e técnicas operacionais padrão adequadas, assim como aplicar todos os princípios, mencionados anteriormente, que garantam a qualidade no manuseamento de PSE. No decurso de uma investigação, os investigadores podem deparar-se com situações onde se enquadrem um ou mais dos seguintes níveis de análise e devem, portanto, ter o nível adequado de formação para realizar esses exames, ou ter conhecimento de quem deve contactar para a realização dos mesmos (Scientific Working Group on Digital Evidence, 2013, p. 4).

Os níveis de análise dependem do pedido e das especificidades da investigação. Níveis mais elevados de análise exigem um exame mais abrangente, habilidades adicionais e podem não ser aplicáveis ou possíveis para cada dispositivo ou situação. Os níveis são os seguintes: a) *manual* – um processo que envolve a operação manual do teclado e do visor do aparelho para documentar os dados presentes na memória interna do telemóvel (pode ser feito em qualquer local); b) *lógico* – um processo que fornece acesso aos arquivos acessíveis ao usuário. Esse processo não permite aceder, normalmente, a dados eliminados (pode ser feito em qualquer local); c) *Hex Dump* – um processo que fornece uma aquisição física de dados de um dispositivo e que permite fornecer acesso a dados eliminados mas que ainda não foram substituídos (pode ser feito em qualquer local); d) *chip-off* – um processo que envolve a remoção de um chip de memória para realizar a análise (deve ser

feito em laboratório); e) *MicroRead* – processo que envolve o uso de um microscópio de alta potência para fornecer uma visão física do circuito eletrónico de memória. Este método deve ser usado para adquirir dados de chips de memória danificados fisicamente (deve ser feito em laboratório) (Scientific Working Group on Digital Evidence, 2013, p. 5).

Os *first responders da prova em suporte eletrónico (DEFR*[30]*)* podem ser definidos como indivíduos responsáveis pela aquisição e por exames básicos a dispositivos eletrónicos como os *smartphones* (ISO, 2012, p. 6). O SWGDE apresenta dois níveis de DEFR. Os *DEFR* de nível 1 são indivíduos capazes de adquirir ou examinar manualmente os dispositivos mobile como *smartphones*. Por sua vez, os *first responders* de nível 2 são profissionais capazes de utilizar ferramentas ou *software* para extrair dados dos mesmos dispositivos eletrónicos. Contudo, importa referir que o uso de qualquer ferramenta para extrair dados de um dispositivo exige treino e formação (Scientific Working Group on Digital Evidence, 2013, p. 5).

2.2.1 Competências essenciais para first responders de nível 1

As competências supramencionadas descrevem os requisitos mínimos para um *first responder* analisando manualmente um dispositivo eletrónico sem o uso de uma ferramenta de exame. Um exemplo de um FR de nível 1 seria um investigador numa situação em que o mesmo se depara com um smartphone durante o curso de uma investigação (Scientific Working Group on Digital Evidence, 2013, p. 6). Desta forma tentaremos relacionar este conjunto de competências com aquelas que são as funções dos NIC.

Os exames manuais acima mencionados incluem: a) navegar através de um *smartphone* para visualizar os dados armazenados; b) fotografar ou filmar os dados encontrados através do ecrã; ou c) transcrever manualmente os dados visualizados para um auto (Scientific Working Group on Digital Evidence, 2013, p. 6).

Para executar corretamente os exames manuais, os DEFR de nível 1 devem ser conhecedores dos seguintes aspetos: a) manuseamento, etiquetagem, preservação e apreensão de PSE (por exemplo, obter códigos PIN ou padrões de bloqueio do ecrã, antes da apreensão); b) consequências e riscos associados à manipulação do dispositivo a ser examinado; c) modificação de dados se forem colocados diferentes cartões SIM ou de memória nos computadores ou telemóveis; d) remover e substituir baterias pode fazer com

[30] Em inglês *Digital Evidence First Responders*

que o dispositivo reinicie e se percam dados; e) disposições processuais aplicáveis, como por exemplo, necessidade de autorização judicial ou Termo de Consentimento; f) importância de documentar adequadamente todos os equipamentos apreendidos e quais as ações feitas nos mesmos (Scientific Working Group on Digital Evidence, 2013, p. 6).

2.2.2 Competências essenciais para first responders nível 2

Relativamente aos DEFR de nível 2, os mesmos devem ser capazes de ter em consideração todos os pontos que mencionamos anteriormente mais aqueles que elencaremos de seguida. Neste tipo de situações são utilizados *software*s para extrair dados. A presente norma ISO, apresenta como um exemplo de DEFR nível 2 um investigador devidamente formado e treinado para através de um *software* analisar um telemóvel, extraindo os dados necessários, por exemplo. Para isso, são efetuados exames lógicos aos dispositivos que permitem conhecer, entre outras coisas, a lista de contactos, histórico de chamadas, mensagens de texto, imagens, vídeos, áudios, e-mails, dados de aplicações, histórico da Web, calendário e notas (ISO, 2012, p. 42).

Estes DEFR devem então ser capazes de: identificar quais as informações que podem ser armazenadas num dispositivo, num cartão SIM ou ainda noutros locais; isolar um telemóvel do sinal do provedor, por exemplo, através da colocação em modo voo; capacidade de explicar as vantagens e desvantagens de desligar os dispositivos relativamente à volatilidade dos dados; conhecimento das funcionalidades do *software* de extração de dados, como por exemplo, entender que os exames lógicos não permitem recuperar dados apagados dos dispositivos, cartões SIM ou cartões de memória; entender as diferenças entre as mensagens lidas das não lidas e como o processamento de um dispositivo as pode alterar; conhecer as implicações legais de abrir mensagens não abertas; capacidade de defender em tribunal o uso das ferramentas ou *softwares* utilizados (ISO, 2012, p. 18).

PARTE II – PRÁTICA

CAPÍTULO 3.
METODOLOGIA E PROCEDIMENTOS

Neste capítulo apresenta-se o modelo de análise proposto, assim como as hipóteses em estudo nesta investigação. Expõe-se também a discussão e análise da fase metodológica da investigação a que recorremos durante a realização da mesma. Refere-se igualmente questões relacionadas com a amostra e procedimentos de amostragem, bem como com as técnicas estatísticas utilizadas na análise dos dados.

Trata–se de um capítulo essencial, do ponto de vista da estruturação do processo de investigação que antecede a análise e discussão dos dados propriamente dita, quer na sua abordagem qualitativa, quer na perspetiva quantitativa, assim como na combinação de ambos os métodos. Comecemos então, pela génese da investigação científica.

A Metodologia aplicada em determinada investigação permite "que o investigador seja capaz de conceber e de pôr em prática um dispositivo para a elucidação do real, isto é, no seu sentido mais lato, um método de trabalho (...) como um percurso global do espírito que exige ser reinventado para cada trabalho" (Quivy & Campenhoudt, 2008, p. 15). Segundo Carvalho (2009, p.42) cit. in (Santos, et al., 2016) este tipo de investigação – Aplicada– "tem por objetivo encontrar uma aplicação prática para novos conhecimentos adquiridos no decurso da realização de trabalhos originais.

3.1. Modelo de análise

Por forma a estruturar a investigação e permitir materializar o método científico bem como o tipo de abordagem, que será explicado posteriormente, surge a necessidade de prosseguir um modelo de análise (Cfr. Apêndice A) que oriente a investigação. Assim, Quivy e Campenhoudt (Quivy & Campenhoudt, 2008, p. 150) descrevem-no como "o prolongamento natural da problemática, articulando de forma operacional os marcos e as pistas que serão finalmente retidos para orientar o trabalho de observação e de análise".

A exploração da temática que esta investigação encerra levou à elaboração da Pergunta de Partida (PP) consubstanciada no seguinte: "Os militares dos Núcleos de Investigação Criminal têm capacidade para executar as diligências processuais adequadas e necessárias para manusear a prova em suporte eletrónico?"

Seguidamente, no intuito de operacionalizar a Pergunta de Partida elaboraram-se as seguintes Perguntas Derivadas (PD):

PD.1 – Os militares dos Núcleos de Investigação Criminal têm capacidade para executar as diligências processuais adequadas e necessárias para manusear a prova em suporte eletrónico?

PD.2 – Quais os conhecimentos técnicos adquiridos em formação ou trabalho em equipa para identificar, adquirir e preservar PSE?

PD.3 – Os militares dos NIC dispõem de capacidades técnicas, enquanto *first responders*, para identificar, adquirir e preservar PSE?

PD.4 – Quais as capacidades dos Núcleos de Investigação Criminal, ao nível do suporte técnico, para garantir o manuseamento da PSE, em testemunhas e vítimas, em sede de processos crime?

3.2. Metodologia e tipos de abordagem

A problemática da prova em suporte eletrónico, tem sido alvo de vários estudos conforme demostra a bibliografia apresentada, o que revela diferentes tipos de abordagens. Para além das respostas quanto às capacidades dos NIC para manusear PSE, as dificuldades que a esta dizem respeito e os requisitos para que se verifiquem melhorias, pretende-se retirar ilações sobre o papel deste tipo de prova como contributo para a eficácia da Investigação Criminal.

Desta forma, para podermos alcançar os objetivos estabelecidos, foi adotado o método indutivo, proposto por Francis Bacon (Oliveira, 2011).“Este método fundamenta-se num raciocínio baseado na experiência, que parte do particular para o geral” (Sarmento, 2013, p. 8). De acordo com (Marconi & Lakatos, 2003, p. 86), este método consiste num “processo mental por intermetido do qual, partindo de dados particulares, suficientemente constatados, infere-se uma verdade geral ou universal”. Tendo em conta as palavras de Guerra (2006, p. 22), o método indutivo é diferente dos restantes pelo facto de que a “intenção dos investigadores não é comprovar hipóteses definidas a priori e estanques, mas antes identificar as lógicas e racionalidades dos atores confrontando-as com o seu modelo de referência”.

O método indutivo verifica-se de uma forma faseada em três etapas (Prodanov, 2013, p. 23). Em primeiro lugar estabelece-se uma observação dos factos, de seguida,

descobrem-se as relações entre esses factos e, por último estabelecem-se relações gerais relativamente àquilo que de comum se verifica.

A presente investigação segue uma abordagem qualitativa, por um lado, e quantitativa, por outro. A primeira, segundo Fortin (2009, p. 32), pretende "descobrir, explorar, descrever fenómenos e compreender a sua essência". A investigação de cariz qualitativo apresenta-se como preponderante na área das ciências sociais por ser "particularmente importante para o estudo das relações sociais, dada a pluralidade dos universos de vida" (Flick, 2005, p. 2). Neste sentido, recorda Freixo (2012, p. 173) que "o objetivo desta abordagem de investigação utilizada para o desenvolvimento do conhecimento é descrever ou interpretar, mais do que avaliar (...) é uma extensão da capacidade do investigador em dar um sentido ao fenómeno".

Na segunda abordagem, quantitativa, recorreu-se a um "processo sistemático de colheita de dados observáveis e quantificáveis" (Fortin, 2009, p. 22) relativamente a uma dimensão de análise, nomeadamente, um questionário respondido pelos militares dos NIC.

3.2.1. Abordagem qualitativa

No que concerne à abordagem qualitativa, a investigação iniciou-se com uma análise documental, conduzindo-se a revisão da literatura acerca da temática.

A consulta dos documentos que preenchem a análise do estado da arte foi conduzida recorrendo a bibliografia escrita, bases de dados *online* e portais, repositórios institucionais, motores de busca, revistas eletrónicas e bibliotecas digitais.

Após a análise documental, iniciamos o trabalho de campo através da realização de entrevistas presenciais. Estas, através da informação que permitem obter, constituem-se como "elementos de reflexão muito ricos e matizados" (Quivy & Campenhoudt, 2008, p. 192) permitindo retirar fundadas conclusões acerca da problemática em estudo. Acrescenta Sarmento (2013, p. 31) que estas conferem ao investigador a "oportunidade para esclarecer alguma resposta do entrevistado, no decorrer da entrevista, compreender e aprofundar o conhecimento sobre factos, informações e situações, recorrendo a entrevistados, que são peritos ou especialistas na matéria, ter oportunidade para inquirir novas perguntas".

Os entrevistados receberam previamente o guião das entrevistas acompanhado de uma Carta de Apresentação (Cfr. Apêndices E e F) para que tivessem oportunidade de refletir sobre as mesmas. Na condução destas, assumiu-se uma forma semi-estruturada,

pois o entrevistado respondeu às perguntas do guião, mas também pôde falar sobre outros assuntos relacionados (Sarmento, 2008, p. 17).

Segundo Guerra (Guerra, 2006, p. 53), "o mais importante é a clarificação dos objetivos e dimensões de análise da entrevista." Neste sentido, o guião de entrevista foi estabelecendo forte correspondência entre as questões do mesmo e as perguntas derivadas, e estas alinhadas com os objetivos da investigação. Assim, estabeleceu-se um fio condutor entre a pergunta de partida, as perguntas derivadas, o objetivo geral e objetivos específicos, bem como todas as perguntas constantes no guião de entrevista.

3.2.2. Abordagem quantitativa

Foram também aplicados questionários com o intuito de "recolher informação factual sobre acontecimentos ou situações conhecidas, sobre atitudes, crenças, conhecimentos, sentimentos e opiniões" (Norwood, 2000) cit. in (Fortin, 2009, p. 380). A escolha pela opção do inquérito por questionário como meio de recolha de dados resultou do facto do universo em estudo ser elevado e da sua dispersão por todo o território nacional.

O questionário foi aplicado por administração direta, visto que foi o próprio inquirido que o preencheu (Quivy & Campenhoudt, 2008). As questões são todas fechadas no que respeita à forma, pois as respostas são pré-estabelecidas (Sarmento, 2013). Foram usadas duas das três categorias de questões fechadas neste questionário: uma questão de resposta múltipla, em que "o inquirido escolhe as que entender, do conjunto de respostas possíveis, pode escolher uma, todas ou algumas" (Sarmento, 2013, p. 107); e, as restantes, questões de resposta com escala em que "há apenas uma resposta possível para a pergunta, que apresenta graduação" (Sarmento, 2013, p. 106), tendo-se optado pela Escala de Likert, impar com cinco níveis, para avaliar o grau de concordância desde o *discordo totalmente* (nível 1), até ao *concordo totalmente* (nível 5), o que possibilita ao inquirido optar por um valor positivo, um valor negativo ou um valor neutro.

A versão preliminar foi testada e validada com a elaboração de um pré-teste junto de um painel composto por pessoas que integram a amostra, nomeadamente elementos dos NIC de Mirandela, Albufeira e Viana do Castelo. Através do *feedback* deste painel que preencheu o pré-teste, transformou-se o questionário pré-definitivo em definitivo, modificando-se algumas questões de terminologia.

3.3. Tratamento e análise de dados

Segundo Quivy e Campenhoudt (2008, p. 185), "os métodos de recolha e os métodos de análise dos dados são normalmente complementares e devem, portanto, ser escolhidos em conjunto, em função dos objetivos de trabalho".

3.3.1. Tratamento e análise das entrevistas

De acordo com Guerra (2006), se possível, as entrevistas devem ser gravadas e acompanhadas de notas tomadas pelo investigador. Neste sentido, todas as entrevistas decorreram de forma presencial, gravadas e tomados os apontamentos julgados necessários. Continua a autora destacando que a transcrição destas é aconselhável, atendendo ao tempo disponível, e julgado pertinente, pelo que foram transcritas integralmente todas as entrevistas.

De acordo com esta autora, durante a leitura das entrevistas procede-se a uma análise temática, que consiste na informação mais sintetizada, e a uma análise problemática, que se prende com os pontos incontornáveis que surgem das respostas dos entrevistados (Guerra, 2006). Acrescenta Sarmento (2013, p. 53) que "a análise de conteúdo consiste em efetuar a categorização dos dados brutos da entrevista, que passam a dados organizados e com sentido bem estabelecido". Neste sentido, procedeu-se à leitura das entrevistas e sintetizaram-se os dados recolhidos, por forma a categorizar por um lado, as respostas dadas e argumentos apresentados como fundamento.

A análise das entrevistas consiste na contraposição das diferentes perspetivas, recorrendo às ideias-chave nas respostas dos entrevistados às questões colocadas. Assim, Guerra (2006, p. 73) entende esta análise como "sínteses dos discursos que contêm a mensagem essencial da entrevista e são fiéis, inclusive na linguagem, ao que disseram os entrevistados". Por último, a autora reitera a diminuição substancial da quantidade de informação, pois contrapondo as perspetivas e posições dos entrevistados, subjacentes às categorizações, é possível discernir acerca do conteúdo ao qual deve conceder-se importância.

Nos quadros onde constam as diferentes respostas e argumentos apresentados pelos entrevistados, salientámos aqueles que se destacaram, bem como as colunas onde constam a posição dos entrevistados da GNR e do MP (E1, E2, E3 e E4). Assim, torna-se mais fácil triangular a forma como os NIC se colocam em matéria de prova em suporte eletrónico.

3.3.2. Tratamento e análise dos questionários

Os inquéritos por questionário foram realizados a partir do Google Forms, tendo sido previamente testados. Posteriormente, seguiram para serem autorizados superiormente antes de distribuídos pelo dispositivo da GNR que serviu de amostra, autorização esta que foi concedida e foram assim, partilhados pelos respondentes.

