ACADEMIA MILITAR

Núcleo Digital Forense da Guarda Nacional Republicana

Autor: Aspirante GNR Infantaria José Miguel Armada de Matos

Orientadora: Doutora Paula Sofia de Vasconcelos Casimiro

Coorientador: Tenente-Coronel GNR Infantaria Tiago Lourenço Lopes

Mestrado Integrado em Ciências Militares – Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, maio de 2021

ACADEMIA MILITAR

Núcleo Digital Forense da Guarda Nacional Republicana

Autor: Aspirante GNR Infantaria José Miguel Armada de Matos

Orientadora: Doutora Paula Sofia de Vasconcelos Casimiro

Coorientador: Tenente-Coronel GNR Infantaria Tiago Lourenço Lopes

Mestrado Integrado em Ciências Militares – Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, maio de 2021

EPÍGRAFE

"A tecnologia é uma faca de dois gumes: se pode ser manipulada no âmbito de atividades ilícitas, também pode ser utilizada para combater estas últimas."

Carrapiço (2005, p. 177)

AGRADECIMENTOS

Ao longo da presente investigação, muitos foram aqueles que, através do seu contributo a nível da sua experiência e conhecimento, contribuíram significativamente para o desenvolvimento da mesma. Assim, a presente investigação representa por um lado a reta final de um ciclo de formação de cinco anos, e por outro, o início de carreira de Oficial da Guarda Nacional Republicana. Desta forma, considerando a simbologia associada à mesma, os reconhecimentos inframencionados, dizem respeito à mesma e a todos aqueles que contribuíram para a sua execução.

À minha orientadora, a Senhora Professora Doutora Paula Sofia de Vasconcelos Casimiro pela ajuda inicial da presente investigação, nomeadamente a estrutura da mesma e quais as temáticas que seriam importantes abordar e também pelas correções dos guiões de entrevista a serem usados nos inquéritos por entrevista aos Chefes de Secção de Informações e Investigação Criminal e aos Procuradores do Ministério Público, dos questionários a serem distribuídos aos militares dos Núcleos Digitais Forenses e do Trabalho de Investigação Aplicada.

Ao meu coorientador, o Senhor Tenente-Coronel da Guarda Nacional Republicana Tiago Lourenço Lopes por toda a predisposição de me auxiliar e esclarecer todas as dúvidas que foram surgindo ao longo da investigação, abdicando muitas horas do seu tempo pessoal para que fosse possível resolver todas as dúvidas no mais breve tempo possível.

Ao Senhor Major da Guarda Nacional Republicana Rui Valente Cipriano Alfaro Pereira que, como Diretor de Curso do XXVI Tirocínio para Oficiais na Escola da Guarda, se constituiu como um pilar importantíssimo neste último ano de formação, mostrando-se sempre disponível para atender a todos os problemas não só durante a execução do Trabalho de Investigação Aplicada, bem como durante toda a formação na Escola da Guarda.

Ao Senhor Tenente-Coronel Diogo Almeida e Brito Moreira Dores, Chefe da Divisão de Criminalística da Direção de Investigação Criminal da Guarda Nacional Republicana por todo o auxílio fornecido durante a execução da presente investigação, não só pelas informações que me pôde fornecer relativas ao tema da mesma, bem como pela divulgação dos inquéritos por questionário aos militares dos Núcleos Digitais Forenses.

Ao Senhor Sargento-Chefe José António Santana de Campos, Chefe da Secção de Recolha de Prova Digital da Direção de Investigação Criminal da Guarda Nacional

Republicana pela prontidão com que me pôde fornecer dados relacionados com o tema da investigação.

A todos os entrevistados que, quer na qualidade de Chefes da Secção de Informações e Investigação Criminal, quer na qualidade de Procuradores do Ministério Público, contribuíram com a sua experiência permitindo assim uma visão mais prática sobre a temática da prova digital.

A todos os militares dos Núcleos Digitais Forenses que responderam ao inquérito, pois estes são aqueles que trabalham com a prova digital diariamente, tornando assim percetível uma visão muito mais profunda no que toca não só ao trabalho dos Núcleos Digitais Forenses, bem como dos próprios militares.

RESUMO

Tendo em conta que os Núcleos Digitais Forenses começaram a ser implementados no ano de 2018, ainda são relativamente recentes na Guarda Nacional Republicana. Assim, a presente investigação tem como objetivo geral, analisar as capacidades dos militares pertencentes a qualquer Núcleo Digital Forense da Guarda Nacional Republicana no âmbito do tratamento da prova digital. Tem ainda como objetivos específicos: analisar se a formação que os militares constituintes dos NDF receberam é adequada à sua função; analisar se os NDF se encontram munidos com os recursos tecnológicos (*hardware* e *software*) e humanos necessários para o tratamento da prova digital; determinar o tempo das pendências, ou seja, o tempo que demoram a ser realizados os diversos exames à prova digital; determinar o valor da prova digital como meio de prova; perceber se os militares são ouvidos durante o processo em tribunal e se sim, se são ouvidos como testemunhas ou como peritos.

A presente investigação baseia-se no método dedutivo, assim, o ponto de partida da mesma é a conceção da pergunta de partida e das perguntas derivadas, objetivo geral e objetivos específicos, respetivamente. No que concerne às técnicas de recolha de dados, a presente investigação é apoiada em conteúdo documental, inquéritos por entrevista e inquéritos por questionário.

Como principais resultados, constatou-se que os militares têm uma boa formação para a realização do seu trabalho e que deve haver um reforço não só a nível de *software* e de *hardware*, mas também a nível de recursos humanos. Também se auferiu que o tempo das pendências deverá ser calculado de uma outra forma, fruto de todas as variáveis relacionadas com o mesmo, que a prova digital é cada vez mais importante no âmbito dos processos e que os militares são ouvidos em tribunal de forma informal, de modo a auxiliar o juiz, magistrado ou procurador.

PALAVRAS-CHAVE

Guarda Nacional Republicana; Investigação Criminal; Prova Digital; Núcleo Digital Forense.

ABSTRACT

Bearing in mind that the Forensic Digital Nuclei began to be implemented in 2018, they are still relatively recent in the Republican National Guard. Thus, the present investigation has as its general objective, to analyze the capabilities of the military belonging to any Digital Forensic Nucleus of the National Republican Guard in the scope of the treatment of the digital evidence. It also has the following specific objectives: to analyze if the training that the military members of the NDF received is adequate for their function; analyze if the NDF are equipped with the technological resources (hardware and software) and human resources necessary for the treatment of the digital evidence; determine the pending time, that is, the time it takes to perform the various digital proof exams; determine the value of digital proof as a means of proof; understand whether the military is heard during the court process and if so, whether it is heard as witnesses or experts.

The present investigation is based on the deductive method, thus, the starting point of it is the conception of the starting question and the derived questions, general objective and specific objectives, respectively. With regard to data collection techniques, the present investigation is supported by documentary content, surveys by interview and surveys by questionnaire.

As main results, it was found that the military has a good training to carry out their work and that there should be a reinforcement not only in terms of software and hardware, but also in terms of human resources. It should also be noted that the pending time must be calculated in another way, as a result of all the variables related to it, that digital evidence is increasingly important in the context of cases and that the military is heard in court informally, in order to assist the judge, magistrate or prossecutor.

KEYWORDS

Republican National Guard; Criminal Investigation; Digital Evidence; Digital Forensic Nucleus.