Os resultados dos inquéritos por questionário, bem como das entrevistas apresentam- se no Capítulo seguinte da presente investigação.

3.4. Caracterização do contexto de observação

"Na seleção do processo de amostragem desenvolve-se um procedimento sistemático de recolha de dados que assegure a fiabilidade e a comparabilidade desses dados". Por isso, "o processo de amostragem deverá ser escolhido, de tal modo que a amostra final seja representativa da população" (Sarmento, 2013, p. 75).

No que toca aos questionários, esta investigação teve como população, os elementos dos NIC de todo o país, o que perfaz um universo de 553 indivíduos. Quanto às entrevistas, foram inquiridos os chefes de SIIC de Bragança e de Setúbal e dois Magistrados do MP. Os primeiros, por um lado, são os superiores hierárquicos imediatamente acima dos NIC e por isso detêm uma responsabilidade acrescida sobre o conhecimento e atuação dos investigadores e, por outro, os Procuradores do MP que enquanto titulares da ação penal dirigem e delegam os inquéritos à GNR.

Ainda assim, os indivíduos selecionados contam com uma vasta experiência a nível investigação criminal e da valoração dos meios de prova. Destas entrevistas foram apenas transcritos os excertos imprescindíveis para a investigação.

Através desta estruturação do contexto de observação foi possível atingir a diversidade e saturação. Como refere Guerra (2006, pp. 40, 41), "a diversidade relaciona-se com a garantia de que a utilização das entrevistas se faz tendo em conta a heterogeneidade dos sujeitos ou fenómenos que estamos a estudar". Neste âmbito, consideramos que a aplicação de entrevistas aos chefes de SIIC de Bragança e de Setúbal e a dois Magistrados do MP permitiu atingir-se uma diversidade essencialmente externa, na medida em que foi possível obter contributos de militares da instituição e de elementos externos à mesma. A saturação diz respeito ao ponto em que durante a recolha de dados, por intermedio das entrevistas, se verificam continuadas repetições da mesma informação. Assim, atinge-se a saturação quando "depois de um certo número de entrevistas, o

investigador – ou a equipa – tem a noção de nada recolher de novo quanto ao objeto de pesquisa" (Guerra, 2006, p. 42).

Através da aplicação de questionários aos NIC foi possível atingir uma diversidade interna, na medida que se obteve a perceção de militares de diferentes Unidades da Guarda, com características de serviço operacional distintas.

CAPÍTULO 4.
ANÁLISE E DISCUSSÃO DOS RESULTADOS

No presente capítulo, são apresentados e analisados todos os dados recolhidos através dos inquéritos por questionário e das entrevistas realizadas. De seguida é exposta a análise estatística e a análise de conteúdo desses mesmos dados. Num terceiro e último momento, interpretam-se e discutem-se os dados obtidos, comparando os mesmos com resultados de investigações anteriores, mencionadas no enquadramento teórico.

4.2. Análise e Discussão das Entrevistas

A análise qualitativa e quantitativa das entrevistas confirmatórias consistiu na verificação da presença ou ausência de determinadas características no conteúdo da entrevista.

4.2.1. Identificação dos Entrevistados, Local e Data da Recolha de Dados

A seleção dos entrevistados (E) foi efetuada com base em dois critérios. Por um lado, dois Chefes das SIIC, que exercem autoridade técnica e funcional sobre todos os órgãos IC da estrutura do CTer. Por outro lado, dois procuradores adjuntos, que enquanto Autoridade Judiciária (AJ) que ordenam as diligências efetuadas pelos NIC na investigação dos processos-crime. As pessoas entrevistadas estão identificadas no Quadro n.º 5.

Quadro n.º 1: Identificação dos Entrevistados e Descrição dos Locais e Data da Recolha de Dados.

Código	Posto	Função	Local	Data	Hora	Modo
E1	Tenente-Coronel	Chefe da SIIC Bragança	CTer Bragança	29/03/2018	14:30	Presencial
E2	Tenente-Coronel	Chefe da SIIC Setúbal	CTer Setubal	02/04/2017	14:30	Presencial
E3	Procurador-Adjunto	Grupo técnico do gabinete do Cibercrime	Procuradoria-Geral da República	12/04/2017	10:00	Presencial
E4	Procurador-Adjunto	Procurador-Adjunto	Tribunal Judicial da Comarca de Vila Flor	15/04/2017	14:00	Presencial

4.2.2 Análise e discussão do conteúdo das Entrevistas

Relativamente à questão n.º1 – "**Da sua experiencia profissional, no âmbito de processos-crime, considera que a PSE tem contribuído para a eficácia da investigação criminal?**" – a mesma visou estabelecer uma ponte de situação geral, através do contato dos entrevistados com o terreno, do papel que a PSE tem na investigação criminal.

Quadro n.º 2: Respostas e argumentos Questão n.º1.

N.º	Resposta	Argumentação
E1	"(...)tem de facto contribuído para a eficácia e eficiência das inúmeras investigações onde surge".	- "(...) assistimos à utilização massiva de dispositivos eletrónicos"; -"(...) o potencial de informação que estes equipamentos permitem obter e transmitir é ilimitado (...) permitindo não só a partilha de voz e texto, como também fotografias e vídeos".
E2	"Tem contribuído e muito".	-"os indivíduos reincidentes no crime (...) começam a sofisticar o modo como comunicam entre si. E começaram, por exemplo, a utilizar outras plataformas de conversação diferentes dos SMS como o WhatsApp".
E3	"A prova eletrónica não é a prova do presente nem a prova do futuro, é a prova do passado".	-"A lei do Cibercrime aplica-se a tudo quanto sejam processos onde haja necessidade de recolher prova em formato digital"; -"(...) as forças de segurança em Portugal e o sistema formal de justiça demoraram tempo demais a acordar para uma realidade que já estava connosco"; -"(...) o grande problema é que há muita incompreensão e infelizmente ainda há um longo caminho a percorrer na formação quer das forças de segurança quer do sistema formal de justiça português (...)".
E4	"A prova digital está presente em todo o lado"	-"(...) a Criminalidade em geral socorre-se dos suportes eletrónicos que permitem armazenar dados informáticos que são relevantes para a investigação(...)

Fonte: Elaboração própria

De forma geral, todos os entrevistados consideraram que a presença deste tipo de prova, na investigação de processos-crime é cada vez mais acentuada tendo o E1 afirmado que a PSE "tem de facto contribuído para a eficácia e eficiência das inúmeras investigações onde surge". Os argumentos utilizados pelo E1, E2 e E4 foram, praticamente, os mesmos e remeteram, sobretudo, para a "utilização massiva de dispositivos eletrónicos" que permitem "não só a partilha de voz e texto, como também fotografias e vídeos". O E2 acrescenta que a importância da PSE se fica a dever à sofisticação dos indivíduos reincidentes na prática de crimes, tendo estes começado a utilizar, por exemplo, "outras plataformas de conversação diferentes dos SMS como o WhatsApp".

Apesar de todos os entrevistados concordarem com o contributo positivo da PSE, o E3 afirma que "as forças de segurança em Portugal e o sistema formal de justiça demoraram tempo demais a acordar para uma realidade que já estava connosco",

apresentando como soluções para esse atraso "um longo caminho a percorrer na formação".

Conforme havíamos constatado no enquadramento teórico, existe uma utilização transversal a toda a sociedade de diferentes tipos de tecnologias. Este facto leva à possibilidade de se cometerem crimes onde os equipamentos servem de repositório de provas que contribuem para a eficácia da investigação criminal (Casey, 2011). Contudo, para que isso se verifique devem ser respeitados os princípios (Rodrigues B. S., 2011) e as características da PSE (ENISA, 2014).

No que toca à pergunta n.º2 – "**Durante o desempenho das suas funções já teve diligências de processos confiados a militares dos NIC em que tenha sido necessário o manuseamento de PSE? –** todos os entrevistados responderam de forma afirmativa. Isto deixou clara a posição de proximidade entre os entrevistados e os militares dos NIC e, por outro lado, reforçou a ideia de que a PSE está presente na investigação dos crimes delegados à GNR.

Desta forma, destacamos a resposta do E1 que afirma que "dificilmente existirão processos em que a PSE não esteja presente", pois segundo o E2 todos os NIC do CTer a que pertence "já tiveram inquéritos onde foi necessário apreender material informático, telemóveis e computadores, que posteriormente foram enviados para perícia". O E4 deu como exemplos de tipologias de crimes onde considera haver uma maior relevância deste tipo de prova "a investigação do tráfico de estupefacientes (...) e os furtos".

O E3 acrescenta, contudo, que "nas situações de abordagem ao cenário do crime existe ainda uma incompreensão muito grande sobre como abordar os equipamentos", pelo que, segundo este entrevistado, é de relevar o apoio técnico dado, por exemplo, pelo NTP de Coimbra, ao NIC daquela área. Esta questão foi aprofundada por este, e outros entrevistados, na resposta a outras questões, como iremos demonstrar.

Quadro n.º 3: Respostas e argumentos Questão n.º2.

N.º	Resposta	Argumentação
E1	"(...)dificilmente existirão processos em que a PSE não esteja presente".	- Os órgãos da estrutura de IC da Guarda lidam no seu quotidiano com este tipo de prova".
E2	"Sim".	-" Qualquer um dos meus NIC já tiveram inquéritos onde foi necessário apreender material informático, telemóveis e computadores, que posteriormente foram enviados para perícia ".
E3	" Claro que sim".	-"(...) pelo menos em Coimbra existe um departamento específico para exames forenses de PSE onde há uma atividade bastante notável desenvolvida no seio da GNR (...) todos os NIC naquela área beneficiam deste departamento, de forma direta. ". -"(...) nas situações de abordagem ao cenário do crime existe ainda uma incompreensão muito grande sobre como abordar os equipamentos".
E4	"Sim claro".	-"Principalmente na investigação do tráfico que é a criminalidade que nós trabalhamos mais com os NIC. -"Outro exemplo são os furtos mais qualificados onde muitas vezes é necessário proceder à análise de equipamentos informáticos".

Fonte: Elaboração própria

A questão n.º3 – **"Considera que os militares das GNR, nomeadamente dos NIC, têm um conhecimento adequado relativo às disposições processuais no âmbito da PSE?" –** visava incidir, objetivamente, nos Arts. 12º,15º e 16º, do capítulo III da Lei do Cibercrime, que estabelecem as disposições processuais para a preservação, pesquisa e apreensão de dados informáticos, respetivamente. Na resposta a esta questão não verificamos existir uma coerência, como nas perguntas anteriores.

Quadro n.º 4: Respostas e argumentos Questão n.º3.

N.º	Resposta	Argumentação
E1	"(...) a estrutura de IC integra profissionais que deverão possuir os necessários conhecimentos das disposições legais e processuais que regulam esta matéria ".	- "(...) a PSE (...) já não se constitui como novidade"; - "(...) independentemente de estes terem ou não tido formação nessa área, providenciada pela Instituição é sua responsabilidade estarem permanentemente atualizados face às alterações legislativas e novos procedimentos".
E2	"Eles têm obrigatoriamente conhecimento".	-" (...) pelos pedidos de diligências que fazem ao MP onde são invocados esses conhecimentos"; -"Contudo essa matéria poderia ser mais explorada ao nível da formação".
E3	" Os militares do NIC vão tendo e vão procurando saber".	-"(...) existem necessidades ao nível da formação, para poderem não só saber como abordar o cenário de crime, mas também para a recolha de PSE simples(...)"; -"(...) existe a consciência, pelo menos, do problema que necessita de uma resposta".
E4	"Confesso que poderiam ter um conhecimento melhor".	-"um melhor conhecimento proveniente de formação seria necessário visto que esta área é muito específica e técnica contudo também existem procedimentos válidos que eles vão adquirindo com a experiência"; -"O Ministério Público vai dando algumas indicações sobre como se deve proceder, em alguns casos".

Fonte: Elaboração própria

Por um lado, o E1 revela que "(...) a estrutura de IC integra profissionais que deverão possuir os necessários conhecimentos das disposições legais e processuais que regulam esta matéria". O argumento base desta afirmação está relacionado com a responsabilidade pessoal de cada militar em estar "permanentemente atualizado face às alterações legislativas e a novos procedimentos independentemente de estes terem ou não tido formação nessa área, providenciada pela instituição – GNR".

Por outro lado, as respostas do E2, E3 e E4 vão de encontro com a existência de um conhecimento superficial, onde "os militares dos NIC vão tendo conhecimento e vão procurando saber". Para além disto, os três entrevistados apontam para "(...) necessidades ao nível da formação, para poderem não só saber como abordar o cenário de crime, mas também para a recolha de PSE simples (...)". Sobre este assunto, acrescentou o E4 que o "MP vai dando algumas indicações sobre como se deve proceder, em alguns casos".

A questão n.º 4 – "**Da sua experiência, que capacidades técnicas deveriam ser melhoradas nos NIC para identificar, adquirir, preservar e analisar PSE para os processos crime?"** – visava recolher dados dos entrevistados sobre a necessidade de existirem melhorias no manuseamento da PSE, por parte dos NIC. Assim como na questão anterior, as respostas dividiram-se em três categorias.

Quadro n.º 5: Respostas e argumentos Questão n.º4.

z		
E1	"O trabalho desenvolvido pelos NIC tem correspondido àquelas que são as suas obrigações no que tange ao manuseamento da PSE".	- "(...) a competência para o manuseamento da PSE deveria estar no patamar de atuação do NAT que (...)tem a responsabilidade de proceder à recolha de vestígios na cena do crime (biológicos, lofoscópicos, fisico-químicos). Se assim é então este órgão deveria estar igualmente capacitado e dotado do necessário equipamento tendente á recolha de PSE";
E2	"Existe falta de formação (...)".	-" (...)os militares têm conhecimento da importância de apreender computadores e telemóveis mas por exemplo não fazem o mesmo com os routers. Estas carências poderiam ser ultrapassadas através de ações de formação(...)"; -"As melhorias deveriam ser no âmbito da identificação, transporte e preservação"; -"A colocação de um perito digital forense em cada CTer atenuaria estas carências técnicas".
E3	"todos os NIC deveriam ter pelo menos duas pessoas com formação de *first responder* certificada".	-"(...) formação técnica implica (...) a parte legal que é essencial, (...)conhecimento técnico para o manuseamento de ferramentas necessárias e (...)investimento em equipamentos que permita fazer essa recolha. -"(...) a questão do software *digital forensics* tem, logicamente, custos acrescidos".
E4	"(...) o que nos é proposto é feito, de forma correta mas não, necessariamente, suficiente."	-"(...) maior capacidade técnica poderia trazer mais coisas ao processo e com maior qualidade -"(...) se alguns aparelhos importantes não são identificados e não chegam ao conhecimento do MP não podem, naturalmente, ser utilizados"

Fonte: Elaboração própria

Em primeiro lugar, o E1 considera que "o trabalho desenvolvido pelos NIC tem correspondido àquelas que são as suas obrigações no que tange ao manuseamento da PSE". De seguida este entrevistado menciona considerar que "o manuseamento da PSE não deve ser feito pela vertente operativa, ou seja os NIC". O mesmo afirma que "a competência para o manuseamento da PSE deveria estar no patamar de atuação dos NAT que têm a responsabilidade de proceder à recolha de vestígios na cena do crime (biológicos, lofoscópicos e físico-químicos), (...) se assim é então este órgão deveria estar, igualmente, capacitado e dotado do necessário equipamento tendente a recolha de PSE".

Por sua vez, o entrevistado E2, considera que, no panorama geral, "existe falta de formação" e apresenta como solução "a colocação de um perito digital forense em cada CTer" o que atenuaria estas carências técnicas. As declarações apresentadas pelo E3 vão, também neste sentido afirmando que, "todos os NIC deveriam ter, pelo menos, duas pessoas com formação de *first responder* certificada". Ainda segundo o E3, existem dificuldades em implementar este conhecimento técnico seja aquele relativo às disposições legais ou ao manuseamento de ferramentas necessárias. Este entrevistado acrescenta ainda

que o investimento em equipamentos que permitam fazer essa recolha têm, logicamente, custos acrescidos.

Por último, o E4 destaca necessidades ao nível da identificação de equipamentos importantes para a aquisição, preservação e análise de PSE, pois afirma que "se alguns aparelhos importantes não são identificados e não chegam ao conhecimento do MP não podem, naturalmente, ser utilizados".

Relativamente a este assunto recordamos o argumento de Ramos (2017) que considera fulcral a rapidez na obtenção deste tipo de prova, assim como uma correta recolha - elementos essenciais para o êxito da investigação. Em concordância Renato Lopes Militão (Militão, s.d.) considera que "as ações de investigação criminal relativas à prova digital exigem aprofundados conhecimentos informáticos e, muitas vezes, meios técnicos e tecnológicos de ponta".

Relativamente à questão 5: **Considera que os NIC têm conhecimentos adequados para efetuar pedidos de diligências para recolha de PSE no âmbito de processos crime, como por exemplo, a preservação de dados em plataformas (Facebook, Instagram), pedido de detalhe de clientes aos ISP ou para cumprir mandados de pesquisa de dados informáticos?"** – as respostas foram, uma vez mais consensuais, na medida em que 3 dos 4 entrevistados (E2, E3 e E4) enumeraram limitações, neste caso, ao tipo de pedidos de diligências que a pergunta enunciada elencou.