ÍNDICE GERAL

ÍNDICE DE QUADROS

ÍNDICE DE TABELAS

LISTA DE APÊNDICES

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AJ	Autoridade Judiciária
AM	Academia Militar
AR	Assembleia da República
art.	artigo
arts.	artigos
CAS	*Cellebrite Advanced Services*
CCTV	*Closed-circuit television*
CDF	Curso Digital Forense
CEPOL	Agência da União Europeia para a Formação Policial
CIATE	Centro Integral de Adestramento Tecno Eletrónico
CIC	Curso de Investigação Criminal
CINEL	Centro de Formação Profissional da Indústria Eletrónica, Energia, Telecomunicações da Informação
CPP	Código de Processo Penal
CTer	Comando Territorial
DC	Divisão Criminalística
DFLM	*Digital Forensic Lab Manager*
DIAP	Departamento de Investigação e Ação Penal
DIC	Direção de Investigação Criminal
DP	Destacamento de Pesquisa
EPTI	Equipas de Perícias e Tecnologias Informáticas
EUROPOL	Agência da União Europeia para a Cooperação Policial
FFSS	Forças e Serviços de Segurança
FS	Força de Segurança
GNR	Guarda Nacional Republicana
IC	Investigação Criminal
IEC	*International Electrotechnical Comission*
IPL	Instituto Politécnico de Leiria
ISO	*International Organization for Standardizaion*
LC	Lei do Cibercrime
LOGNR	Lei Orgânica da Guarda Nacional Republicana

LOIC	Lei de Organização da Investigação Criminal
LPC	Laboratório de Polícia Científica
MP	Ministério Público
n.º	número
NDF	Núcleo Digital Forense
NEP	Norma de Execução Permanente
NTP	Núcleo Técnico Pericial
OE	Objetivo Específico
OG	Objetivo Geral
OPC	Órgão de Polícia Criminal
p.	página
PD	Pergunta Derivada
PJ	Polícia Judiciária
PP	Pergunta de Partida
pp.	páginas
RCFTIA	Relatório Científico Final do Trabalho de Investigação Aplicada
RPDF	Repartição de Perícias Digitais Forenses
SIIC	Secção de Informações e Investigação Criminal
SOP	*Standard Operating Procedures*
SRPD	Secção de Recolha de Prova Digital
ss.	seguintes
SSC	Subsecção de Criminalística
SWGDE	*Scientific Working Group on Digital Evidence*
SWGIT	*Scientific Working Group on Imaging Technology*
SWOT	*Strengths, Weaknesses, Opportunities, Threats*
TIA	Trabalho de Investigação Aplicada
TRP	Tribunal da Relação do Porto
UAF	Unidade de Ação Fiscal
UFED	*Universal Forensic Extraction Device*
UPS	*Unlimited Power Source*
USB	*Universal Serial Bus*

INTRODUÇÃO

O presente Relatório Científico Final do Trabalho de Investigação Aplicada (RCFTIA), insere-se no plano curricular do Mestrado em Ciências Militares na Especialidade de Segurança na Academia Militar (AM). A investigação encontra-se subordinada ao tema: Núcleo Digital Forense da Guarda Nacional Republicana e tem como finalidade analisar a atividade das equipas de Investigação Criminal (IC) da Guarda Nacional Republicana (GNR) e apurar as suas capacidades no manuseamento da prova em suporte eletrónico (doravante também designada prova digital).

Com a globalização e os avanços tecnológicos das últimas décadas, a maior parte da população mundial tem na sua posse um ou mais dispositivos eletrónicos que permitem aceder a todo o tipo de produtos e serviços disponibilizados nos mais diversos pontos do globo. Este fenómeno tem aproximado o cidadão comum do resto do mundo, estreitando distâncias, facilitando o acesso a conteúdos e impulsionando muitas áreas da economia. No entanto, o uso das tecnologias de informação e comunicação oferece igualmente muitos riscos para os seus utilizadores, apresentando-se como um campo de oportunidades para uma miríade de atividades criminosas. A expansão das tecnologias "serve de veículo a um novo tipo de criminalidade imaterial, transfronteiriça e complexa" (Cancela, 2016, p. 10). Associado a este uso crescente de dispositivos eletrónicos surge, assim, o aumento dos índices da prática de ilícitos criminais cuja investigação incide sobre esses dispositivos eletrónicos enquanto fonte de vestígios que possam servir de prova. Percebe-se, pois, que:

> "as novas formas de criminalidade ligadas aos meios tecnológicos destacam-se não porque consistem em condutas substancialmente diferentes daquelas que tradicionalmente preenchem os tipos legais de crime correspondentes, mas porque, e apenas, os instrumentos (os equipamentos eletrónicos e as técnicas informáticas) utilizados na prática das infrações criminosas são diversos dos tradicionalmente previstos pelo legislador penal" (Santos, 2005, p. 24).

Desta forma, com o avançar dos desenvolvimentos da tecnologia e dos instrumentos técnicos usados para cometer os ilícitos, as instituições com competência para investigar esses ilícitos ao manterem o seu "*status quo* dos seus instrumentos de investigação, estas podem revelar-se obsoletas face à constante inovação da contraparte, quando confrontadas por obstáculos processuais na proteção dos deveres fundamentais" (Cancela, 2016, p. 20). Esta realidade traz novos desafios não só no âmbito da cibersegurança, mas também no que concerne aos procedimentos da IC, face ao emergir de um novo tipo de prova: a prova digital.

Assim, sendo esta uma área bastante atual e ainda em crescimento, requer por parte das instituições, incluindo a GNR, uma incessante adaptação e atualização de forma a, não apenas estar atenta às atividades criminais que possam crescer ou aparecer no ambiente digital, como também desenvolver conhecimentos, técnicas e práticas comuns na área da prova digital que possam dar uma resposta cabal às novas necessidades de investigação deste tipo de atividades. Sendo a GNR um Órgão de Polícia Criminal (OPC) com competências em matérias de IC, o tema em causa assume-se relevante, não só pelo facto de o Núcleo Digital Forense (NDF) ser uma valência relativamente recente da GNR, mas também pelo facto de a prova digital assumir uma importância crescente. A prova deixou de ser unicamente física, passando também a ser digital. A importância da presente investigação, prende-se intimamente com a necessidade de analisar a preparação das Forças e Serviços de Segurança (FFSS) e, em particular, da GNR, que se constitui como uma Força de Segurança (FS), para fazer face a este novo fenómeno.

Como objetivo geral (OG) da investigação, pretende-se analisar as capacidades dos militares pertencentes a qualquer NDF da GNR no âmbito do tratamento da prova digital. Considerando que a pergunta de partida (PP) "se constitui como um farol que orienta todo o estudo do investigador e que está obviamente perfilado com os objetivos gerais da investigação" (Rosado, 2017, p. 122), foi formulada a seguinte PP: "*Quais as capacidades dos militares dos Núcleos Digitais Forenses da Guarda Nacional Republicana no âmbito do tratamento da prova digital*?".

Já no que diz respeito à sequência do presente trabalho, este encontra-se estruturado pela seguinte forma: após uma breve introdução, onde é explicado o âmbito e a pertinência do tema, bem como o OG e a PP, seguem-se três Capítulos. O Capítulo 1 – Enquadramento Teórico, no qual são expostos os conceitos e temáticas relacionados com o tema; Capítulo 2 – Metodologia, Métodos e Materiais, no qual são enunciadas as etapas efetuadas pelo autor; Capítulo 3 – Resultados, com o objetivo de ser demonstrado todo o trabalho de campo efetuado, nomeadamente, a apresentação dos resultados da análise documental, das entrevistas e dos questionários. O trabalho termina com as Conclusões que, tal como o nome indica, contém as conclusões que se puderam retirar da realização da investigação e onde irão ser dadas respostas às questões de investigação levantadas na Introdução. Os restantes pontos do trabalho dedicam-se à exposição de informações complementares, como as Referências Bibliográficas, onde serão apresentadas todas as obras e fontes de informação que serviram de apoio e de base para a realização do presente RCFTIA.

CAPÍTULO 1. ENQUADRAMENTO TEÓRICO

O presente capítulo visa criar uma base teórica organizada que reúna os principais conceitos necessários para a compreensão do tema da presente investigação.

Numa primeira fase, será abordado sucintamente o princípio de Locard.

Numa segunda fase, serão abordados alguns aspetos da IC na GNR, nomeadamente o seu enquadramento no ordenamento jurídico português, a competência da GNR nessa matéria, as atividades de IC desenvolvidas pela GNR, o seu órgão técnico, e, por fim, uma categorização, por parte de um grupo de trabalho americano, de todos os intervenientes no processo relacionado com a prova digital.