Quadro n.º 6: Respostas e argumentos Questão n.º5.

N.º	Resposta	Argumentação
E1	"O NIC possui conhecimento por forma a efetuar os pedidos de diligência".	- "(...) os quais devem ser coordenados pelo tutelar de ação penal, o MP".
E2	"Os NIC não estão consciencializados para esse tipo de pedidos".	-" (...)pode ser feito ao nível da análise de investigação criminal(...)"; -"(...) quem faz os pedidos é o MP".
E3	"Depende".	-"Se houvesse formação de first responder em todos os NIC, acreditaria que sim. -" Sem essa formação é extraordinariamente difícil num NIC saber exatamente o que fazer. (...) os investigadores mesmo atuando bem intencionadamente, contudo sem conhecimentos técnicos, podem estar a dar um tiro ao lado porque não é exatamente aquilo que naquela circunstância se deveria solicitar.".
E4	"(...)o pedido é feito diretamente ao MP que posteriormente se dirige às plataformas mencionadas e aos ISP".	-"É mais fácil pedirem ao MP sabendo que nós temos alguns protocolos que depois aceleram estes processos"; - Quanto aos mandados para cumprir pesquisas de dados informáticos vocês têm (...) um NTP (de Coimbra(que executam um trabalho muito importante de apoio aos NIC (...) deveriam existir mais laboratórios com estas capacidades". -"(...) também seria importante os NIC terem militares com formação certificada nesta área mas isto acarreta custos a vários níveis.

Fonte: Elaboração própria

O E1 afirmou que "os NIC possuem conhecimento por forma a efetuar os pedidos de diligências". Ainda assim todos os entrevistados foram unânimes em considerar o MP como peça fundamental no que toca aos pedidos de preservação de dados a plataformas como as redes sociais ou aos ISP. O E3 afirmou que "sem formação é extraordinariamente difícil num NIC saber exatamente o que fazer". Na mesma linha o E4 afirma que "é mais fácil, os OPC, pedirem ao MP sabendo que nós temos alguns protocolos que depois aceleram estes processos e que, posteriormente, quem efetiva as perícias é esta Autoridade Judiciária".

Relativamente ao cumprimento de mandados de pesquisa de dados informáticos o E4 acrescenta que tem conhecimento de um NTP (de Coimbra) onde os profissionais executam um trabalho muito importante de apoio aos NIC e, para além disso, deveriam ainda existir mais laboratórios com estas capacidades. Por último, salienta que "seria também importante os NIC terem militares com formação certificada" nesta área, contudo, este entrevistado afirma que "isto a carreta custos a vários níveis". Recordamos que este último argumento havia sido já utilizado por outros entrevistados nas respostas às questões anteriores.

Na pergunta número 6: **"Considera que os NIC são capazes de adquirir e analisar corretamente PSE, em equipamentos de testemunhas e vítimas, de forma manual e lógica, em sede de processos crime?"** – o único entrevistado a responder de forma totalmente afirmativa foi o E2 referindo que "os NIC fazem esse tipo de diligências".

À semelhança da resposta à questão n.º 4, o E1 afirmou que a recolha e análise da PSE "devem ser garantidos por uma estrutura especializada nesta área" atribuindo estas competências da recolha para os NAT e todos os tipos de análise para "as estruturas laboratoriais dos NTP dotadas de equipamentos para a realização deste tipo de intervenções". Como forma de evitar uma sobrecarga destas estruturas o E1 sugere a "ampliação dos atuais laboratórios da Guarda para os demais comandos territoriais, com o intuito de apoiar os investigadores no que tange a realização dos necessários exames".

Por sua vez, os entrevistados E3 e E4 testemunharam que os NIC têm "apenas capacidade de recolha manual" e que "muitas das vezes cingem-se aos *printscreen"*. Sobre esta situação, refere o E3 que a realização de um *printscreen* pode ser muito útil, mas essa prova não é suficiente". "Numa primeira abordagem a extração manual pode ser feita. Contudo, devem em qualquer uma dessas circunstâncias assegurar-se que é integralidade de todos os dados que podem ser relevantes para a investigação sejam primeiro preservados e depois verdadeiramente recolhidos de forma correta". Como causas para esta limitação o E3 apresenta "necessidades na formação no seio dos NIC" e, o E4 a "falta de aparelhos para extrair os dados de outras formas, neste caso, ao nível lógico".

De acordo com a literatura apresentada, "os investigadores podem deparar-se com situações onde se enquadrem um a mais níveis de análise e devem, portanto, ter o nível de formação para realizar esses exames" (Scientific Working Group on Digital Evidence, 2013), ou ter conhecimento de quem deve ser contactado para prestar o apoio necessário. As respostas dos entrevistados cingiram a capacidade de análise dos NIC ao método manual. Este processo envolve a operação manual do teclado e do visor do aparelho para documentar dados (Scientific Working Group on Digital Evidence, 2013). A falta de suporte necessário e de formação adequada leva a que, segundo os entrevistados, não seja possível proceder às extrações de dados de nível lógico.

Quadro n.º 7: Respostas e argumentos Questão n.º6.

N.º	Resposta	Argumentação
E1	"A recolha e análise (...) devem ser garantidos por uma estrutura especializada nesta área".	- "O patamar da recolha deverá ser garantido pela intervenção do NAT"; -"A realização do exame da PSE deverá ser garantida (...) pelas estruturas laboratoriais dos NTP dotados de equipamentos para a realização deste tipo de intervenções"; -"Considero importante a ampliação dos atuais laboratórios da Guarda para os demais CTer, com o intuito de apoiarem os investigadores no que tange à realização dos necessários exames(...)".
E2	"Os NIC fazem esse tipo de diligências".	
E3	"Apenas capacidade de recolha manual".	-"A realização de um *printscreen* pode ser muito útil (...) mas, essa prova, não é suficiente; -"(...)numa primeira abordagem, a extração manual pode ser feita, contudo, devem em qualquer uma dessas circunstâncias assegurar-se que a integralidade de todos os dados que podem ser relevantes para a investigação sejam primeiro preservados e depois verdadeiramente recolhidos de forma correta". -" A forma de ultrapassar este problema reside na formação para recolher essa prova de forma lógica, no seio dos NIC".
E4	"Essencialmente cingem-se aos *printscreen"*	-"(...) porque não têm aparelhos para extrair os dados de outras formas, neste caso, no nível lógico"; -"(...) os NIC só fazem a extração ao nível físico, o que acaba por se remeter quase sempre ao nível da prova documental".

Fonte: Elaboração própria

4.3. Análise e Discussão dos Inquéritos por Questionário

Relativamente aos Núcleos de Investigação Criminal, que constituem o nosso universo, são constituídos por 554 militares, por sua vez, a amostra é composta por um total de 144 militares.

O rigor do processo de amostragem, depende da medição da sua fiabilidade, dado que, o ato de generalizar um determinado universo, através de uma amostra mais reduzida, releva sempre um valor de erro inerente. Este estudo obteve um nível de confiança, que é, segundo Sarmento (2013, p. 90), "a probabilidade do intervalo de confiança conter o verdadeiro valor do parâmetro", de 95,46%, cuja normal estandardizada é de 1,96 e a margem de erro associada foi de 6%, atribuindo assim, o grau "*Importante"* à validade do estudo.

O presente questionário foi dividido em 5 partes. A primeira aborda a caracterização sociodemográfica dos inquiridos. A segunda parte, visa aferir o conhecimento dos militares dos NIC quanto às disposições processuais que legitimam o manuseamento da PSE. A terceira parte comporta um conjunto de questões relacionadas,

diretamente, com conhecimentos técnicos, adquiridos em formação ou trabalho em equipa, para identificar, adquirir e preservar PSE. Na quarta parte são apresentadas algumas questões relacionadas com a atuação enquanto *first responder*, pelo que essas questões correspondem, maioritariamente, à importância e às consequências de serem adotados alguns procedimentos errados, de acordo com aquelas que são as boas práticas mencionadas no enquadramento teórico. Por último, na quinta parte, foi abordada uma questão que consideramos particular e importante, tendo em conta que faz parte do âmbito de atuação dos NIC. Neste caso referimo-nos às situações em que os equipamentos pertencem às vítimas ou testemunhas e, consequentemente, a PSE se encontra na posse daqueles. Estas situações requerem um conjunto de procedimentos diferentes dos mencionados na quarta parte. À exceção da primeira parte do questionário, as divisões do mesmo vão de encontro com as PD condutoras desta investigação pelo que a parte dois, três, quatro e cinco correspondem diretamente as PD.1, 2, 3 e 4.

4.3.1. Parte 1: Caraterização da Amostra

O presente inquérito por questionário foi endereçado a todos os militares dos NIC (553 militares) que têm a seu cargo a investigação de processos-crime, registando-se uma taxa de resposta de 26% (144 respostas válidas).

Quanto à constituição da amostra, 117 (81,3%) são Guardas, sendo os restantes 27 (18,8%) Sargentos[31]. No que toca ao nível etário, a maior parte dos inquiridos situa-se no escalão dos 31-40 anos (45,8%) e, em segundo lugar entre os 41-50 anos (38,9%)[32]. No que se refere às habilitações literárias, é de salientar que a grande maioria 88 (61,1%) dos inquiridos tem o 12º ano de escolaridade[33]. No que diz respeito ao género, 139 (96,5%) dos inquiridos são homens e 5 (3,5%) são mulheres. Por último, quanto ao tempo de permanência na estrutura de Investigação Criminal da Guarda destaca-se a preponderância dos que têm entre 5 e 10 anos de experiência (41%) e os que têm entre 11 e 15 anos (29,2%). [34]

[31] Cfr. Apêndice D.1, Figura n.º 17
[32] Cfr. Apêndice D.1, Figura n.º 18
[33] Cfr. Apêndice D.1, Figura n.º 19
[34] Cfr. Apêndice D.1, Figura n.º 20

4.3.2. Parte 2 : Conhecimento das disposições processuais no âmbito da PSE

A PQ. 1 visava saber se, de forma geral os NIC conhecem as disposições processuais constantes no capítulo III da Lei 109/2009. As respostas não foram, de todo, unânimes tendo 31 % dos inquiridos respondido de forma negativa (21% discordam e 10% discordam totalmente), 36% de forma positiva (27% concordam e 33% concordam totalmente) e os restantes 33% responderam de forma neutra (não concordam nem discordam), o que pode indicar que estes não se encontram familiarizados com esta questão. Se na pergunta mais geral, sobre o conhecimento das disposições processuais não verificamos unanimidade, o mesmo continuou a suceder quando iniciamos uma abordagem específica desta legislação que, em concreto, afeta a vertente operativa da IC da GNR.

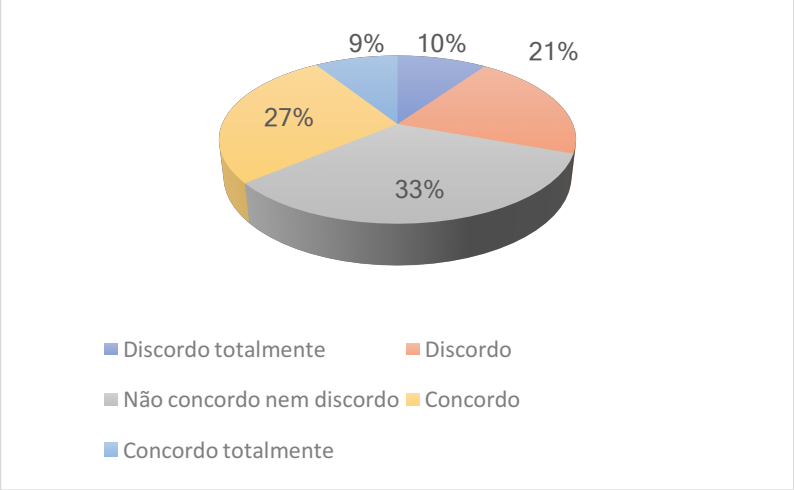


Figura n.º 1: Conhecimento das disposições processuais (PQ.1).

Fonte: Elaboração Própria

Os inquiridos, quando questionados, na PQ 2, sobre a possibilidade de ser feita a preservação, pesquisa e apreensão de PSE para qualquer tipo de crime não demonstraram um grande conhecimento, tendo sido recolhidos 27% de respostas "Concordo" e 9% "Concordo totalmente" e, por outro lado, 10% de respostas "Discordo" e 10% discordam totalmente. A maioria dos inquiridos 33% responde de forma neutra, ou seja, não sente ter conhecimento suficiente para responder sobre estas questões.

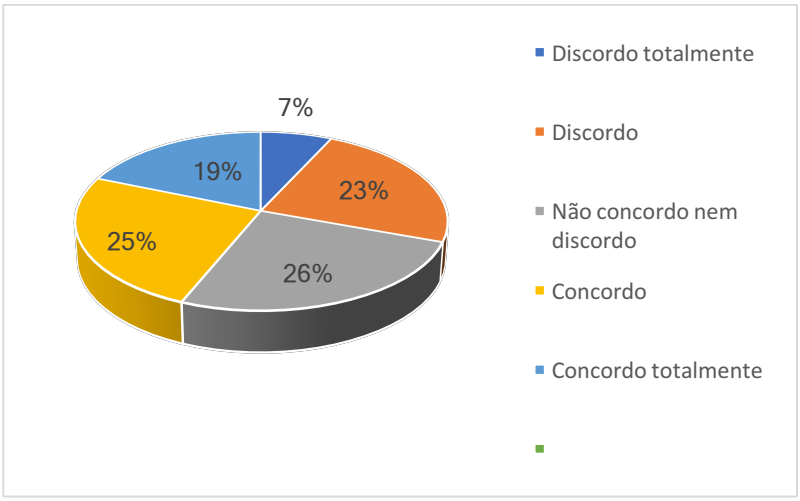


Figura n.º 2: Conhecimento de preservação, pesquisa e apreensão de PSE para qualquer tipo de crime (PQ.2).

Fonte: Elaboração Própria

Relativamente à preservação e pesquisa de dados informáticos, sobre os quais incidem as PQ 3 a 7, existe uma divisão, quase igual, entre aqueles que admitem não conhecer as disposições ou preferem manter uma resposta neutra e aqueles que efetivamente dizem conhecer os termos que constam na Lei 109/2009. Os dados em concreto que recolhemos mostram que a percentagem de respostas "Discordo e Discordo totalmente" variam entre 24% e 36% e as respostas "Não concordo nem discordo" correspondem ao intervalo de 20-28%. Por outro lado as respostas entre "Concordo e Concordo totalmente", ou seja, que demonstram um conhecimento sobre as temáticas em apreço variam entre 39% e 56%[35].

Relativamente à PQ.8 e as suas respetivas alíneas – "Tenho conhecimento de que relativamente à apreensão de dados informáticos, a mesma pode incidir sobre: a) apreensão do suporte físico; ou b) cópia dos dados em suporte autónomo" – e PQ.9 – que incidem sobre a validação das apreensões no prazo de 72 pela AJ competente – demonstraram que a grande maioria das respostas se situa no conhecimento das disposições presentes naquele diploma legal ("Concordo e Concordo Totalmente). Neste caso as respostas que demonstram esse conhecimento variaram entre os 55,6% e os 70,8% dos quais destacamos uma grande taxa de respostas "Concordo totalmente", ou seja, que demonstram um conhecimento total[36].

[35] Cfr. Apêndice D.2, Figuras n.º 22,23,24,25,26,27 e 28.
[36] Cfr. Apêndice D.2, Figuras n.º 29, 30 e 31..

A PQ.10.a) e 10.b) incidia sobre a consciência de serem submetidos à validação do Juiz de Instrução Criminal, dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos ou mensagens de correio eletrónico ou registos de comunicações de natureza semelhante não lidos. Em ambas as perguntas, a maioria dos inquiridos demonstrou ser conhecedor deste pressuposto especial relativo à validação dos conteúdos (55%). Por outro lado, a média das percentagens de respostas que indicam o desconhecimento é de 18,5%.

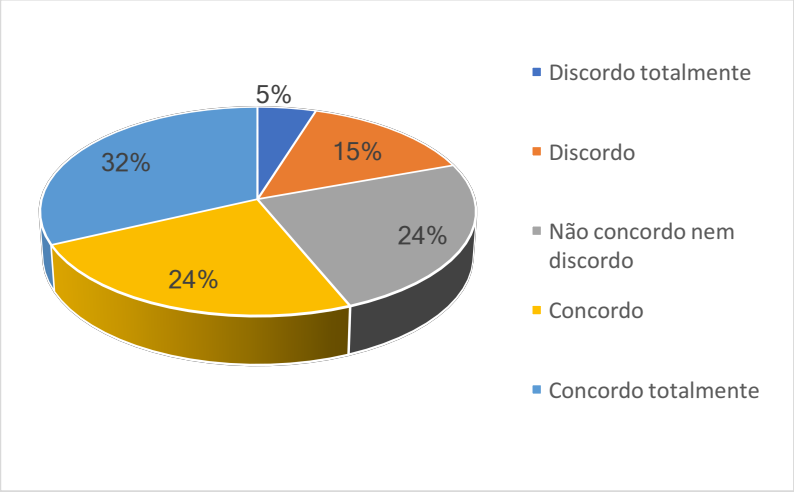


Figura n.º 3: Consciência da validação do JIC de dados íntimos (PQ.10.a).