Posteriormente, dedicam-se umas páginas à prova digital, nomeadamente o seu conceito, características e o seu enquadramento legal no ordenamento jurídico português. Também serão dedicadas algumas linhas à Ciência Digital Forense.

Será ainda feita uma explanação sobre a formação que os diferentes intervenientes na prova digital devem ter, operando-se uma divisão consoante a sua função. Para finalizar, serão abordados os temas de criminalidade informática e da prova digital como prova penal.

1.1. O Princípio de Locard

Um dos princípios fundamentais da atividade forense é o Princípio da Troca de Locard. De acordo com este princípio, qualquer um ou qualquer coisa que entra num local de crime, leva consigo algo desse local e deixa alguma coisa para trás quando sai do mesmo (Kirk, 1953). No mundo virtual, este princípio ainda é válido, ou seja, onde quer que o intruso vá, deixa rasto (neste caso, uma pegada digital). Toda e qualquer informação digital capaz de determinar que houve uma intrusão ou que forneça alguma ligação entre o invasor e a vítima, ou entre a invasão e o atacante, poderá ser considerada como uma evidência.

1.2. A Investigação Criminal na Guarda Nacional Republicana

Ao abordar a prova digital, nomeadamente no âmbito da GNR, é necessário ter em conta toda a atividade de IC. Assim, antes de especificar a organização e as competências da GNR no âmbito da IC, será de extrema importância remetermo-nos para o conceito de IC.

Este conceito vem definido no art. 1.º da Lei n.º 49/2008, de 27 de agosto (Lei de Organização da Investigação Criminal – LOIC) como "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 provas, no âmbito do processo" (Assembleia da República [AR], 2008). Assim, esta vertente da GNR tem como finalidade a recolha de elementos que possam servir de prova em sede de julgamento e que possam contribuir "para a descoberta da verdade relativamente a factos que constituam crime" (Mateus, 2016, p. 3) competindo, assim, à IC "produzir a prova, demonstrando a verdade material de factos pretéritos, penalmente relevantes" (Braz, 2017, p. 58).

No que concerne ao combate à criminalidade, a GNR possui competência não só para a prevenção como para o desenvolvimento de ações de IC que lhe sejam atribuídas, quer por lei, quer por uma Autoridade Judiciária (AJ), de acordo com o art. 3.º, n.º 1, alíneas c), e) e m) da Lei n.º 63/2008, de 18 de novembro (Lei Orgânica da GNR – LOGNR). Tal competência é atribuída à GNR por meio da LOGNR e da LOIC. Desta forma, sendo a GNR um OPC, segundo o art. 3.º, n.º 1, alínea b), da LOIC, "desenvolve um conjunto de ações que visam prevenir a criminalidade em geral e efetuar diligências necessárias tendentes a investigar a existência de um crime e proceder à recolha de prova, determinar os seus agentes, a sua responsabilidade e efetuar as consequentes detenções" (Branco, 2010, p. 246). Sendo a GNR um OPC, compete a esta coadjuvar as AJ com vista à realização das finalidades do processo segundo o art. 55.º n.º 1 do CPP.

Apesar de a GNR ser um OPC de competência genérica (art. 3.º, n.º 1, alínea b), da LOIC), ainda tem competência específica para a investigação de crimes tributários, fiscais e aduaneiros através de uma das suas Unidades Especializadas, neste caso, a Unidade de Ação Fiscal (UAF), de acordo o art. 41.º, n.º 1, da LOGNR. Desta forma, é determinado pela LOIC, no seu art. 7.º, n.º 4, alínea a), que a GNR tem competência para investigar crimes até um valor máximo de 500.000€, ainda referindo que a partir desse valor, a Polícia Judiciária (PJ) começa a ter competência para crimes tributários.

É defendido por Militão (2012, p. 262) que "a lei processual penal, deve permitir que as entidades policiais e judiciárias competentes possam desenvolver todas as ações necessárias e adequadas à obtenção de prova digital de forma agilizada, fácil, em tempo útil". Assim, aliada a esta perspetiva, deve-se combater por forma a que a IC da GNR seja "dotada de recursos humanos e meios técnicos e tecnológicos capazes de dar resposta às referidas dificuldades e complexidades. Pede-se a criação, no seio das polícias criminais, de unidades especializadas para o efeito" (Militão, 2012, p. 262).

Segundo o Despacho n.º 18/14-OG, de 11 de março, que estrutura a IC da GNR, esta consagra três atividades distintas: a operativa, a de análise de informação criminal e a criminalística, sendo que os NDF se encontram incluídos nesta última. O presente Despacho

também refere que, no que concerne à prova digital, são competências genéricas da Direção de Investigação Criminal (DIC) a recolha de prova digital e a investigação de incidentes em redes informáticas.

Tratando da formação que os diferentes intervenientes na prova digital devem ter, o *Scientific Working Group on Digital Evidence* (SWGDE) e o *Scientific Working Group on Imaging Technology* (SWGIT) identificaram e definiram quatro categorias não só para todos os que adquirem, preservam, analisam ou examinam prova digital, mas também para os que supervisionam essas funções, sendo elas (SWGDE/SWGIT, 2010):

- *First Responders*, que são os primeiros a assegurar, preservar e/ou recolher prova digital no local do crime;
- *Technician* que são aqueles com a principal responsabilidade de recolher e/ou preparar a prova digital para exames, análises e perícias;
- *Examiner/Analyst*, que são aqueles que no seu dia a dia, a realização de exames, análises e/ou recuperação de prova digital é uma constante e podem também ser responsáveis pela recolha de prova digital;
- *Manager/Commander/Supervisor*, que são os responsáveis não só pela definição das políticas da instituição à qual pertencem, mas também pelas decisões a nível orçamental. Podem também supervisionar e/ou orientar os elementos que estejam relacionados com a prova digital.

É importante mencionar como é que se enquadram os NDF neste momento no âmbito da atividade de IC da GNR. Atualmente, os NDF não se encontram ainda formalmente constituídos, a nível de orgânica. No entanto, na prática já se encontram a funcionar enquanto unidades especializadas na área de IC da GNR. No Despacho n.º 18/14-OG, de 11 de março, só está prevista a Secção de Recolha de Prova Digital (SRPD), que pertence à Repartição de Perícias Digitais Forenses (RPDF). A GNR utilizou fundos europeus para dar início à criação de uma estrutura digital forense a nível nacional, e assim, em 2018, foram formados os militares que constituem a RPDF e também os militares que, sendo especializados na área digital, foram agrupados nos designados NDF, nomeadamente os 3 militares do NDF de Coimbra, os 2 militares do NDF do Porto e os 2 militares do NDF de Faro. Esses militares dos NDF constituem formalmente as Equipas de Perícias e Tecnologias Informáticas, que fazem parte dos Núcleos Técnico Periciais (NTP), dentro da Subsecção de Criminalística (SSC). Na prática, porém, em antecipação ao que se prevê criar em breve, essas equipas são já designadas NDF. Entretanto, houve a oportunidade de dar mais formação na área da

perícia digital forense e, assim, foram formados todos os restantes militares que, à data de hoje, constituem os NDF a nível nacional. Face ao exposto, e atendendo ao facto de os "NDF" ocuparem uma posição central na investigação e serem referidos várias vezes no trabalho – no plural ou mesmo no singular, referindo-se à totalidade dos NDF, estes devem ser entendidos como as valências da prova digital forense dentro da GNR, independentemente de, neste momento, não ser essa a nomenclatura formalmente prevista.

1.3. A Prova Digital

1.3.1. Conceito

Durante a fase de inquérito, segundo o art. 262.º, n.º 1, do Código de Processo Penal (CPP), aprovado pelo Decreto-Lei n.º 78/87, de 17 de fevereiro, realiza-se um "conjunto de diligências que visam investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles e descobrir e recolher as provas, em ordem à decisão sobre a acusação" (Ministério da Justiça [MJ], 1987) durante as quais os militares da GNR podem encontrar informação relevante para os processos. Esta informação, por sua vez, pode estar contida em dispositivos eletrónicos. É de extrema importância referir que o conceito de prova digital não está presente no ordenamento jurídico português, muito embora seja próximo do conceito de dados informáticos, previsto no art. 2.º, alínea c), da Lei n.º 109/2009, de 15 de setembro, que aprovou a Lei do Cibercrime (LC). De acordo com esta definição, os dados informáticos consistem em "qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função" (Assembleia da República [AR], 2009).

Tendo este conceito como ponto de partida, é desenvolvido o conceito principal e basilar da presente investigação, ou seja, o conceito de prova digital, sendo esta definida como "toda a informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações" (Ramos, 2014, pp. 140-141). A prova digital é descrita por Rodrigues como "qualquer tipo de informação, com valor probatório, armazenada em repositórios eletrónico-digitais de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital" (2009, p. 722). Segundo Ramalho (2017, p. 102), a prova digital:

> "está hoje presente na generalidade dos processos de natureza criminal. Encontra-se em computadores, *tablets*, *smartphones*, dispositivos de armazenamento USB, câmaras fotográficas e ou de vídeo digitais, aparelhos periféricos (como leitores de cartões, impressoras ou *scanners*), gravadores de áudio, sistemas de videovigilância, consolas de videojogos, servidores, *routers*, *access points*, ou em movimento por redes de comunicações eletrónicas, entre outros locais".

A prova digital pode ser também designada por prova eletrónico-digital pois refere Rodrigues que "prova eletrónico-digital pode definir-se como qualquer tipo de informação, com valor probatório armazenada ou transmitida, sob a forma binária ou digital" (2009, p. 39), definição bastante similar ao conceito apresentado por outros autores.

Internacionalmente e mais concretamente pelo SWGDE, a prova digital pode ser caracterizada como a informação que está armazenada ou transmitida na forma binária e que tem um valor probatório (SWGDE, 2013). No entanto, de todas as definições apresentadas previamente, esta última, parece ser a mais clara e concisa, apresentada na ISO/IEC 27037 que define a prova digital como informação ou dados, armazenados ou transmitidos, na forma binária que podem ser considerados prova (*International Organization for Standardization/International Electrotechnical Comission* [ISO/IEC], 2012).

De entre os meios de prova e os seus regimes designados no CPP, os que são mais relevantes para a presente investigação são, a prova pericial (art. 151.º e ss. do CPP) e a prova documental (art. 164.º e ss. do CPP), pois a prova digital pode reconduzir-se a uma destas duas formas. Caracteriza-se então como prova pericial por esta "exigir especiais conhecimentos técnicos para a sua perceção ou apreciação dos factos" (Ramos, 2014, p. 141) e como prova documental "sempre que a mesma possa ser corporizada em escrito ou por outro meio técnico, como, por exemplo, a impressão fotográfica ou audiovisual de uma mensagem de correio eletrónico" (Ramos, 2014, p. 141).

1.3.2. Características da Prova Digital

A prova digital é classificada por Rodrigues como sendo "fragmentária, dispersa, frágil, volátil, alterável, instável, apagável e manipulável, invisível e espacialmente dispersa" (2011, p. 29). A sua apreensão torna-se mais difícil devido à "instabilidade demonstrada por esta prova, provindo da constante mutabilidade que lhe caracteriza" (Cancela, 2016, p. 22).

Tal como refere Militão (2012, p. 261) "a prova digital não é suscetível de apreensão material" logo, a prova digital "consiste (…) numa prova imaterial" (Cancela, 2016, p. 22). Adianta ainda Lessa (2009) que um documento eletrónico é meramente uma sequência de números binários, ou seja, os algarismos zero e um, que, quando reconhecidos, traduzidos e

lidos pelo computador, transformam-se em informação. Esta dificuldade de apreensão, verifica-se em situações nas quais "o investigador se depara inicialmente com uma prova com certas características, e mais tarde, esta se modifica, total ou parcialmente" (Cancela, 2016, p. 22).

Fruto de todas estas características, afirma-se então que a atuação por parte de quem trata da prova digital, neste caso, da IC da GNR deve exigir "aprofundados conhecimentos informáticos e, muitas vezes, meios técnicos e tecnológicos de ponta" (Militão, 2012, p. 261) existindo também a responsabilidade por parte desta, "a necessidade de redobrar os cuidados a tomar" (Cancela, 2016, p. 22).

1.3.3. Enquadramento legal

1.3.3.1. Lei do Cibercrime

A obtenção e tratamento da prova digital não exige do investigador apenas conhecimentos técnicos e informáticos, mas também um conhecimento sobre todas as normas processuais inerentes à prova digital, normas essas, específicas da prova digital que constam na LC, que veio transpor para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho da Europa, relativa a ataques contra sistemas de informação, entretanto revogada pela Diretiva 2013/40/EU do Parlamento Europeu e do Conselho, de 12 de agosto de 2013 adaptando assim o Direito interno à Convenção sobre Cibercrime do Conselho da Europa, de 23 de novembro de 2001, segundo o art. 1.º da LC. No que concerne às mudanças trazidas pela LC no âmbito de prova digital, importa referir que esta, segundo Militão (2012):

- não só introduziu, mas também ampliou os conceitos jurídico-informáticos que se encontram no art. 2.º;
- definiu medidas processuais no que concerne à obtenção de prova digital (presentes nos art. 12.º até art. 17.º);
- fixou medidas para entidades terceiras, nomeadamente as operadoras de comunicação, com o objetivo da preservação e apresentação de prova digital;
- definiu medidas a nível da cooperação internacional no âmbito da prova digital.

Estas normas processuais aplicam-se não só aos crimes previstos na LC, ou seja, cibercrimes, mas também a crimes cometidos através de um sistema informático ou crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, segundo o art. 11.º da LC, recolha essa que é legitimada pelo art. 15.º n.º 1, do mesmo

documento legal. Nessas recolhas ou pesquisas informáticas, segundo o art. 15.º n.º 6 "são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal" (AR, 2009). No entanto, segundo o art. 15.º n.º 5 da LC, está prevista uma extensão relativamente às pesquisas informáticas:

> "quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente" (AR, 2009).

Tal como refere Ramos (2014), nos dias de hoje, a quantidade de suportes e dispositivos eletrónicos onde é possível guardar dados informático é enorme levando assim a que se tornem cada vez mais aliados dos criminosos. É de extrema relevância ainda referir que a LC "confere um regime processual penal geral no que diz respeito à obtenção de prova digital, potencialmente dirigido a todos os tipos de crime" (Almeida, 2014, p. 37).

1.3.3.2. Código de Processo Penal

No que diz respeito ao ordenamento jurídico português, nomeadamente no CPP, a prova digital "é entendida nos art(s). 189.º e 190.º do CPP" (Almeida, 2014, p. 35). No entanto, não encontramos nestes artigos um regime relativo à prova digital, mas sim uma remissão para os arts. 187.º e 188.º do CPP. Assim, no que concerne aos meios de obtenção de prova, o CPP no seu art. 189.º, n.º 1, atribui a quaisquer "conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital" (MJ, 1987) os mesmos requisitos e pressupostos das interceções das escutas telefónicas, não havendo assim um regime legal específico para a prova digital no CPP.

Os meios de obtenção de prova referidos no CPP são os exames, revistas e buscas, apreensões e escutas telefónicas. Refere então Militão (2012, p. 266) que "os meios de obtenção da prova digital, não obstante com as adaptações necessárias, reconduzem-se aos "tradicionais" meios de obtenção de prova. Trata-se, com efeito, (…) de exames, revistas, buscas, apreensões ou interceções de comunicações".