Fonte: Elaboração Própria

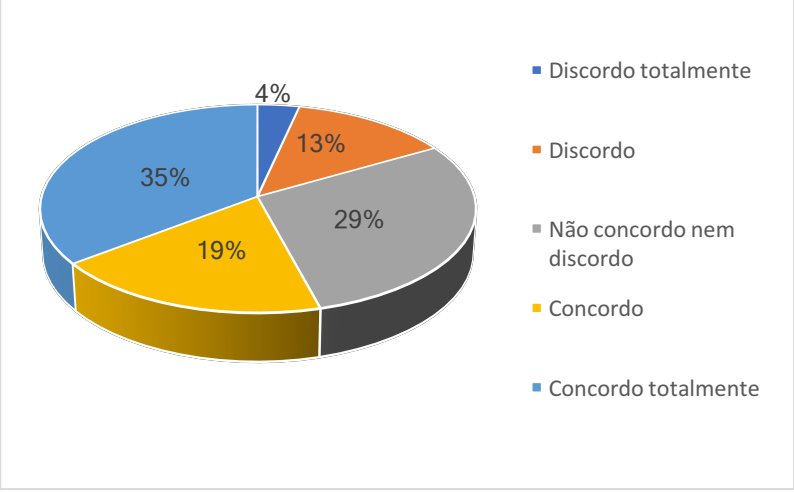


Figura n.º 4: Consciência da validação do JIC de mensagens não lidas (PQ.10.b).

Fonte: Elaboração Própria

4.3.3. Parte 3: Conhecimentos técnicos adquiridos em formação ou trabalho em equipa para identificar, adquirir e preservar PSE

Relativamente à PQ.11 – "Considero que conheço o conceito de PSE: "qualquer dado guardado ou transmitido através da utilização de um dispositivo eletrónico que suporte ou refute a teoria de como um crime ocorreu ou todas as circunstâncias que possam provar uma intenção ou um álibi" – destacamos uma grande taxa de respostas "Não concordo nem discordo" (24%) e "Discordo e Discordo totalmente" (25%). Daqui podem decorrer várias interpretações como o desconhecimento do conceito tal como na PQ se encontrava redigido. Mas, por outro lado, os militares podem ter conhecimento de outro conceito ou através da sua aplicação prática, no decorrer das suas competências. Isto porque 51% dos inquiridos afirma conhecer o conceito de PSE.

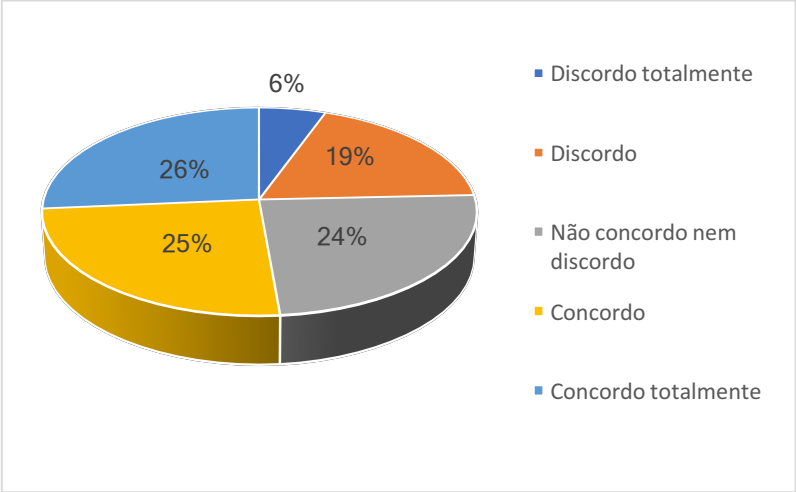


Figura n.º 5: Conhecimento do conceito de PSE(PQ.11).

Fonte: Elaboração Própria

Relativamente à PQ.12 – "Considero que a PSE é um importante meio de obtenção de prova para a investigação criminal" – a mesma versava sobre a importância da prova em suporte eletrónico como meio de obtenção de prova para a investigação criminal. As respostas revelaram que 65% dos inquiridos responderam positivamente (Concordo e Concordo totalmente") e apenas 16% de forma negativa ("Discordo e Discordo totalmente"). Ainda nesta pergunta destacamos que apenas um dos inquiridos discordou totalmente e 41% concordou totalmente com a afirmação.

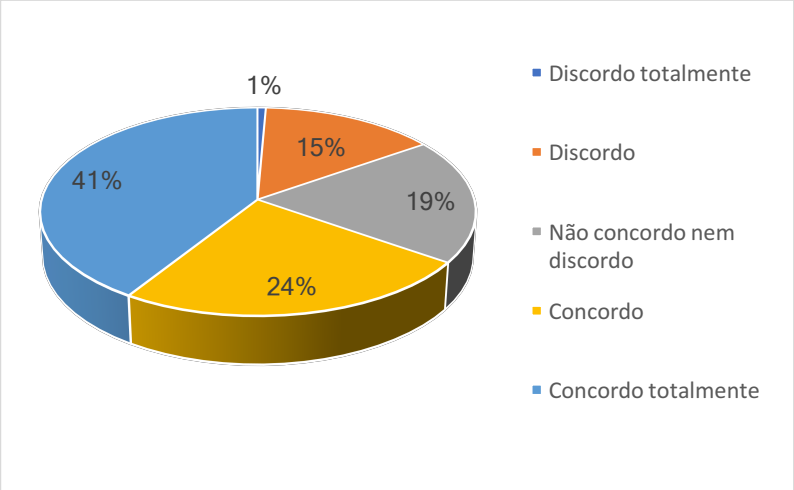


Figura n.º 6: Importância da PSE para a investigação criminal (PQ.12).

Fonte: Elaboração Própria

Quando questionados, na PQ.13, sobre a formação técnica necessária para identificar a forma mais adequada para aceder aos conteúdos de equipamentos 57% dos inquiridos respondeu que discorda ter essa formação e, por outro lado, apenas 10% afirmam ter as mesmas competências adquiridas em formação.

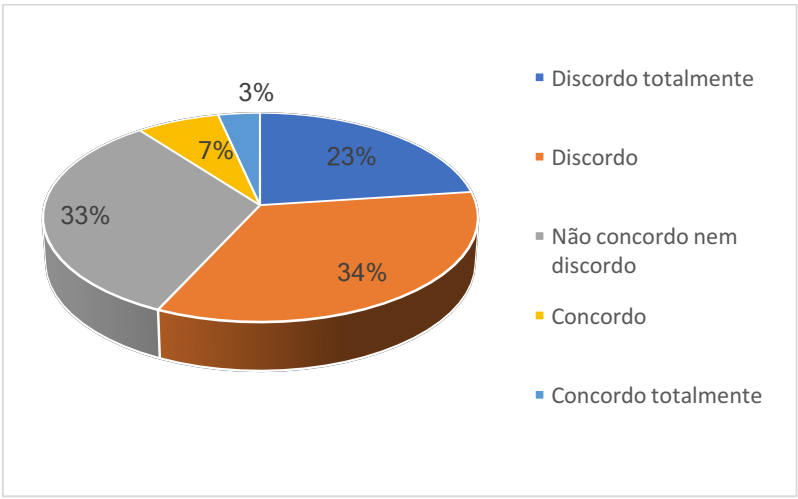


Figura n.º 7: Formação técnica necessária para identificar a forma mais adequada para aceder aos conteúdos de equipamentos (PQ.13).

Fonte: Elaboração Própria

Na PQ.14 suscita-se o conhecimento, por parte dos NIC, dos órgãos especializados tecnicamente para identificar, adquirir e preservar PSE, dentro da GNR. Posto isto, 51% dos inquiridos demonstrou ter capacidade para contactar o apoio técnico especializado

("Concordo e Concordo totalmente") e 25% respondeu no sentido oposto ("Discordo e Discordo totalmente"). Destacamos ainda a disparidade entre aqueles que afirmaram conhecer totalmente (26%) e aqueles que desconhecem totalmente esta capacidade (6%) da GNR e que serve como apoio técnico na realização de exames aos equipamentos eletrónicos.

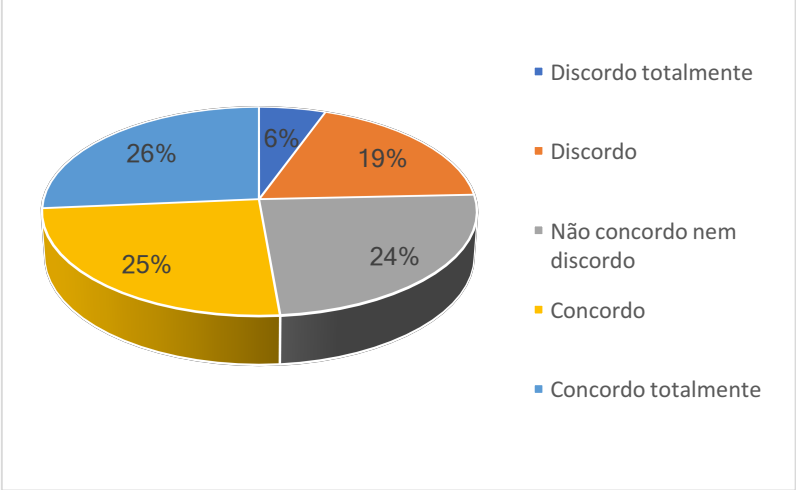


Figura n.º 8: Conhecimento dos órgãos técnicos especializados (PQ.14).

Fonte: Elaboração Própria

Na PQ.15, sobre se a formação técnica e o treino adquirida pelos militares foi feita em autoformação ou pelo trabalho em equipa verificamos que 40,9% respondeu afirmativamente ("Concordo ou Concordo totalmente"). A percentagem de militares que respondeu, precisamente, o contrário, é de 26%. As respostas neutras ("Não concordo nem discordo") obtiveram o maior número de respostas tendo sido registados 33%.

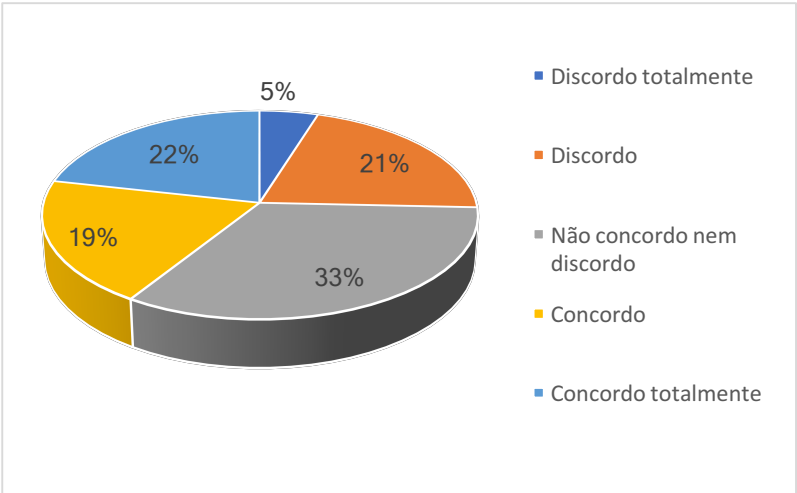


Figura n.º 9: Conhecimentos adquiridos em autoformação ou trabalho em equipa (PQ.15).

Fonte: Elaboração Própria

Na PQ.16 que versava sobre a preocupação em obter conhecimentos sobre os procedimentos e o suporte técnico necessários para o manuseamento da PSE, por parte dos próprios militares, verificamos um número muito baixo de respostas negativas ("Discordo e Discordo totalmente"), tendo sido registados apenas 26% dos inquiridos que não têm essa preocupação. Por outro lado, foram registados 41% de situações em que os militares respondem positivamente ("Concordo e Concordo totalmente"), ou seja, revelando uma preocupação contínua em se manterem atualizados. Ainda assim uma grande percentagem dos inquiridos (33%) respondeu que não concorda nem discorda, ou seja, de forma neutra.

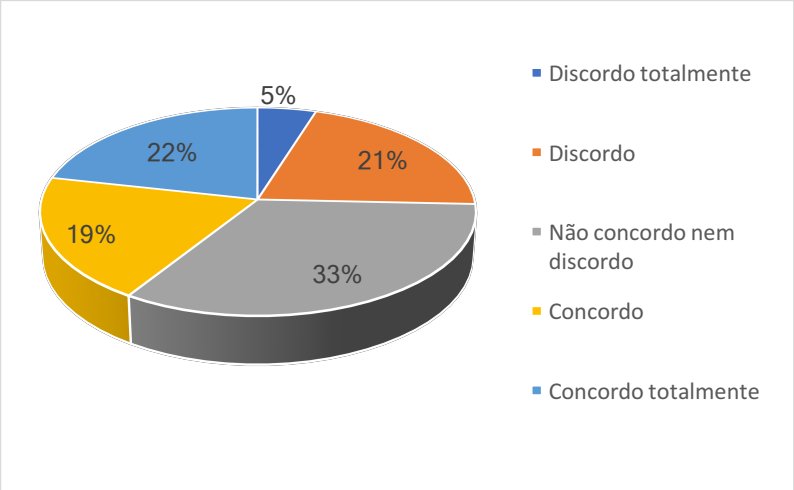


Figura n.º 10: Preocupação em obter conhecimentos sobre os procedimentos e o suporte técnico necessários para o manuseamento da PSE (PQ.16).

Fonte: Elaboração Própria

A PQ.17 não obedecia a uma escala de 1 a 5, como todas as outras. Para responder esta questão os inquiridos deveriam selecionar quais os equipamentos que mais dúvidas lhes suscitam para a pesquisa, preservação e apreensão de PSE e que, consequentemente, implicam uma maior necessidade de formação e treino técnico.

Das respostas destacaram-se os computadores padrão, com possibilidade de conexões de rede (93,8%); todas as informações que podem constar nos veículos como os eventos do mesmo, dados de localização e dados de rede (90,3%); suportes para armazenamento digital usados em computadores como discos rígidos (90,3%). Os dispositivos menos selecionados foram as *pens drive* USB e cartões de memória (73,6%); câmaras fotográficas digitais e de vídeo e CCTV (79,2%); sistemas de navegação móvel (85,4%).

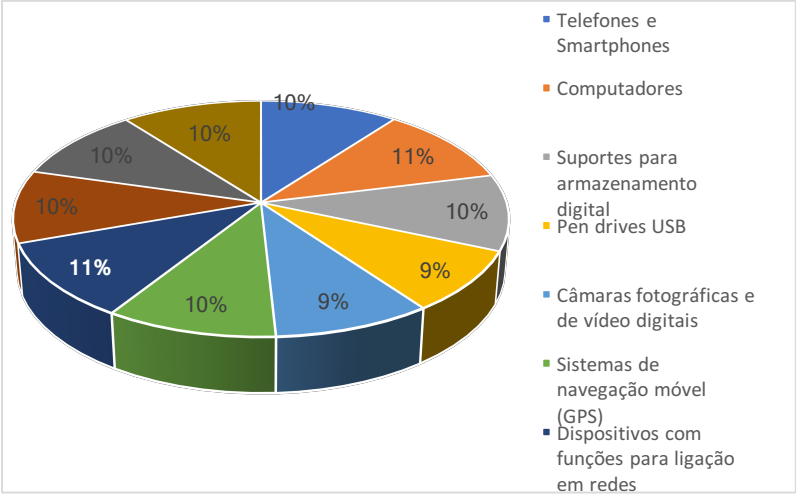


Figura n.º 11: Fontes de PSE que necessitam de maior formação para o seu manuseamento (PQ.17).

Fonte: Elaboração Própria

4.3.4. Parte 4: Capacidades técnicas enquanto *first responders*

As PQ.18 a 25 incidiam sobre o entendimento da importância de serem tomados determinados procedimentos, ou por outro lado, serem evitados determinadas ações que possam trazer consequências, como a perda ou alteração dos dados informáticos originais, numa cena de crime. Apresentamos como exemplo a documentação de códigos pin, a colocação de cartões SIM ou de memória em diferentes telemóveis ou computadores, remoção ou substituição de baterias e a importância dos dados voláteis armazenados num dispositivo ligado. Nas respostas notámos existir uma forte tendência para o conhecimento por parte dos militares. Em média 62% dos inquiridos respondeu afirmativamente ("Concordo e Concordo Totalmente") e apenas 15% de forma negativa ("Discordo e Discordo totalmente")[37].

Contudo, na PQ.24 à semelhança dos dados recolhidos na PQ.14, e que se remetem para o apoio técnico especializado na GNR (os NTP), os inquiridos apresentaram respostas muito distintas. Das 144 respostas, 38% refere que não considera ter um apoio nas diligências que executa por parte de pessoal especializado; por outro lado, 35% indica, precisamente, o contrário. Importa ainda mencionar que 27% dos inquiridos responderam de forma neutra ("Não concordo nem discordo").

[37] Cfr. Apêndice D.3, Figuras n.º 32, 33, 34, 35, 36, 37, 38 e 39..

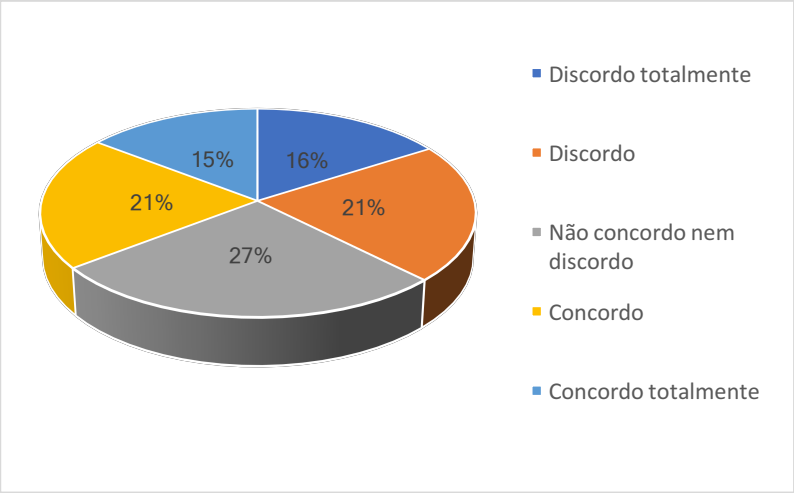


Figura n.º 12: Apoio técnico especializado na execução de diligências processuais (PQ.24).

Fonte: Elaboração Própria

Ao contrário do que podemos verificar no conjunto de questões anteriores, a resposta às PQ 26.a), 26.b), 26.c) e 27 – "Conheço os procedimentos para preservar dados a) se o dispositivo estiver ligado; b) se estiver conectado a uma rede wifi ou outra; c) se estiver desbloqueado; ou d) se estiver desligado e "Tenho conhecimento de que quando se efetua a apreensão de dados a custódia e integridade dos mesmos deve ser garantida pelo cálculo do valor *Hash* e efetuar o seu registo nos autos" – demonstraram um fraco conhecimento por parte dos inquiridos. Estas questões abordavam a familiarização relativamente a procedimentos para preservação de dados em situações distintas, como por exemplo: quando os dispositivos se encontram ligados; se estiverem conectados a uma rede wi-fi ou outra; se estiverem desbloqueados e; no que toca ao cálculo do valor *Hash*. Em concreto, a média das respostas às questões anteriormente mencionadas, demonstraram que 42% dos inquiridos não tem conhecimento sobre os procedimentos a adotar ("Discordo e Discordo totalmente") e, por outro lado, 26% dos inquiridos afirmam que conhecem estes procedimentos ("Concordo e Concordo totalmente")[38].

Em relação à PQ.27 destacamos uma percentagem muito reduzida de conhecimento no que toca à garantia da custódia e integridade dos dados através do cálculo do valor *Hash* (apenas 13% responderam que concordam ou concordam totalmente) e, consequentemente, o seu registo nos autos.

[38] Cfr. Apêndice D.3, Figuras n.º 40, 41 e 42.

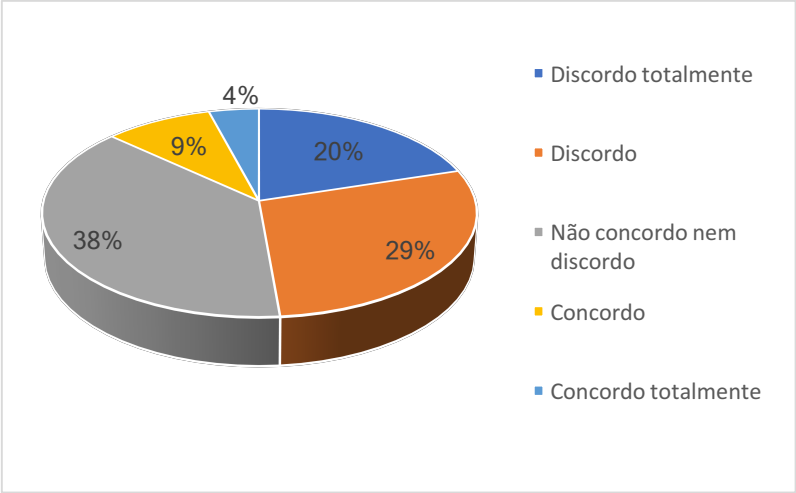


Figura n.º 13: Conhecimento do cálculo do valor *Hash* (PQ.27).

Fonte: Elaboração Própria

4.3.5. Parte 5: Capacidades técnicas para adquirir, em testemunhas e vítitmas, de forma manual e lógica, bem como para analisar PSE

A quinta parte do presente questionário abordava uma situação particular. Neste caso, não nos estávamos a referir a um cenário de crime onde, normalmente, o conteúdo apreendido e analisado pertence aos suspeitos. Pelo contrário, neste conjunto de questões (PQ.28 e PQ.29) incidimos sobre a aquisição, de forma manual e lógica, assim como a análise, de prova em suporte eletrónico no equipamento de testemunhas e vítimas. Quando questionados sobre os conhecimentos técnicos quer de forma manual, quer de forma lógica, as respostas incidiram para uma grande maioria (em média 82%) que não sabe ou responde de forma neutra ("Discordo, Discordo totalmente e Não concordo nem discordo") e apenas 18% admite ter conhecimentos nesta área[39].

A PQ.30 visava aferir se os inquiridos, em caso de necessidade, facultavam um computador da GNR para que a vítima pudesse aceder, por exemplo, à sua conta de correio eletrónico para poder ceder, sob termo de consentimento, os dados relevantes. Os resultados demonstram que 27% responde de forma afirmativa ("Concordo ou Concordo totalmente") e 38% de forma negativa ("Discordo ou Discordo totalmente"), restando 35% dos inquiridos que responderam de forma neutra ("Não concordo nem discordo").

[39] Cfr. Apêndice D.4, Figuras n.º 43 e 44.

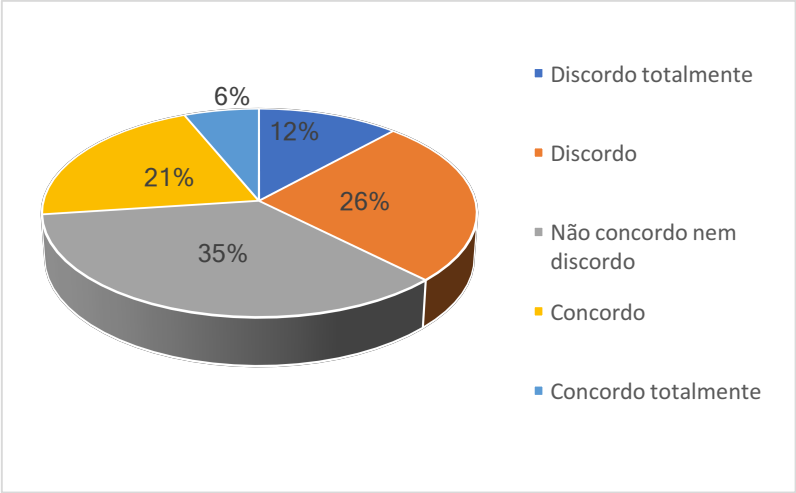


Figura n.º 14: Importância de ceder um computador da GNR para a vítima ou testemunha aceder a dados (PQ.30).

Fonte: Elaboração Própria

A PQ. 31, incide sobre a possibilidade de a vítima ser notificada para que entregue, em 10 dias, a prova em suporte eletrónico armazenada num dispositivo da sua propriedade. Uma vez mais, não existe um consenso nas respostas tendo-se verificado que 39% afirma que faria essa notificação e, por outro lado, 26% dos entrevistados rejeitam essa possibilidade.

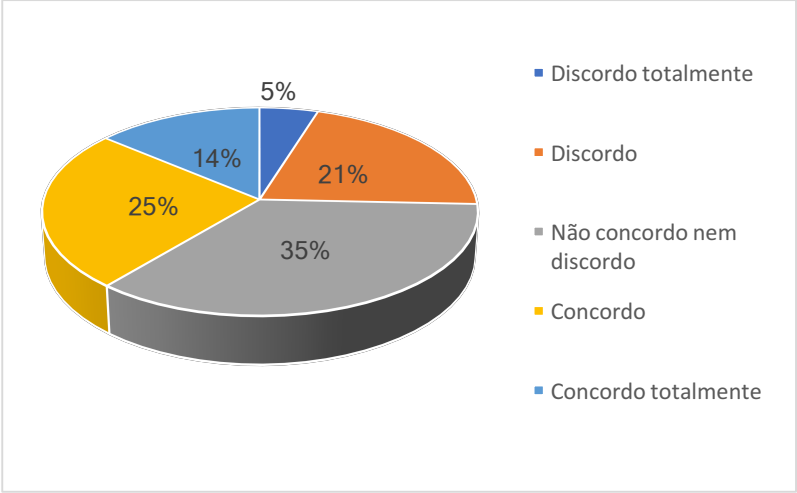


Figura n.º 15: Importância da notificação da vítima para entregar a PSE num dispositivo da sua propriedade (PQ.31).

Fonte: Elaboração Própria

Por último, na PQ.32 questionou-se sobre a utilidade de agendar e notificar uma vítima ou testemunha para que comparecesse num laboratório da GNR para que seja possível adquirir a prova em suporte eletrónico armazenada, num dispositivo da sua propriedade. Uma vez mais, destacamos a dualidade de respostas tendo por um lado,

afirmativo, respondido 40% dos inquiridos ("Concordo ou Concordo totalmente") e de forma negativa ("Discordo ou Discordo totalmente"), 31%. As respostas neutras, ou seja, "Não concordo nem discordo", foram as que obtiveram o maior número de respostas 29%.

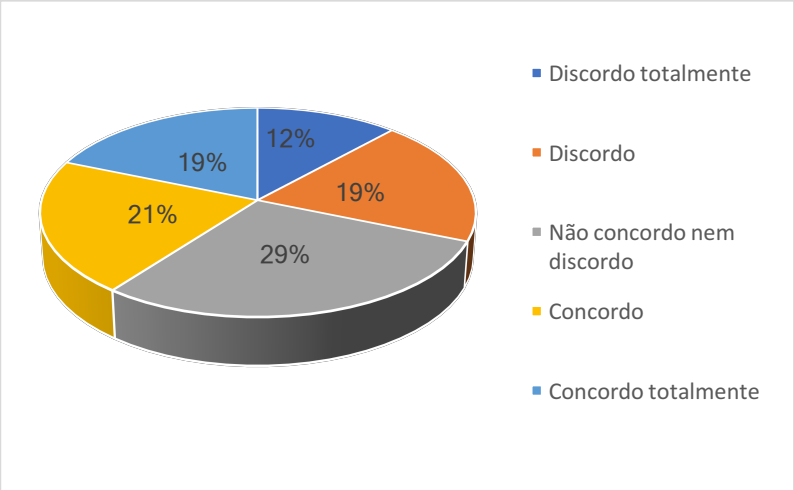


Figura n.º 16: Utilidade de agendar e notificar uma vítima ou testemunha para entregar num laboratório da GNR a PSE (PQ.32).

Fonte: Elaboração Própria

CONCLUSÕES E RECOMENDAÇÕES

Concluídas a parte I e II do presente RCFTIA, iniciaremos as conclusões com a resposta às PD e, seguidamente, à pergunta de partida. De seguida apresentaremos os objetivos gerais e a sua confirmação total, parcial ou infirmação, assim como, dos objetivos específicos. Posteriormente, efetuarmos as reflexões finais que considerarmos pertinentes. Ainda neste capítulo incluiremos as limitações que encontramos para a realização da presente investigação, assim como, aquilo que fizemos para as ultrapassar. Concluímos com uma análise que visa apoiar o desenvolvimento de investigações sucedâneas.

Com vista a dar resposta à PD.1 – "Os militares dos NIC têm conhecimento das disposições processuais que legitimam o manuseamento da PSE?" – podemos concluir que existe um conhecimento superficial.

Relativamente às entrevistas um dos intervenientes mencionou que estar a par das atualizações legislativas faz parte da obrigação de todos os militares enquanto profissionais. Por outro lado, os restantes entrevistados mencionaram existir um conhecimento básico que carece de necessidades ao nível da formação.

Através dos questionários percebemos que, relativamente à preservação e pesquisa de dados, mais de metade dos inquiridos indica não conhecer ou não estar à vontade com tais mecanismos legais. No que toca a apreensão de equipamentos e/ou dados, os resultados recolhidos indicam um conhecimento que ronda os 63%, por parte dos inquiridos. Contudo, em traços gerais, notamos uma grande taxa de respostas "não concordo nem discordo" o que pode ir ao encontro do que foi mencionado nas entrevistas, ou seja, existe conhecimento, mas o mesmo não é aprofundado.

Relativamente à PD.2, a mesma consiste em saber se "Os militares dos NIC têm conhecimentos técnicos, adquiridos em formação ou trabalho em equipa, para identificar, adquirir e preservar PSE"?

A questão n.º 4 da entrevista resultou em dois dados importantes. Por um lado, um dos entrevistados refere que estas competências não devem estar atribuídas aos NIC, adiantando que as mesmas devem ser delegadas nos núcleos de apoio técnico (NAT). Os restantes entrevistados apontam para a falta de formação e apresentam como soluções a colocação de um perito digital forense em cada CTer. Contudo são apontados custos, desde

logo na própria formação, mas também na aquisição de equipamentos importantes, que contribuem para a dificuldade da sua implementação.

Quanto aos questionários, estes permitiram concluir que existe um fraco conhecimento do conceito de prova em suporte eletrónico, mas, por outro lado, os militares demonstram ter uma grande consciência da importância deste tipo de prova. No que toca aos conhecimentos que possuem, 40% mencionou que os mesmos foram adquiridos em autoformação e apenas 25% refere o contrário. Para isto releva ainda o facto de que a maioria dos inquiridos menciona ter uma preocupação constante em permanecerem atualizados naquilo que toca às matérias foro digital.

Quanto à PD.3, a mesma tinha o intuito de esclarecer se "Os militares dos NIC dispõem de capacidades técnicas, enquanto *first responders*, para identificar, adquirir e preservar PSE"?

Através dos dados que foram recolhidos pelas respostas à pergunta n.º 5 do guião de entrevista percebemos que: no que concerne aos pedidos de diligências é o Ministério Público quem assume um papel predominante. Isto deve-se ao facto de, por um lado existir falta de formação, que limita o conhecimento daquilo que deve ser pedido, numa circunstância em concreto, e a forma como deve ser feito. Por outro lado, o Ministério Público detém alguns protocolos juntamente com os fornecedores de serviço que agilizam todo o processo de preservação ou pedidos de detalhe de clientes, como a pergunta exemplifica.

Como consequência do que foi mencionado no parágrafo anterior, podemos perceber que, apesar da lei 109/2009 permitir que todas estas diligências sejam iniciadas pelos OPC, sem autorização prévia do Ministério Público, quando haja urgência ou perigo na demora, existem ainda algumas reticências por parte dos fornecedores de serviço para o cumprimento destas ordens.

A análise dos inquéritos por questionário permitiu concluir que existe um conhecimento de que é importante aplicar procedimentos específicos, numa cena de crime e que, os mesmos podem variar dependendo do tipo de equipamento, estado de funcionamento, assim como cuidados para os documentar e preservar. Contudo quando questionados sobre alguns desses procedimentos os inquiridos revelam não os conhecer totalmente ou, em determinadas situações, não se sentirem capazes de os aplicar. Quanto ao apoio técnico (NTP), praticamente um terço dos inquiridos indica que têm sido um bom suporte, um segundo terço menciona o contrário e, os restantes respondem de forma neutra. Consideramos assim importante uma descentralização das capacidades de apoio técnico

especializado e que possam servir diretamente de apoio aos investigadores na prossecução de diligências em todo o território nacional e não apenas nas zonas da ação mais próximas dos locais onde existem Núcleos Técnico-periciais.

A PD.4 visava perceber se "Os militares dos NIC têm capacidade, ao nível do suporte técnico, para garantir o manuseamento da PSE, em testemunhas e vítimas, em sede de processos crime".

Nas entrevistas foi suscitada uma planificação de um quadro de competências a este nível. Pois alguns dos entrevistados mencionam que a recolha e aquisição deveria ser da competência dos núcleos de apoio técnico e, por sua vez, a análise deveria ser feita pelos núcleos técnico periciais.

À semelhança da resposta à PD.3, os inquiridos destacam que o pequeno número de laboratórios da GNR, apesar de realizarem um trabalho muito relevante nesta matéria, pode ajudar a compreender o reduzido nível de respostas positivas quando questionados sobre se consideram ter um apoio técnico especializado sempre que tal se afigura necessário. A falta de formação surge, novamente, como argumento utilizado pelos entrevistados, acrescentando o facto de que não existem equipamentos nem softwares, homogeneamente, distribuídos pelos NIC que permitam a extração de forma lógica, e que agilizaria o decurso dos inquéritos.

De seguida, apresentaremos a resposta à pergunta de partida que guiou toda a investigação: "Os militares dos NIC têm capacidade para executar as diligências processuais adequadas e necessárias para manusear a prova em suporte eletrónico?

De um ponto de vista geral consideramos que sim. Contudo, iremos tecer algumas conclusões relativamente à identificação, preservação, apreensão, aquisição ou extração e, por último, a análise.