Para se poder realizar a apreensão de dispositivos eletrónicos que possam servir de prova de um crime e caso esses dispositivos se encontrem em lugar reservado ou não livremente acessível, é ordenada uma busca para que essa pesquisa informática seja possível, segundo o art. 174.º, n.s.º 1 e 2 do CPP. Assim, conforme referido no Acórdão do Tribunal

da Relação do Porto (TRP) de 7 de julho de 2016, "a busca de onde resulte a apreensão de um computador é regulada pelas normas do Código de Processo Penal. A pesquisa dos dados informáticos, num computador, bem como a apreensão desses dados, é regulada na Lei do Cibercrime" (Tribunal da Relação do Porto [TRP], 2016).

Está consagrado no CPP, nomeadamente no art. 125.º, o princípio da liberdade da prova, sendo que este artigo refere que as provas admissíveis são aquelas que não são proibidas por lei.

1.4. Ciência Digital Forense

A Ciência Digital Forense é classificada por Ramalho (2017), como o ramo da ciência forense com enfoque na realidade digital e que abrange, em sentido amplo, as atividades de identificação, recolha e análise da prova digital. Esta é também conceptualizada por Rodrigues que afirma que tem o objetivo de "orientar a investigação criminal, em matéria de criminalidade informático-digital, para a preservação, recolha, gravação, validação, identificação, análise, interpretação, documentação e apresentação deste específico tipo de prova" (2011, p. 31).

1.5. Formação no âmbito da Prova Digital

Todos aqueles que preservam, analisam e/ou examinam prova digital, ou ainda que supervisionam estas atividades devem estar cientes das capacidades e das limitações de cada tecnologia diferente. Estes, devem estar cientes também, dos procedimentos que são utilizados no meio da atividade forense e de novos desenvolvimentos que possam ocorrer.

Por forma a cumprir estes objetivos, o SWGDE/SWGIT (2010) definiu as seguintes recomendações:

- definição e utilização de programas fiáveis que garantam a implementação de procedimentos válidos;
- manutenção da proficiência ao estar de forma contínua em cursos e formações relacionados com tecnologias de prova digital;
- consciencialização dos novos desenvolvimentos jurídicos relacionados com prova digital;
- consciencialização dos novos avanços tecnológicos;
- implementação de programas de avaliação contínua às capacidades técnicas de todos aqueles que trabalham com prova digital.

1.5.1. Categorias de Formação

O SWGDE/SWGIT (2010) definiu um conjunto de categorias que devem ser tidas em conta aquando da formação na área da prova digital, sendo elas as seguintes:

- consciencialização – treino desenvolvido para fornecer ao formando, um conhecimento geral da prova digital (por exemplo, análise de vídeo, áudio forense, análise de imagem e computação forense), incluindo também noções gerais de capacidades e limitações quer de *hardware* como de *software*;
- habilidades e técnicas – treino desenvolvido com o objetivo de fornecer ao formando a capacidade de usar ferramentas e procedimentos específicos com o máximo de competência;
- conhecimento de procedimentos – treino desenvolvido para fornecer ao formando uma compreensão dos procedimentos da prova digital e como aplicar essa compreensão em várias situações;
- desenvolvimento de habilidades para processos judiciais – dividida em duas subcategorias sendo a primeira o testemunho de perito, que tem o objetivo de criar no formando a habilidade de apresentar em tribunal um testemunho, no âmbito da prova digital, claro e não técnico, mas baseado em provas. A segunda subcategoria está relacionada com a preparação de resultados forenses, que tem o objetivo de capacitar o formando a preparar documentação precisa e confiável e/ou recursos visuais (por exemplo, notas, relatórios, impressões, gravações de áudio);
- formação contínua – fornecer ao formando a capacidade de obter o conhecimento da tecnologia em evolução no âmbito da prova digital;
- aplicações e tecnologias especializadas – treino em áreas especializadas (por exemplo, telemóveis, comparação de imagens, autenticação de áudio, otimização de vídeo).

1.5.2. Formação consoante a função

Conforme já indicado foram identificadas as quatros categorias dos que trabalham com prova digital, sendo elas: *First Responders*, *Technician*, *Examiner/Analyst* e *Manager/Commanders/Supervisors*.

Os seguintes quatro subcapítulos irão explanar áreas específicas nas quais os agentes que trabalham com prova digital devem receber formação com o intuito de potenciar as suas funções neste âmbito, segundo o SWGDE/SWGIT (2010).

1.5.2.1. *First Responders*

Todos os *First Responders* devem ser capazes de reconhecer a presença de outras formas de prova física não relacionadas com a prova digital, como as impressões digitais ou outros tipos de provas biológicas num local de crime. Devem também ter formação em áreas como: procedimentos de segurança e proteção, saber com quem entrar em contacto caso necessite de suporte técnico, técnicas de recolha e preservação adequadas, criação e manutenção da cadeia de custódia da prova, fazer uso dos *Standard Operating Procedures* (SOP), demonstração de competência (através de exames escritos ou práticos), questões éticas e legais, princípios e práticas forenses gerais e capacidade de documentação e redação técnica.

1.5.2.2. *Technician*

Tal como os *First Responders*, também os *Technician* devem ser capazes de reconhecer a presença de outras formas de prova física não relacionadas com a prova digital, como as impressões digitais ou outros tipos de provas biológicas num local de crime. Devem também ter formação em áreas como: procedimentos de segurança e proteção, saber com quem entrar em contacto caso necessite de suporte técnico, identificação de prova digital, atualização no que concerne às novas tecnologias relacionadas com a prova digital (*software* e *hardware*), manuseamento da prova por forma a preservar a sua integridade, uso de ferramentas para aquisição de prova digital (*software* e *hardware*), manutenção da cadeia de custódia da prova, fazer uso dos SOP, demonstração de competência (através de exames escritos ou práticos), questões éticas e legais, princípios e práticas forenses gerais, garantia de qualidade (agir de acordo com as práticas comuns da comunidade forense) e capacidade de documentação e redação técnica.

1.5.2.3. *Examiner/Analyst*

Tal como os *First Responders* e *Technician*, também os *Examiner/Analyst* devem ser capazes de reconhecer a presença de outras formas de prova física não relacionadas com a prova digital, como as impressões digitais ou outros tipos de provas biológicas num local de crime. Devem também compreender o procedimento adotado pela sua instituição no caso de se ter de lidar com prova física.

Estes especialistas devem ter formação em agentes patogénicos que se podem transmitir através do sangue, incêndios e problemas elétricos e produtos contaminantes.

No que respeita à manutenção da integridade dos dados, que se apresenta como algo essencial para a preservação da prova, estes especialistas asseguram o princípio de que preferencialmente, se deverá evitar a modificação dos dados, muito embora, algumas alterações possam vir a demonstrar-se necessárias. A ter lugar, as modificações devem ser técnica e cientificamente corretas e devidamente registadas e documentadas.

Estes especialistas devem ainda ter formação em áreas como ética, princípios e práticas gerais forenses, manuseamento de prova e cadeia de custódia, capacidades de testemunho em tribunal, regime legal relacionado com estas matérias, garantia da qualidade (o que implica agirem de acordo com as práticas comuns da comunidade forense), gestão básica do local do crime (o que exige que compreendam a sua complexidade e a da prova), devendo ainda demonstrar capacidades de redação técnica, e de aplicar, em cada momento, as melhores práticas (por exemplo: procedimentos técnicos), bem como fazer uso dos SOP.

Quanto à computação forense, a formação destes intervenientes deve-se focar em aspetos das estruturas e sistemas de arquivo e da programação de computadores.

Relativamente a fundações técnicas, devem ter formação em: tecnologia de interface de dados e fundamentos do sistema operacional nomeadamente a sua instalação, configuração, atualização e diagnóstico de solução de problemas.

No que concerne ao equipamento, abordagem dos seguintes temas: manutenção preventiva do computador, segurança e questões ambientais; *motherboards*, processadores, dispositivos de memória, etc; dispositivos internos e externos; duplicadores; e bloqueadores de escrita.

No que diz respeito à temática do *networking*, a formação destes intervenientes deverá abordar os seguintes tópicos: topologia de rede, sistemas operacionais de rede, segurança de rede, infraestrutura e protocolos de *internet* e dispositivos de *hardware* específicos de rede.

Formação a nível de *software* em: identificação de arquivos, programas forenses e não forenses, sistemas operacionais e reconhecimento de *malware*.

Por fim, e em relação à temática do armazenamento, deverão ser abordadas as seguintes vertentes do mesmo: lógico, físico, tipos de média, em rede e remoto (sem fios).

1.5.2.4. *Manager/Commanders/Supervisors*

Estes intervenientes a nível do estado da tecnologia relativa à prova digital, deverão ter formação em: questões jurídicas; tendências de indústria, do mercado e do utilizador para

novas tecnologias; fonte de prova digital na atividade criminosa; e comparações atuais de custo do ciclo de vida e das limitações de *software* e de *hardware*.

Quanto à descrição das principais tecnologias, na sua formação, devem ser abordados os seguintes pontos: ciência forense básica; tecnologia básica relacionada com a prova digital; pontos fortes e limitações em processos forenses; e pontos fortes e limitações das ferramentas forenses digitais (*software* e *hardware*).

A nível de gestão de pessoal deverá ter formação que o capacite com os seguintes tópicos: pontos fortes e limitações das capacidades do seu pessoal; competência e formação contínua no âmbito da tecnologia da prova digital; *stress* psicológico; e capacidade de gerir tanto o seu tempo como o seu pessoal.

No que concerne à temática das alternativas estratégicas deverá: saber quem contactar quando necessita de suporte técnico e estar ciente das atuais referências e fontes de informação relativas à prova digital.

1.6. Criminalidade Informática

A criminalidade informática pode ser conceptualizada num sentido amplo e num sentido restrito, entre vários outros possíveis. Em sentido amplo, a criminalidade informática "englobará toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais do que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios" (Venâncio, 2011, p. 17). Já em sentido restrito, apenas "abarcará aqueles crimes em que o elemento digital surge como parte integrador do tipo legal ou mesmo como seu objeto de proteção" (Venâncio, 2011, p. 17).

1.7. A Prova Digital como Prova Penal

É defendido por Mendes (2014) que a prova pode ser definida segundo duas perspetivas – enquanto atividade probatória e enquanto resultado de atividade probatória. Assim, enquanto atividade probatória, a prova é "o método através do qual são demonstrados os factos relevantes para a existência do crime, a punibilidade do arguido e a determinação da pena ou medida de segurança aplicáveis" (Mendes, 2014, p. 173). Por outro lado, enquanto resultado da atividade probatória, a prova é definida como "a motivação da convicção da entidade decisora acerca da ocorrência dos factos relevantes, contanto que essa motivação se conforme com os elementos adquiridos representativamente no processo e

respeite as regras da experiência, as leis científicas e os princípios da lógica" (Mendes, 2014, p. 173).

Existe uma necessária adaptação do ordenamento jurídico no que concerne à matéria da prova digital pois:

> "a evolução da criminalidade e o constante perfeccionismo técnico dos agentes criminais leva à necessidade de dar relevância no ordenamento jurídico à figura da prova digital, enquanto instrumento fundamental ao bom curso da investigação e de apresentação em julgamento, garantindo que a cadeia de custódia foi cumprida e que esta prova mantém a sua força probatória inicial" (Cancela, 2016, p. 19).

Por forma a que a prova digital mantenha a sua integridade, o investigador "deverá identificar, de forma ainda mais rigorosa, qual o tipo de prova digital em causa. Apenas com essa identificação, poderá o investigador garantir a força probatória da prova digital, sem perigo de esta ser alterada ou desaparecer" (Cancela, 2016, p. 22). Refere ainda Cancela (2016) que à prova digital deverá estar associado um princípio de não alteração da prova no ato de recolha, ou seja, é exigido que "durante o decurso da investigação, o investigador digital exclua da sua conduta qualquer atuação que contamine os dados obtidos com elementos alheios ao sistema ou rede informáticos investigados" (Rodrigues, 2011, p. 726). Assim, existe uma necessidade de especialização no âmbito da prova digital para que esta possa ser admitida como prova em sede de inquérito pois o "acesso, recolha, conservação e análise estarão na esfera de competência de pessoal especializado, que, dotados de conhecimentos técnicos, impedem o corrompimento ou o deficiente manuseamento da prova, e a sua posterior inadmissibilidade" (Cancela, 2016, p. 23). Assim, um dos fatores que pode influenciar a validade da prova digital em sede de inquérito é a atuação do militar da GNR que trabalha neste âmbito, pois esta, "tem de reter o seu valor probatório, para que este seja suscetível de ser valorado pelo julgador" (Almeida, 2014, p. 27).

De todas as classificações explanadas pelo CPP, a prova digital deve-se incluir:

> "na prova pericial (por exigir conhecimentos técnicos qualificados de quem a recolhe), (…) também poderá ser classificada enquanto prova documental (na medida em que "possa ser corporizada em escrito ou por outro meio técnico, como, por exemplo, a impressão fotográfica ou audiovisual de uma mensagem de correio eletrónico")" (Ramos, 2014, p. 76).

Para que a cadeia de custódia da prova seja corretamente executada, Cancela (2016) defende três princípios:

- o da garantia de documentação em todas as fases processuais relativas à prova digital, ou seja, acesso, recolha, armazenamento, transferência, preservação e apresentação ou repetição da prova digital;

- o da responsabilidade pessoal, ou seja, todos aqueles que intervirem na investigação forense digital, são responsáveis por manter e controlar a cadeia de custódia da prova com o objetivo de garantir a força probatória dessa mesma prova. Este princípio também define que terceiros à investigação ficam excluídos do acesso a quaisquer fontes de prova digital levando a que cada prova no âmbito da prova digital seja apenas recolhida, manuseada, analisada e fundamentada por peritos ou conjunto de peritos da área da prova digital;
- o da responsabilização repartida dos vários intervenientes na produção da prova respeitantes dos princípios forenses digitais ou seja:

> "caberá a cada agência ou perito a responsabilidade por recolher, aceder, armazenar e transferir a prova sob a sua alçada investigativa. Estando os técnicos e os organismos intervenientes na investigação obrigados a respeitar os princípios relativos à produção e análise forense, assegura-se, de forma complementar e cumulativa, o valor probatório e a integridade da prova objeto da investigação forense digital" (Cancela, 2016, p. 24).

Assim, para garantir a cadeia de custódia da prova digital e a sua validade em sede de inquérito "as fases processuais da prova deverão ser regidas por regras de cumprimento imperativo. Para tal, releva (…) a documentação de qualquer operação efetuada e a intervenção no processo de peritos tecnicamente aptos para garantir admissão da prova" (Cancela, 2016, pp. 24-25).

CAPÍTULO 2. METODOLOGIA, MÉTODOS E MATERIAIS

No presente capítulo irá ser abordada a metodologia adotada para a realização da investigação. Esta consistiu num raciocínio dedutivo e numa abordagem mista, ou seja, tanto qualitativa como quantitativa, tendo em conta a natureza investigacional do tema tratado na mesma. É abordado o modelo de análise, que é constituído pelos objetivos geral e específicos, aos quais correspondem a pergunta de partida e as perguntas derivadas, respetivamente. O presente capítulo também refere as técnicas de recolha de dados, questões relacionadas com a amostra tanto dos inquéritos por entrevista como dos inquéritos por questionário, as técnicas de tratamento e análise de dados e, por fim, uma caracterização do contexto de observação.

Durante uma investigação, a metodologia aplicada na mesma 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).

A problemática do presente RCFTIA centra-se na prova digital, mais concretamente nos NDF.

O presente RCFTIA encontra-se redigido e articulado de acordo com as indicações determinadas pela AM, mais precisamente pela Norma de Execução Permanente (NEP) 520/4.ª referente ao Trabalho de Investigação Aplicada (TIA) e pela NEP 522/1.ª referente às Normas para a Redação de Trabalhos de Investigação.