Relativamente a identificação e preservação consideramos que existem ainda necessidades de formação e apoio técnico para que sejam explorados todos os meios de prova presentes no local do crime e que possam contribuir para uma maior eficácia da investigação criminal.

No que toca à apreensão, em especial do suporte físico, consideramos que os militares executam as diligências com bastante conhecimento. No âmbito da aquisição ou extração dos dados encontramos algumas limitações. Por um lado, existe falta de um quadro de competências que clarifique, dentro da estrutura da investigação criminal da GNR quem deve fazer o quê e como é que se devem praticar determinadas ações neste

âmbito. Por outro lado, verificam-se muitos casos de sobrecarga nos NTP relativamente a equipamentos, cujos dados relevantes, poderiam ser extraídos nos próprios CTer.

Por último consideramos que, ao nível da análise, os NIC se encontram bastante limitados. Posto isto releva o facto de que um maior conhecimento sobre prova em suporte eletrónico pode levar a uma maior capacidade de interpretar os relatórios que são feitos após a aquisição dos dados.

Este RCFTIA tinha como OG: "Caracterizar a capacidade dos militares dos Núcleos de Investigação Criminal da GNR no manuseamento da prova em suporte eletrónico.

Tendo em consideração todos os dados recolhidos através das entrevistas e dos inquéritos por questionário e, consequentemente, as conclusões que tecemos anteriormente consideramos que existem ainda um caminho a percorrer no âmbito da prova em suporte eletrónico dentro da GNR e, particularmente, nos NIC. Os investigadores têm contacto com este tipo de prova regularmente o quê contribui para o maior sucesso daqueles que são os objetivos da investigação criminal e, sobretudo, da lei penal e processual penal.

Contudo podemos perceber que a maioria dos militares que integram esta estrutura operativa nunca teve formação nesta área. Por outro lado, notamos também algumas carências ao nível do suporte informático que permitam a extração de dados simples dos equipamentos apreendidos ou que são voluntariamente cedidos por parte de testemunhas e vítimas.

Para além disto, consideramos como dificuldade na caracterização destas capacidades a falta de um quadro de competências e procedimentos que sejam aplicados dentro de toda a estrutura de investigação criminal na GNR.

REFERÊNCIAS BIBLIOGRÁFICAS

Acórdão n.º 241/2002/T. Constitucional. (23 de 07 de 2002). Obtido em 04 de 10 de 2019, de Diário da República Eletónico: https://dre.pt/web/guest/pesquisa/-/search/1778690/details/maximized?p_p_auth=kyMpU0hm

Acórdão Tribunal Relação do Porto. (12 de 09 de 2012). *Bases Jurídico-Documentais: IGFEJ.* Obtido em 13 de 02 de 2019, de http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/877e0322acde18d080257a8300393cc6?OpenDocument

American Psychological Association [APA]. (2012). *Manual de publicação da APA* (6ª Edição ed.). Porto Alegre: Penso Editora.

Assembleia da República. (1987). *Decreto lei nº 78/87, de 17 de fevereiro: Código de Processo Penal.* Diário da República, 1ª série, nº 40.

Assembleia da República. (2007). *Lei n.º 63/2007: Lei Orgânica da GNR.* Diário da República n.º 213/2007, 1ª Série.

Assembleia da República. (2008). *Lei nº 49/2008 de 27 de agosto: Lei de Organização da Investigação Criminal.* Diário da república nº 165, 1ª Série.

Assembleia da República. (2009). *Lei nº 109/2009 de 15 de Setembro: Lei do Cibercrime.* Diário da República, 1ª série, nº 40.

Brenner, S. W. (2010). *Cybercrime Criminal Threats from Cyberspace.* (M. a. Crime, Ed.) Praeger.

Casey, E. (2011). *Digital Evidence And Computer Crime* (Vol. 3rd ed.). Maryland: Elsevier.

Clough, J. C. (2010). *Principles of Cybercrime.* New York: Cambridge University Press.

CyberCrime@IPA. (2014). *Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecuters and Judges.* França: Conselho da Europa.

ENISA. (2014). *Electronic evidence - a basic guide for First Responders Good practice material for CERT first responders.*

Flick, U. (2005). *Métodos Qualitativos na Investigação Científica.* Lisboa: Monitor.

Fortin, M. (2009). *Fundamentos e Etapas do Processo de Investigação.* (N. Salgueiro, Trad.) Loures: Lusodidáctica.

Freixo, M. J. (2012). *Metodologia Científica* (4ª Edição ed.). Lisboa: Instituto Piajet.

GNR. (2016). *Plano de Atividades 2018.* Lisboa: Divisão de Planeamento Estratégico e Relações Internacionais.

GNR. (2017). *Relatório de Atividades 2017.* Lisboa: Divisão de Planeamento Estratégico e Relações Internacionais.

GNR. (2014). *Despacho nº 18/14-OG, 11 de Março 2014.* Lisboa: Comando Operacional.

Guerra, I. C. (2006). *Pesquisa Qualitativa e Análise de Conteúdo.* Lisboa: Princípia.

ISO. (2012). *ISO/IEC 27037:2012(E) — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.*

Lee, D. (17 de 05 de 2012). *Met Police to extract suspects' mobile phone data.* Obtido em 26 de 04 de 2019, de BBC: https://www.bbc.com/news/technology-18102793

Marconi, M. d., & Lakatos, E. M. (2003). *Fundamentos de Metodologia Científica* (5ª Edição ed.). São Paulo: Editora Atlas.

Mateus, M. (2016). *Crimes em ambiente digital - Investigação da GNR para a obtenção de prova.* Academia Militar, Lisboa.

Mesquita, P. D. (2010). *Processo Penal Prova e Sistema Judiciário.* Coimbra: Coimbra Editora.

Militão, R. L. (s.d.). *A Propósito da Prova Digital no Processo Penal*. Obtido em 21 de 04 de 2019, de Ordem dos Advogados: https://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf

Oliveira, M. M. (2011). *Como fazer projetos, relatórios, monografias, dissertações e teses* (5ª Edição ed.). Rio de Janeiro: Elsevier.

Prodanov, C. &. (2013). *Metodologia do Trabalho Científico.* Rio Grande do Sul: Editora FreeVale.

Quivy, R., & Campenhoudt, L. (2008). *Manual de Investigação em Ciências Sociais* (5ª ed.). Lisboa: Gradiva.

Ramalho, D. S. (2017). *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina.

Ramos, A. D. (2017). *A prova digital em processo penal: O correio eletrónico* (2ª Edição ed.). Lisboa: Chiado Editora.

Rodrigues, B. S. (2009). *Direito Penal. Parte Especial, I, Direito Penal Informático-Digital.* Coimbra: Coimbra Editora.

Rodrigues, B. S. (2011). *Da Prova Penal – Tomo IV, Da Prova Electrónico-Digital e da Criminalidade Informático-Digital* (1ª Ed. ed.). Rei dos Livros.

Santos, L., Francisco, G., Monteiro, F., Lima, J., Silva, N., Silva, J., . . . Afonso, C. (2016). *Orientações Metodológicas Para a Elaboração de Trabalhos de Investigação* (Vol. Caderno 8). Lisboa: Instituto de Estudos Superiores Militares.

Sarmento, M. (2008). *Guia prático sobre a metodologia científica para a elaboração, escrita e apresentação de teses de doutoramento, dissertações de mestrado e trabalhos de investigação aplicada.* Lisboa: Universidade Lusíada Editora.

Sarmento, M. (2013). *Metodologia científica para a elaboração, escrita e apresentação de teses* (1ª ed.). Lisboa.

Scientific Working Group on Digital Evidence. (11 de 02 de 2013). *SWGDE Core Competencies for Mobile Phone Forensics.* Obtido em 08 de 04 de 2019, de swgde: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Core%20Competencies%20for%20Mobile%20Phone%20Forensics

Scientific Working Group on Digital Evidence. (23 de Junho de 2016). *SWGDE Digital & Multimedia Evidence Glossary.* Obtido em 14 de Dezembro de 2017, de swgde: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Digital%20and%20Multimedia%20Evidence%20Glossary

Scientific Working Groups on Digital Evidence and Imaging Technology. (15 de Janeiro de 2010). *Guidelines & Recommendations for Training in Digital & Multimedia Evidence Version: 2.* Obtido em 13 de Dezembro de 2017, de swgde: https://www.swgde.org/documents/Current%20Documents/SWGDE-SWGIT%20Guidelines%20and%20Recommendations%20for%20Training

Sistema de Segurança Interna. (2016). *Relatório Anual de Segurança Interna.* Lisboa.

Venâncio, P. D. (2011). *Lei do Cibercrime Anotada e Comentada.* Coimbra: Coimbra Editora.

Verdelho, P., Bravo, R., Rocha, M. L., & Veiga, P. (2003). *Leis do Cibercrime* (Vol. I). Lisboa: Centro Atlântico.

APÊNDICES

Apêndice A – Estrutura da Investigação Aplicada

Objetivo geral (OG)	**Pergunta de partida (PP)**	**Objetivos específicos (OE)**	**Perguntas derivadas (PD)**
Caracterizar a capacidade dos militares dos Núcleos de Investigação Criminal da GNR no manuseamento da prova em suporte eletrónico.	Os militares dos Núcleos de Investigação Criminal têm capacidade para executar as diligências processuais adequadas e necessárias para manusear a prova em suporte eletrónico?	(OE.1) Determinar se os militares dos Núcleos de Investigação Criminal têm um conhecimento atual das disposições processuais no âmbito da PSE.	(PD.1) Os militares dos NIC têm conhecimento das disposições processuais que legitimam o manuseamento da PSE?
		(OE.2) Determinar se os militares dos Núcleos de Investigação Criminal têm a formação técnica adequada para identificar, adquirir e preservar PSE.	(PD.2) Os militares dos NIC têm conhecimentos técnicos, adquiridos em formação ou trabalho em equipa, para identificar, adquirir e preservar PSE?
		(OE.3) Analisar as capacidades técnicas que os NIC têm, enquanto *first responder*, para identificar, adquirir e preservar PSE relevante em diligências processuais (no âmbito das medidas cautelares ou em buscas) em sede de processos crime.	(PD.3) Os militares dos NIC dispõem de capacidades técnicas, enquanto *first responders*, para identificar, adquirir e preservar PSE?
		(OE.4) Analisar as capacidades técnicas que os NIC têm para adquirir, em testemunhas e vítimas, de forma manual e lógica bem como para analisar PSE em sede de processos crime.	(PD.4) Os militares dos NIC têm capacidade, ao nível do suporte técnico, para garantir o manuseamento da PSE, em testemunhas e vítimas, em sede de processos crime?

Quadro n.º 8: Estrutura da Investigação Aplicada

Pergunta de partida (PP)	**Perguntas derivadas (PD)**	**Guião de Entrevista**
(PP) Os militares dos Núcleos de Investigação Criminal têm capacidade para executar as diligências processuais adequadas e necessárias para manusear a prova em suporte eletrónico?	(PD.1) Os militares dos NIC têm conhecimento das disposições processuais que legitimam o manuseamento da PSE?	3- Considera que os militares das GNR, nomeadamente, dos Núcleos de Investigação Criminal têm um conhecimento adequado relativo às disposições processuais no âmbito da PSE?
	(PD.2) Os militares dos NIC têm conhecimentos técnicos, adquiridos em formação ou trabalho em equipa, para identificar, adquirir e preservar PSE?	4- Da sua experiencia, que capacidades técnicas deveriam ser melhoradas nos NIC para identificar, adquirir, preservar e analisar PSE para os processos crime?
	(PD.3) Os militares dos NIC dispõem de capacidades técnicas, enquanto *first responders*, para identificar, adquirir e preservar PSE?;	5- Considera que os NIC têm conhecimentos adequados para efetuar pedidos de diligências distintos aos processos crime para recolha de PSE, como por exemplo, a preservação de dados em plataformas (Facebook, Instagram), pedido de detalhe de clientes aos ISP ou para cumprir mandados de pesquisa de dados informáticos.
	(PD.4) Os militares dos NIC têm capacidade, ao nível do suporte técnico, para garantir o manuseamento da PSE, em testemunhas e vítimas, em sede de processos crime?	6- Considera que os NIC são capazes de adquirir corretamente prova em suporte eletrónico, em equipamentos de testemunhas e vítimas, de forma manual e lógica bem como para analisar PSE em sede de processos crime.

Quadro n.º 9: Relação entre as as perguntas do Guião de Entrevista, a pergunta de partida e perguntas derivadas.

Apêndice B – Pedido de divulgação dos Inquéritos por Questionário

Divulgação de questionário

Vitor Manuel Seixas Teixeira
GNR_CO_DIC; Tiago Lourenco Lopes
segunda-feira, 1 de abril de 2019, 13:43
Mostrar Detalhes

Bom dia Meu Coronel,

Eu, Vitor Manuel Seixas Teixeira, Aspirante da GNR, a frequentar o 5.º e último ano do Mestrado Integrado em Ciências Militares, na especialidade de Segurança, venho por este meio solicitar a V. Ex.ª, Coronel de Infantaria da GNR Amândio Manuel de Jesus Marques, a colaboração no âmbito do Trabalho de Investigação Aplicada. O presente pedido reflete a necessidade de realização de entrevistas com vista à recolha de informações, bem como ao esclarecimento de questões decorrentes da investigação científica, subordinada ao tema: "Os Núcleos de Investigação Criminal da Guarda Nacional Republicana e o manuseamento da prova em suporte eletrónico".
Desta forma questiono a possibilidade de serem difundidos aos militares dos NIC, através da Divisão de Investigação Criminal, um inquérito por questionário por forma a poder caracterizar as suas capacidades no manuseamento da prova digital.
O formulário supramencionado, encontra-se em https://docs.google.com/forms/d/e/1FAIpQLSfsZU53Tz1tT9tDZaA5NipHQlLOZZs80dTA1T-7vEBBGsnHoA/viewform?usp=sf_link e o mesmo estará disponível para preenchimento até ao dia 150900ABR19.
O presente email foi em enviado com conhecimento do Major de Infantaria da GNR Tiago Lourenço Lopes, coorientador desta investigação científica.

Apêndice C – Inquérito por Questionário

Perguntas Derivadas (PD)	Perguntas Questionário (PQ)
(PD.1) Os militares dos NIC têm conhecimento das disposições processuais que legitimam o manuseamento da PSE?	PQ1. Tenho conhecimento do capítulo III da Lei 109/2009 de 15 de Setembro (Lei do cibercrime) que define as disposições processuais especiais para manusear prova em suporte eletrónico? PQ2. Tenho consciência de que a preservação, pesquisa e apreensão de prova em suporte eletrónico pode ser feita para qualquer tipo de crime. PQ3. Enquanto OPC, posso ordenar a quem tiver a disponibilidade ou controlo de dados em suporte eletrónico, nos casos de urgência ou perigo na demora, a sua preservação, até um máximo de três meses. PQ4. Numa diligência processual para preservar dados em suporte eletrónico, tenho consciência que posso notificar quem tiver a disponibilidade ou controlo dos mesmos, quando: a) quem tem disponibilidade ou controlo de dados não os fornece de imediato; b) não existe o suporte técnico necessário para os adquirir no momento; ou c) ser necessário uma ordem judicial para apreender os dados. PQ5. Enquanto OPC, posso efetuar a pesquisa de dados informáticos específicos e determinados armazenados num determinado sistema informático, quando existir consentimento por quem tiver a disponibilidade ou controlo dos mesmos. PQ6. Conheço os termos a lavrar no Termo de Consentimento para efetuar uma pesquisa de dados com vista a notificar quem tiver a disponibilidade ou controlo dos mesmos. PQ7. A pesquisa de dados sem autorização prévia da Autoridade Judiciária está prevista para os casos de criminalidade violenta, onde exista perigo para a vida ou situações de ofensas à integridade física graves. PQ8. Tenho conhecimento de que relativamente à apreensão de dados informáticos, a mesma pode incidir sobre: a) apreensão do suporte físico; ou b) cópia dos dados em suporte autónomo. PQ9. Tenho conhecimento que as apreensões de prova em suporte eletrónico devem ser validadas no prazo de 72 horas, pela AJ competente. PQ10. Tenho consciência de que, se durante uma pesquisa, a) identificar dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiros; ou b) várias mensagens de correio eletrónico ou registos de comunicações de natureza semelhante não lidos, tenho de os submeter para validação para o JIC.

(PD.2) Os militares dos NIC têm conhecimentos técnicos, adquiridos em formação ou trabalho em equipa, para identificar, adquirir e preservar PSE?	PQ11. Considero que conheço o conceito de PSE: "qualquer dado guardado ou transmitido através da utilização de um dispositivo eletrónico que suporte ou refute a teoria de como um crime ocorreu ou todas as circunstâncias que possam provar uma intenção ou um álibi". PQ12. Considero que a PSE é um importante meio de obtenção de prova para a investigação criminal. PQ13. Considera ter a formação técnica necessária, para identificar a forma mais adequada (manual, lógica ou física), para aceder aos conteúdos de equipamentos. PQ14. Considero que caso necessite de apoio técnico especializado para identificar, adquirir e preservar prova em suporte eletrónico relevante para um processo crime, sei a que órgão ou a que especialista posso recorrer. PQ15. A formação técnica e o treino que possuo para identificar, adquirir e preservar prova em suporte eletrónico foi adquirida em autoformação ou através de trabalho em equipa. PQ16. Preocupo-me, continuamente, em obter mais conhecimentos sobre procedimentos e suporte técnico que possam garantir o manuseamento de prova em suporte eletrónico. PQ17. Considero que necessito de formação e treino técnico para efetuar, pesquisa, a preservação e a apreensão de PSE nos seguintes tipos de dispositivos: Telefones celulares (incluindo smartphones) e cartões SIM Computador padrão, com possibilidade de conexões de rede Suportes para armazenamento digital usada em computadores: discos rígidos (HDD, SSD), discos ópticos (CD/DVD/Dual Layer), Pen drives USB e cartões de memória Câmaras fotográficas e de vídeo digitais (incluindo o CCTV) Sistemas de navegação móvel (GPS) Dispositivos com funções para ligação em redes (TCP / IP e outros protocolos digitais), tais como HUB's, switches, routers, pontos de acesso wireless Dispositivos IoT (Playstation, Xbox, Smart tv, etc.) Sistemas de acesso a armazenamento remoto (drives, clouds) Veículos (eventos do veículo, dados de localização, dados de rede)

(PD.3) Os militares dos NIC dispõem de capacidades técnicas, enquanto *first responders*, para identificar, adquirir e preservar PSE?	PQ18. Entendo a importância de no momento da apreensão, etiquetar e preservar os códigos de PIN ou padrão de bloqueio de acesso aos dispositivos eletrónicos. PQ19. Compreendo as consequências e os riscos associados à alteração da integridade da prova durante a pesquisa a um dispositivo apreendido. PQ20. Compreendo que a colocação de cartões SIM ou de memória em diferentes computadores ou dispositivos móveis podem alterar os dados originais. PQ21. Entendo que a remoção ou a substituição de uma bateria pode fazer com que o telefone reinicie, altere ou elimine dados. PQ22. Considero que um computador ligado pode conter dados voláteis armazenados (memória RAM, ID, Históricos), que podem ser importantes adquirir e preservar. PQ23. Tenho consciência da importância da documentação dos dados voláteis com vista a garantir a cadeia de custódia da prova. PQ24. Considero ter um apoio técnico especializado na GNR disponível para dar apoio a diligências confiadas ao NIC para adquirir prova em suporte eletrónico. PQ25. Estou consciencializado para a importância de, numa cena de crime ou numa busca, questionar o detentor dos dados sobre passwords, quais os utilizadores, possíveis conexões a redes, e registar essas informações. PQ26. Conheço os procedimentos para preservar dados a) se o dispositivo estiver ligado; b) se estiver conectado a uma rede wifi ou outra; c) se estiver desbloqueado; ou d) se estiver desligado. PQ27. Tenho conhecimento de que quando se efetua a apreensão de dados a custódia e integridade dos mesmos deve ser garantida pelo cálculo do valor *Hash* e efetuar o seu registo nos autos.

(PD.4) Os militares dos NIC têm capacidade, ao nível do suporte técnico, para garantir o manuseamento da PSE, em testemunhas e vítimas, em sede de processos crime?	PQ28. Considera que tem os conhecimentos técnicos adequados para adquirir de forma manual e documentar os dados presentes na memória interna de um telemóvel. PQ29. Considera que tem os conhecimentos técnicos adequados para adquirir, no nível lógico, e documentar os dados presentes na memória interna de um telemóvel. PQ30. Caso seja necessário adquirir dados de uma vítima armazenados no seu email particular, após a elaboração do respetivo Termo de Consentimento, para a pesquisa de dados informáticos, cedo o computador da GNR para a vítima aceder à conta e retirar os dados relevantes. PQ31. Considero útil notificar uma vítima ou testemunha para entregar em 10 dias ao processo crime, a prova em suporte eletrónico armazenada num dispositivo da sua propriedade. PQ32. Considero útil agendar e notificar uma vítima ou testemunha para comparecer num laboratório (NTP do Porto, Coimbra, Lisboa ou Faro) para adquirir a prova em suporte eletrónico armazenada num dispositivo da sua propriedade.

Quadro n.º 10: Relação entre as perguntas do questionário e as perguntas derivadas.

Apêndice D – Análise dos Resultados do Inquérito por Questionário

D.1. Resultados da Parte 2 - Caraterização Sociodemográfica

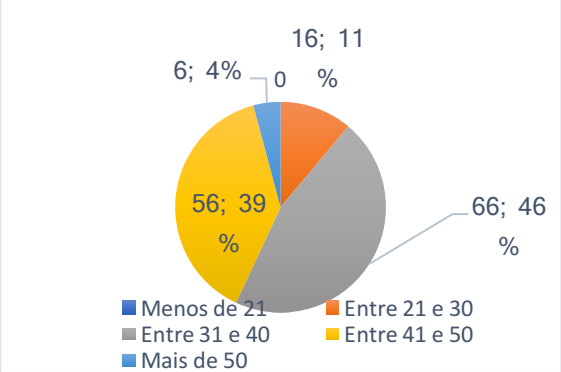


Figura n.º 17: Nível etário.

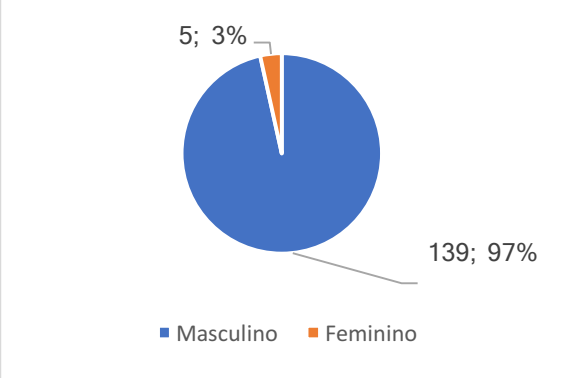


Figura n.º 18: Género.

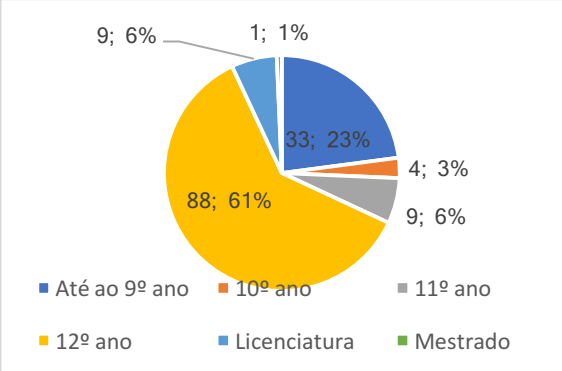


Figura n.º 19: Habilitações literárias.

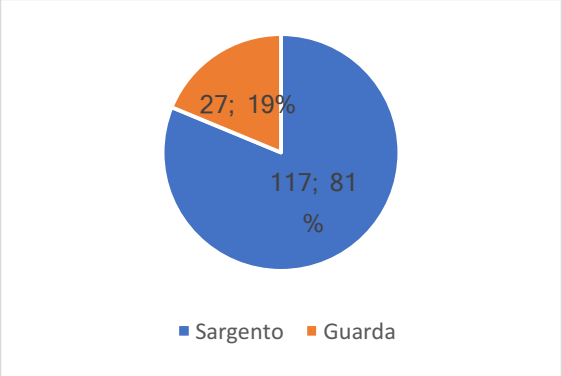


Figura n.º 20: Categoria profissional.

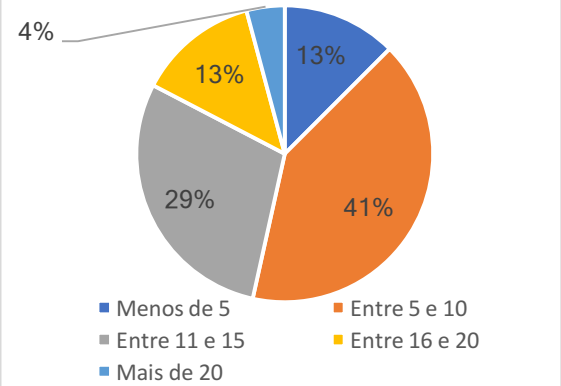


Figura n.º 21: Anos na estrutura da IC.

D.2. Resultados da Parte 2 – Diposições processuais no âmbito da prova em suporte eletrónico

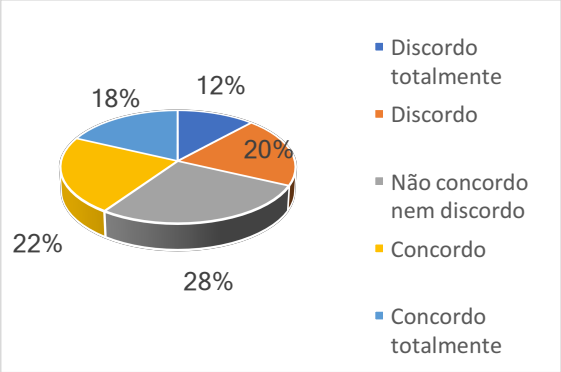


Figura n.º 22: Ordem para preservação de dados pelo OPC (PQ3).

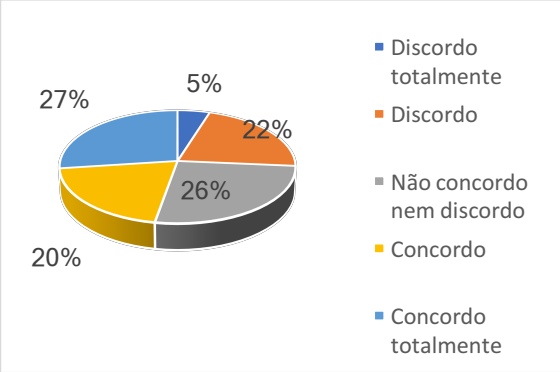


Figura n.º 23: Notificação para preservar quem não fornece os dados de imediato(PQ4.a).

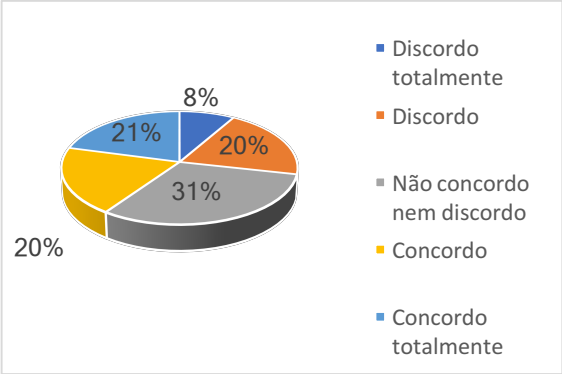


Figura n.º 24: Notificação para preservar quando não existe suporte técnico (PQ4.b).

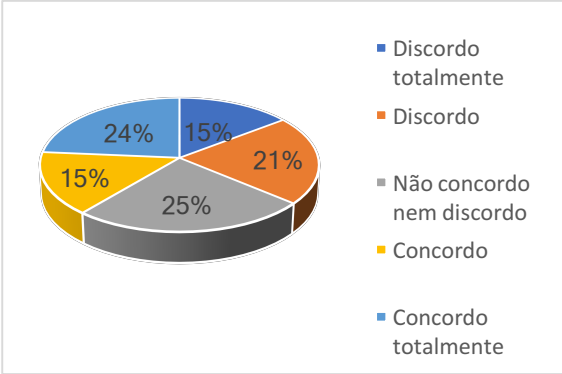


Figura n.º 25: Notificação para preservar quando é necessário ordem judicial para apreender(PQ 4.c).

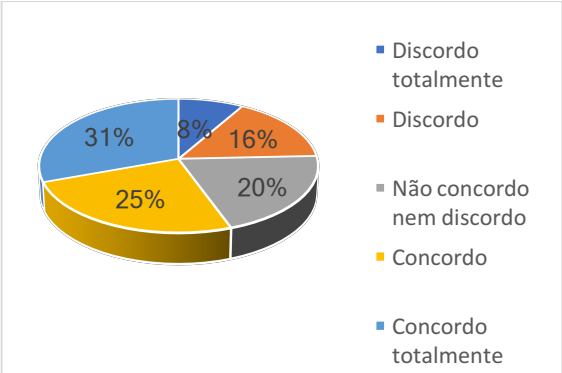


Figura n.º 26: Pesquisa de dados quando existe consentimento pelo detentor (PQ 5).

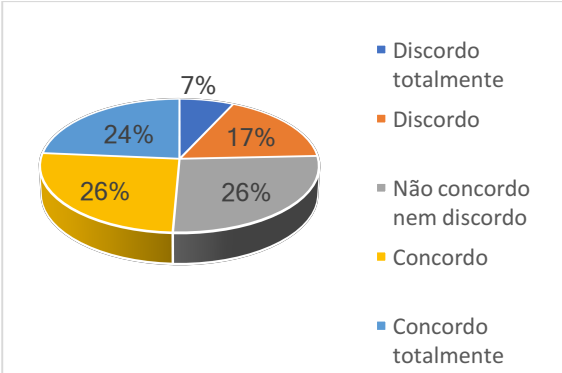


Figura n.º 27: Conhecimento dos Termos de Consentimento (PQ 6).

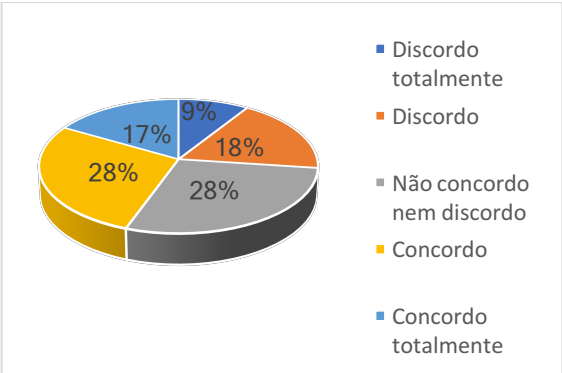


Figura n.º 28: Pesquisa de dados sem autorização prévia da AJ (PQ 7).

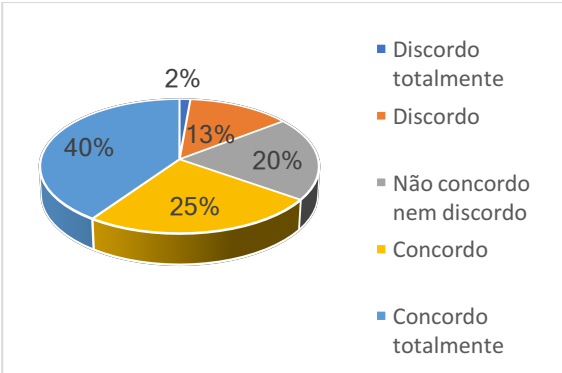
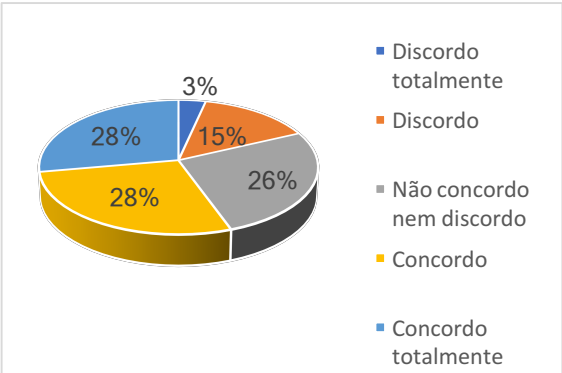


Figura n.º 29: Apreensão do suporte físico (PQ 8.a).



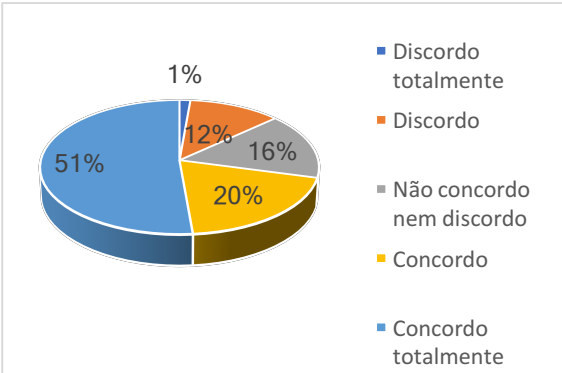


Figura n.º 30: Apreensão através de cópia dos dados(PQ 8.b).

Figura n.º 31: Conhecimento do espaço temporal para validação das PSE (PQ 9).

D.3. Resultados da Parte 3 – Capacidades técnicas enquanto *First Responders*

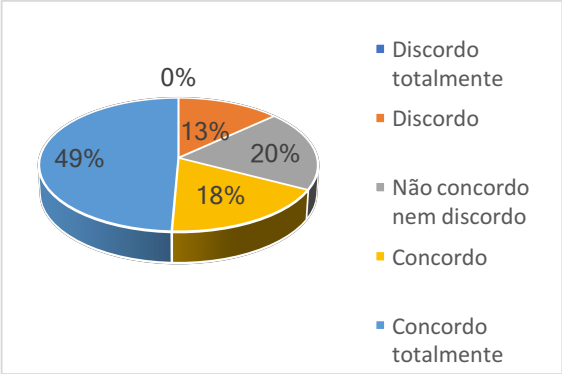


Figura n.º 32: Importância do registo de códigos e padrões durante a apreensão(PQ 18).