2.1. Modelo de Análise

Com o objetivo de não só estruturar a investigação, mas também de permitir a materialização do método científico e do tipo de abordagem, foi necessário seguir as linhas orientadoras de um modelo de análise (ver Apêndice A) que oriente a investigação, modelo esse que é caracterizado 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" (Quivy & Campenhoudt, 2008, p. 150).

Tal como já foi anteriormente referido no Capítulo da Introdução, a presente investigação tem como objetivo geral (OG), analisar a capacidade de resposta dos militares pertencentes a qualquer Núcleo Digital Forense (NDF) da GNR no âmbito do tratamento da

prova digital. Sendo assim, por forma a cumprir este objetivo, foi formulada a seguinte pergunta de partida (PP): "*Quais as capacidades dos militares dos Núcleos Digitais Forenses da Guarda Nacional Republicana no âmbito do tratamento da prova digital?*".

Como objetivos específicos (OE), pretende-se analisar se a formação que os militares constituintes dos NDF receberam é adequada à sua função e se estes possuem os conhecimentos adequados para que possam realizar um bom trabalho; analisar se os NDF se encontram munidos com os recursos tecnológicos (*hardware* e *software*) e humanos (quer em quantidade, quer em qualidade) necessários para o tratamento da prova digital; determinar o tempo das pendências, ou seja, o tempo que demoram a ser realizados os diversos exames à prova digital; perceber se os militares são ouvidos durante o processo em tribunal e se sim, se são ouvidos como testemunhas ou como peritos. Assim, para que seja possível cumprir estes objetivos e apoiar a PP, foram formuladas as seguintes Perguntas Derivadas (PD):

- PD1: "*A formação dos militares que integram os NDF em matéria de prova digital é adequada à sua função?;*
- PD2: "*Os recursos tecnológicos e humanos que os NDF têm ao seu dispor são adequados para o bom cumprimento da sua missão?*";
- PD3: "*Qual o tempo das pendências nos diferentes NDF?*";
- PD4: "*Qual o valor da prova digital como meio de prova?"*;
- PD5: "*São os militares ouvidos durante o processo em tribunal? Como testemunhas ou como peritos?*".

O desenvolvimento principal da presente investigação centra-se no Capítulo 3 onde é feita a análise de todos os dados fornecidos pela DIC e dos dados obtidos através dos inquéritos por questionário e dos inquéritos por entrevista e onde também é feita uma comparação entre ambos.

Nas conclusões é retomado o tema central da investigação, referindo-se os principais aspetos abordados ao longo da investigação e apresentando-se as principais conclusões obtidas através dessa investigação.

Por fim, nas recomendações, são referidas as limitações do trabalho, as dificuldades encontradas durante o processo de investigação e são feitas recomendações para investigações futuras.

2.2. Metodologia e tipos de abordagem

O tema da prova digital tem sido alvo de vários estudos e o tema central de várias obras. No entanto, o tema da presente investigação não se centra essencialmente na prova digital *per si*, mas sim na prova digital dentro da GNR.

Desta forma, para que se pudesse alcançar os objetivos da investigação, seguiu-se o método dedutivo, caracterizado como sendo um método que "parte do geral, e a seguir desce ao particular" (Prodanov & Freitas, 2013, p. 27).

Por outro lado, esta investigação segue tanto uma abordagem qualitativa como uma abordagem quantitativa. A abordagem qualitativa pretende "descobrir, explorar, descrever fenómenos e compreender a sua essência" (Fortin, 2009, p. 32) e tem como objetivo "descrever ou interpretar, mais do que avaliar (…) é uma extensão da capacidade do investigador em dar um sentido ao fenómeno" (Freixo, 2012, p. 173). Por outro lado, a abordagem quantitativa define-se como um "processo sistemático de colheita de dados observáveis e quantificáveis" (Fortin, 2009, p. 22).

2.3. Métodos e Técnicas de Recolha de Dados

A recolha de dados da presente investigação encontra-se apoiada em análise documental, em inquéritos por entrevista e em inquéritos por questionário, pois tal como refere Sarmento (2013, p. 27) "para que a informação recolhida no universo informacional seja fiável e os resultados da investigação sejam válidos, os instrumentos e métodos científicos utilizados, devem ser apropriados".

Já em relação aos instrumentos utilizados, a presente investigação pode ser classificada como mista, visto que utiliza informação quantitativa decorrente da análise documental efetuada pelo autor e informação qualitativa decorrente dos inquéritos por entrevista e dos inquéritos por questionário (Sarmento, 2013).

2.3.1 Análise Documental

A análise documental da presente investigação pode-se dividir em duas fases. Numa primeira fase, foi realizada uma análise documental, recorrendo a bibliografia escrita, bases de dados *online*, repositórios de Universidades, motores de busca e bibliotecas digitais, aquando da elaboração do Capítulo 1 da presente investigação, ou seja, numa fase onde a conceptualização de determinados temas e conceitos se mostrou essencial para que se pudesse, numa fase seguinte, proceder ao trabalho de campo, no qual também foi realizada

uma análise documental, nomeadamente no que concerne aos pedidos de informação realizados à Direção de Investigação Criminal (DIC) da GNR.

Numa primeira fase, procedeu-se à recolha do máximo de informação e bibliografia sobre a IC na GNR, prova digital, ciência digital forense, informações a nível internacional sobre formação dos intervenientes no âmbito da prova digital, criminalidade informática e por fim prova digital como prova penal.

Seguidamente, foi solicitado à DIC a cedência de informações relativas à atividade digital forense nacional realizada pela GNR nos anos de 2018, 2019 e 2020. Informações essas que foram obtidas através da *Digital Forensic Lab Manager* (DFLM) e dos Mapas Anuais da Digital Forense dos anos de 2018, 2019 e 2020. O conteúdo dessas informações (relativas aos anos de 2018, 2019 e 2020) consiste no tipo de equipamentos analisados, o tipo de crime associado a cada processo, o número de solicitações (casos ou processo) de cada Unidade da GNR, o número de solicitações (casos ou processo) de cada NDF, o tempo de execução de exame consoante o tipo de equipamento e por NDF, o número de militares por NDF e quais os Comandos da GNR que não têm NDF na sua estrutura de IC.

Relativamente ao número de solicitações (casos ou processo), não só de cada Unidade da GNR, mas também de cada NDF, é necessário ter em conta os seguintes aspetos: a UAF só começou a comunicar os seus registos a partir do ano de 2020; os NDF do Porto e de Faro só começaram a trabalhar em pleno no ano de 2019; os NDF de Beja, Braga, Castelo Branco, Leiria, Portalegre, Santarém, Setúbal, Viana do Castelo, Vila Real e Viseu só começaram a trabalhar em pleno no ano de 2020; e a estrutura de IC dos Comandos dos Açores, Aveiro, Bragança, Évora, Guarda, Lisboa e Madeira não conta com a constituição de um NDF.

Estas informações fornecidas pela DIC são de elevada importância para a presente investigação pois a sua análise e tratamento constituiu-se não só como o ponto inicial de todo o trabalho de campo, mas também como informação crucial para o bom desenrolar e coerência da investigação.

2.3.2. Inquérito por Questionário

O inquérito pode ser definido como "um conjunto de perguntas (designado por questionário), que são respondidas obrigatoriamente por escrito" (Sarmento, 2013, p. 30). Assim, este instrumento de investigação "permite conhecer e aprofundar o conhecimento através das opiniões de vários indivíduos, de uma forma incisiva" (Sarmento, 2013, p. 28).

Quanto ao processo de elaboração dos inquéritos por questionário, foram seguidas indicações definidas por Marconi e Lakatos (2003), nomeadamente a elaboração de um questionário inicial aquando da construção do inquérito, que foi revisto e alterado pela Orientadora da presente investigação.