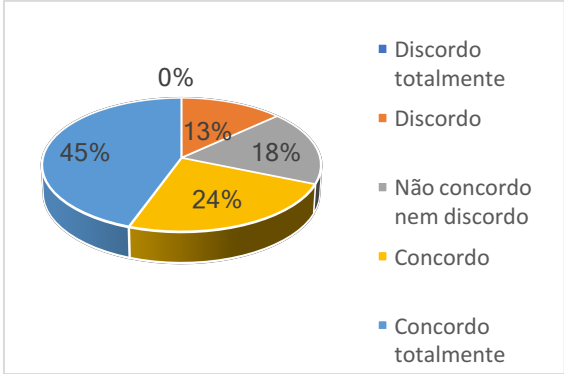


Figura n.º 33: Consequências da alteração da integridade da prova durante a pesquisa(PQ 19).

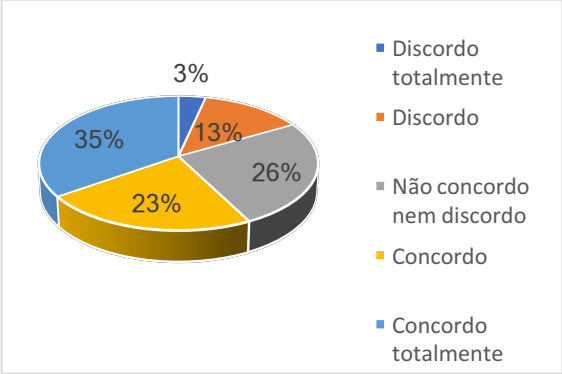


Figura n.º 34: Consequências da colocação de cartões SIM ou de memória(PQ 20).

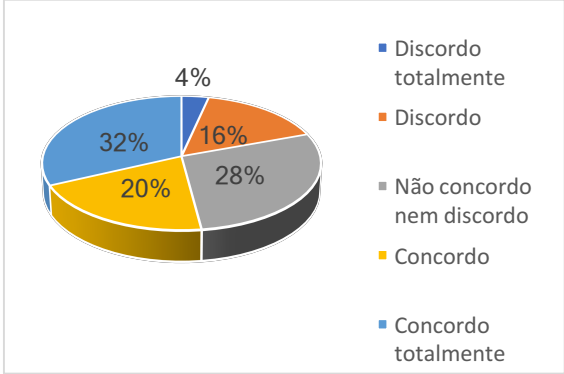


Figura n.º 35: Consequências da remoção de uma bateria (PQ 21).

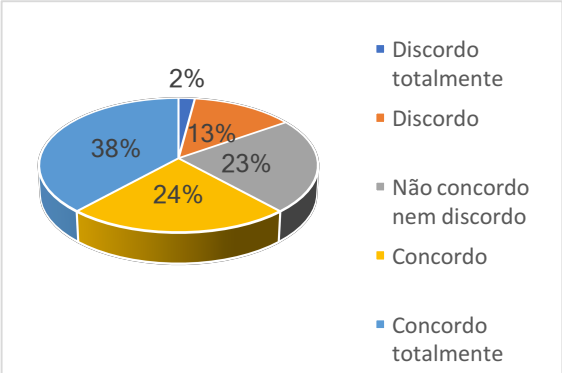


Figura n.º 36: Conhecimento de dados voláteis (PQ 22).

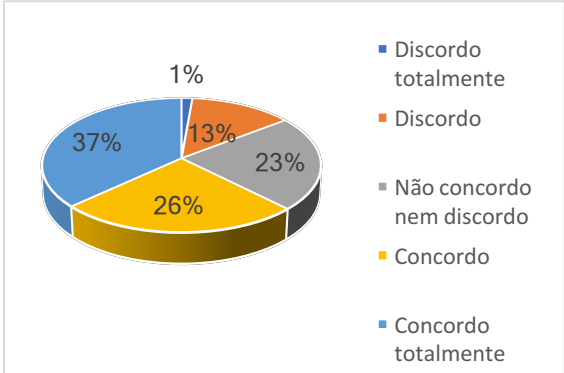


Figura n.º 37: Importância da documentação dos dados voláteis (PQ 23).

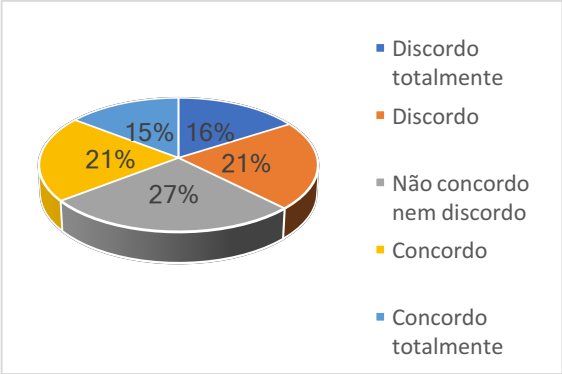


Figura n.º 38: Consideração sobre o apoio técnico existente (PQ 24).

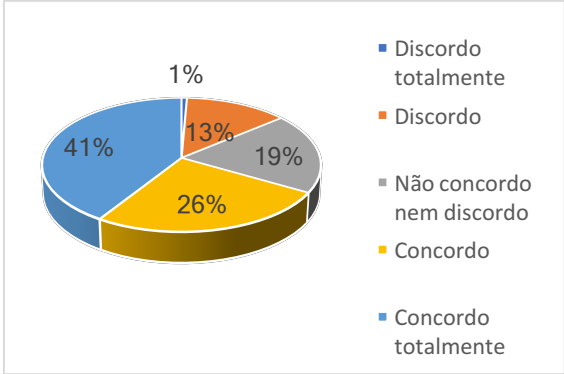


Figura n.º 39: Importância de questionar sobre passwords (PQ 25).

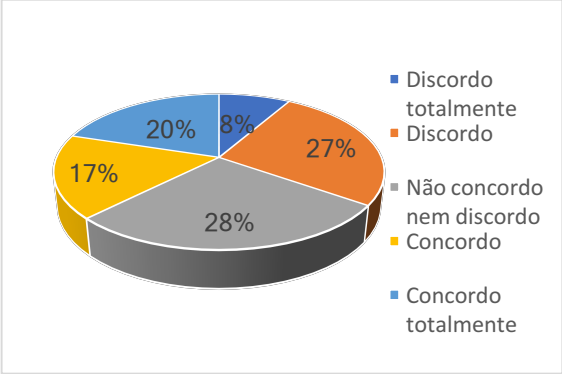


Figura n.º 40: Conhecimentos para preservar se o dispositivo estiver ligado (PQ 26.a).

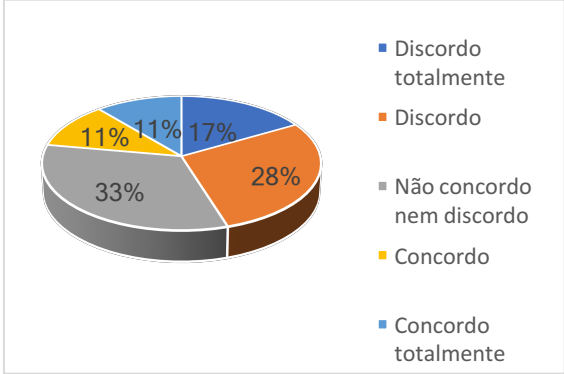


Figura n.º 41: Conhecimentos para preservar se o dispositivo estiver conectado a uma rede(PQ 26.b).

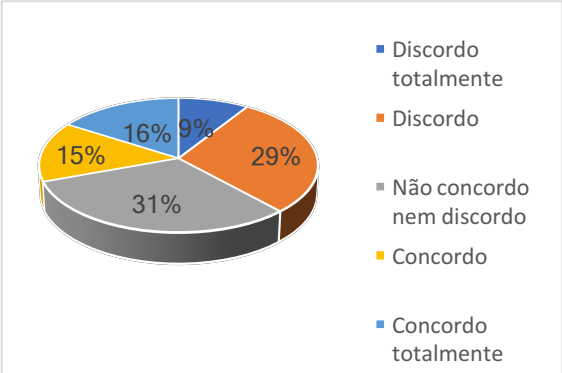


Figura n.º 42: Conhecimentos para preservar se o dispositivo estiver desbloqueado (PQ 26.c).

D.4. Resultados da Parte 4 – Capacidades técnicas para adquirir, em testemunhas e vítimas, de forma manual e lógica, bem com para analisar PSE

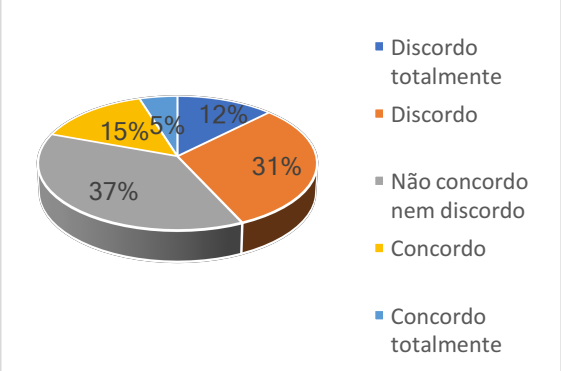


Figura n.º 43: Conhecimentos técnicos para adquirir manualmente dados presentes na memória de um telemóvel(PQ 28).

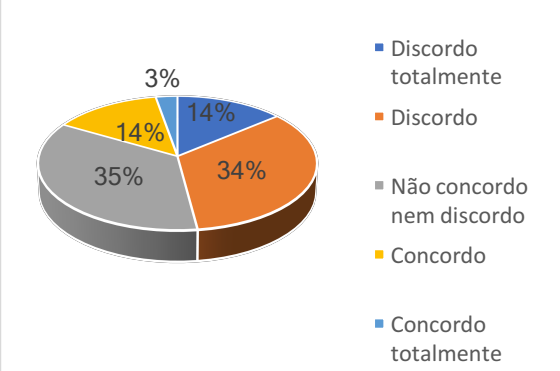


Figura n.º 44: : Conhecimentos técnicos para adquirir logicamente dados presentes na memória de um telemóvel (PQ 29).

Apêndice E – Carta de Apresentação

ACADEMIA MILITAR

Os Núcleos de Investigação Criminal da Guarda Nacional Republicana e o manuseamento da prova em suporte eletrónico

Autor: Aspirante Aluno de Cavalaria da GNR Vitor Manuel Seixas Teixeira

Orientador: Professora Doutora Ana Maria Carapelho Romão Leston Bandeira
Coorientador: Major de Infantaria da GNR Tiago Lourenço Lopes

Relatório Científico Final do Trabalho de Investigação Aplicada
Lisboa, maio de 2019

CARTA DE APRESENTAÇÃO

A Academia Militar (AM) é um estabelecimento de ensino superior público universitário militar com a finalidade principal de formar Oficiais destinados aos quadros permanentes do Exército e da Guarda Nacional Republicana (GNR).

Na fase final dos ciclos de estudos integrados, com vista à obtenção do grau de mestre, os Alunos da AM executam um Relatório Cientifico Final do Trabalho de Investigação Aplicada (RCFTIA), o qual é submetido à apreciação e discussão pública perante um júri, tendo como finalidade a aplicação de competências adquiridas, o desenvolvimento de capacidades e a exposição das suas conclusões, em contexto de investigação, nos domínios da segurança e defesa.

Desta forma, eu, Vitor Teixeira, Aspirante da GNR, a frequentar o 5.º e último ano do Mestrado Integrado em Ciências Militares, na especialidade de Segurança, venho por este meio solicitar a V. Ex.ª a colaboração no âmbito do TIA, dada a necessidade de realização de entrevistas com vista à recolha de informações, bem como ao esclarecimento de questões decorrentes da investigação, subordinada ao tema: "Os Núcleos de Investigação Criminal da Guarda Nacional Republicana e o manuseamento da prova em suporte eletrónico".

Esta investigação tem como objetivo geral caracterizar a capacidade dos militares dos Núcleos de Investigação Criminal da GNR no manuseamento da prova digital.

Os entrevistados foram escolhidos com base no seu elevado grau de conhecimento e domínio sobre os assuntos tratados na investigação.

Assim sendo, solicito a V. Ex.ª que me conceda uma entrevista, tendo em conta que o seu contributo será preponderante para que se atinjam os objetivos propostos na investigação.

Grato pela colaboração e disponibilidade.

Atenciosamente,
Vitor Teixeira
Aspirante de Cavalaria da GNR

ENQUADRAMENTO

No âmbito do mestrado integrado em Ciências Militares, na especialidade de Segurança da Guarda Nacional Republicana (GNR), surge o presente Relatório Científico Final do Trabalho de Investigação Aplicada (RCFTIA), subordinado ao tema: "Os Núcleos de Investigação Criminal da GNR e o manuseamento da prova em suporte eletrónico". Para além de representar a conclusão do curso de formação de Oficiais da GNR, o RCFTIA revela-se como uma mais-valia para a GNR na medida em que contribui para o conhecimento aprofundado em diversas matérias institucionais. A presente investigação focaliza-se na problemática do manuseamento da prova em suporte eletrónico por parte dos Núcleos de Investigação Criminal, tendo como objetivo caracterizar a capacidade dos militares dos Núcleos de Investigação Criminal da GNR no manuseamento da prova em suporte eletrónico.

Uma das orientações estratégicas para o ano 2017, mencionadas no Relatório Anual de Segurança Interna, no âmbito da segurança no ciberespaço é "reforçar a área da prevenção e repressão do cibercrime e reforçar a capacidade de aquisição da prova digital" (Sistema de Segurança Interna, 2016, p. 231).

A preocupação levantada no anterior parágrafo decorre do acréscimo generalizado da prática de condutas criminosa através do uso de meios informáticos ou contra um bem informático, e ainda, crimes comuns onde é cada vez mais relevante a prova eletrónica armazenada em dispositivos e nas redes (Sistema de Segurança Interna, 2016, p. 31).

No RASI de 2016 pode ler-se que o sucesso da prevenção e da investigação criminal nesta tipologia de crimes passa pela "formação profissional continuada" (Sistema de Segurança Interna, 2016, p.31). Esta determinação encontra-se igualmente patente no Scientific working groups on Digital Evidence and Imaging Technology onde consta que todo o pessoal encarregue por adquirir, preservar, analisar e/ou examinar provas digitais ou multimédia deve estar a par dos procedimentos comummente seguidos pela comunidade forense e devem seguir as recomendações que os próprios emanam (Scientific Working Groups on Digital Evidence and Imaging Technology, 2010, p. 3). O autor Armando Dias Ramos reforça esta ideia escrevendo que o "investigador criminal que proceda à apreensão de prova informático-digital, para além dos conhecimentos técnicos informáticos que lhe são requeridos, também terá que saber lidar convenientemente com este tipo de prova, quer

na sua apreensão, manuseamento e transporte, quer na análise/exame que posteriormente irá recair sobre a mesma" (Ramos, 2017, p. 194) .

Caso não sejam adotados procedimentos que respeitem as características das provas digitais, o "risco de não se conseguir efetuar uma perícia forense condigna" é elevado (Ramos, 2017, p. 199). "O mesmo é dizer que não se conseguirão reunir elementos de prova que possam ser, em sede de audiência e julgamento, valorados condignamente e relevantes para a discussão da causa" (Ramos, 2017, pp. 199-200).

Para além das competências e dos procedimentos, existe um terceiro fator preponderante para a redução da volatilidade dos dados informáticos recolhidos. Este fator, que denominamos por suporte informático, caracteriza-se pela necessidade de existirem softwares e hardwares que permitam não só a recolha de indícios mas também o seu armazenamento e transporte (Scientific Working Groups on Digital Evidence and Imaging Technology, 2010, p. 8).

O estudo incidirá nos Núcleos de Investigação Criminal (NIC) que executam funções operativas de IC e estão distribuídos pelos Comandos Territoriais (CTer). Os NIC encontram-se fisicamente sediados nos Destacamentos Territoriais (DTer), embora dependam funcionalmente das Secções de Informações e Investigação Criminal dos CTer. Os NIC têm como missão genérica desenvolver a atividade de investigação criminal, compreendendo esta o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo.

Apêndice F – Guião da Entrevista

GUIÃO DA ENTREVISTA

DADOS SOCIOMÉTRICOS

- **Instituição:**
- **Funções:**
- **Idade:**

ENTREVISTA

Perguntas (P):

1- Da sua experiência profissional no âmbito de processos-crime, considera que a PSE tem contribuído para a eficácia da investigação criminal?

2- Durante o desempenho das suas funções já teve diligências de processos confiados a militares dos NIC em que tenha sido necessário o manuseamento de PSE?

3- Considera que os militares das GNR, nomeadamente dos NIC, têm um conhecimento adequado relativo às disposições processuais no âmbito da PSE?

4- Da sua experiência, que capacidades técnicas deveriam ser melhoradas nos NIC para identificar, adquirir, preservar e analisar PSE para os processos crime?

5- Considera que os NIC têm conhecimentos adequados para efetuar pedidos de diligências, para recolha de PSE no âmbito de processos crime, como por exemplo, a preservação de dados em plataformas (Facebook, Instagram), pedido de detalhe de clientes aos ISP ou para cumprir mandados de pesquisa de dados informáticos?

6- Considera que os NIC são capazes de adquirir e analisar corretamente PSE, em equipamentos de testemunhas e vítimas, de forma manual e lógica, em sede de processos crime?

Muito obrigado pela sua colaboração