Os questionários foram divulgados para todos os 24 militares dos NDF, só tendo sido obtidas 22 respostas, através da DIC e tinham o objetivo de recolher informações relevantes para a presente investigação por parte de quem trabalha no terreno. O questionário, que pode ser consultado no Apêndice B, encontra-se dividido em 7 partes. A primeira parte tinha o intuito de fazer uma caracterização sociodemográfica, para que se pudesse fazer uma caracterização da amostra usada no questionário. Na segunda parte abordou-se o tema da formação dos militares. A terceira parte tratou de perceber a posição dos militares em relação aos recursos tecnológicos e humanos dos NDF. Na quarta parte tentou-se perceber se o trabalho dos militares ao nível da prova digital era valorado ou não. A quinta parte tinha o objetivo de perceber se, quando os militares se dirigem a tribunal para prestar esclarecimentos, vão na qualidade de testemunha ou na qualidade de perito. Na sexta parte procurou-se perceber um pouco do que era o trabalho realizado pelos militares dos NDF, por forma a que se pudessem chegar a algumas conclusões relativamente às dificuldades que os mesmos sentem na execução desse trabalho. A sétima e última parte foi destinada a uma pergunta aberta, permitindo que os militares teçam um breve comentário sobre algo que não tenha sido abordado ao longo do questionário. Os questionários foram respondidos através do *Google Forms* entre as 10 horas do dia 01/03/2021 e as 23 horas do dia 17/03/2021. A análise aos mesmos foi efetuada com recurso também ao *Google Forms*.

2.3.2.1. Caracterização da Amostra

Os inquéritos por questionário numa amostra de 22 militares, correspondente a 91,6%, num total de 24 militares. No que diz respeito à caracterização sociodemográfica da amostra, na totalidade dos 22 inquiridos apresentam-se os seguintes dados:

- uma média de 41,59 anos de idade, tendo o mais novo 33 anos de idade e o mais velho 50 anos de idade;
- 22 elementos do género masculino;
- quanto ao grau de escolaridade, 1 militar (4,5%) tem o 11.º ano, 17 militares (77,3%) têm o 12.º ano, 1 militar (4,5%) encontra-se a frequentar o ensino superior e 3 militares (13,6%) são licenciados;

- quanto ao posto, 7 militares (31,8%) são Guardas Principais, 3 militares (13,6%) são Cabos, 10 militares (45,5%) são Cabos de Curso, 1 militar (4,5%) é Primeiro-Sargento e 1 militar (4,5%) é Sargento-Chefe;
- uma média de 8,41 anos de experiência na estrutura de IC, sendo que o militar com menos tempo de IC tem 2 anos e o militar com mais tempo de IC tem 21 anos.

2.3.3. Inquérito por Entrevista

A entrevista constitui-se como um instrumento que permite ao autor "explorar um domínio e aprofundar o seu conhecimento através da inquirição presencial a um ou mais indivíduos" (Sarmento, 2013, p. 28) e que está organizada num "conjunto de perguntas (designado por guião), que são respondidas necessariamente por via oral" (Sarmento, 2013, p. 30). A sua importância revela-se pelo facto de, com a realização de entrevistas, ser possível percecionar certos aspetos de um determinado tema que não se encontram versados em quaisquer tipo de obras literárias e oferecem ainda a oportunidade ao investigador de "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" (Sarmento, 2013, p. 31).

Foram realizadas entrevistas, com o principal objetivo de perceber a importância da prova digital na fase de inquérito de um processo, o contributo da GNR em matéria de prova digital, potenciais vulnerabilidades que o dispositivo da GNR possa ter e a formação dada aos militares para que possam desempenhar funções num NDF. Tendo em conta que compete ao Ministério Público (MP) dirigir o inquérito segundo o art. 53.º n.º 2 alínea b) do CPP e que compete aos OPC coadjuvar as AJ tais como o MP com vista à realização das finalidades do processo segundo o art. 55.º n.º 1 do CPP, pode-se dizer que existe um trabalho conjunto entre ambos. Atendendo ao exposto, foram então realizadas entrevistas não só a Oficiais da GNR, nomeadamente a Comandantes das SIIC, mas também a Procuradores do MP, por forma a ser possível obter contributos da GNR e do MP.

Para a realização das entrevistas, foram elaborados 3 guiões de entrevistas distintos, sendo que o primeiro se destinava aos Chefes de SIIC que têm na sua dependência um NDF (ver Apêndice D); o segundo aos Chefes de SIIC que não têm na sua dependência um NDF (ver Apêndice E); e o terceiro aos Procuradores do MP (ver Apêndice F).

Na preparação das entrevistas, foram seguidas as indicações definidas por Marconi e Lakatos (2003), nomeadamente a elaboração de 3 guiões iniciais aquando da construção das entrevistas, que foram devidamente revistos e alterados pela Orientadora da presente investigação.

Os entrevistados receberam, dias antes da realização da entrevista, o respetivo guião, acompanhado de uma Carta de Apresentação e da Declaração de Consentimento (Apêndices C e G, respetivamente).

2.3.3.1. Caracterização da Amostra

Tendo em conta as entrevistas que foram realizadas e que "o universo ou população é o conjunto de indivíduos (…) com uma ou mais características comuns, que se pretende analisar ou inferir" (Sarmento, 2013, p. 71), pode-se afirmar que a presente investigação conta com apenas uma população, ou seja, a dos magistrados do MP e dos Oficiais da GNR, nomeadamente aqueles que estão inseridos na estrutura de IC.

A amostra é definida como um "conjunto de elementos retirados da população, que é representativo e significativo desta população" (Sarmento, 2013, p. 71). Assim, da parte do MP, foram entrevistados dois procuradores que já tiveram contacto com a matéria da prova digital em sede de inquérito e da parte da GNR, foram entrevistados os Comandantes das SIIC, não só os que dispõem de NDF mas também aqueles que não dispõem de NDF. Apresenta-se então no Quadro n.º 1 a amostra da população que foi entrevistada.

Quadro 1 - Caracterização dos Entrevistados

Entrevistados		Função	Data	Local
E1	Capitão Joana Raquel da Silva Lourenço	Chefe da SIIC do CTer Coimbra	23/03/2021	*Microsoft Teams*
E2	Tenente-Coronel Paulo Joaquim Babo Nogueira	Chefe da SIIC do CTer Porto	24/03/2021	*Microsoft Teams*
E3	Major Pedro Miguel Afonso dos Reis	Chefe da SIIC do CTer Aveiro	26/03/2021	*Microsoft Teams*
E4	Major Carlos Manuel Neves Bengala	Chefe da SIIC do CTer Faro	26/03/2021	*Microsoft Teams*
E5	Capitão Hugo de Albuquerque Neves Campos	Chefe da SIIC do CTer Viseu	28/03/2021	*Microsoft Teams*
E6	Capitão Pedro Manuel Neto Pino	Chefe da SIIC do CTer Bragança	30/03/2021	*Microsoft Teams*
E7	Dr. Rogério Gomes Osório	Procurador da República Dirigente da Comarca do Porto Este e Ponto de Contacto da Rede	29/03/2021	*Zoom*

		Nacional de Cibercrime		
E8	Dr. Zélia Maria Almeida Marques	Procuradora da República da 1.ª Secção do DIAP de Viseu	09/04/2021	*Zoom*

Fonte: Elaboração Própria

Tendo em conta que a amostra acima mencionada conta com magistrados do MP e com Oficiais da GNR da estrutura de IC, foi possível obter então contributos de dois pontos de vista levando a um enriquecimento das conclusões tiradas pela ressente investigação.

2.4. Técnicas de tratamento e análise de dados

2.4.1. Inquérito por questionário

As técnicas empregues na redação e posterior avaliação das respostas dos inquiridos visou compreender as perspetivas que os mesmos tinham, tendo em conta que os inquiridos são quem trabalha diariamente na temática da prova digital.

A técnica mais utilizada neste inquérito por questionário foi a Escala de Likter, que tem como objetivo tirar conclusões sobre o grau de concordância acerca das questões abordadas no mesmo. Esta Escala de Likter vai de um nível 1 correspondente a uma opinião de discordo totalmente a um nível 5, correspondente a uma opinião de concordo totalmente, passando pelos níveis 2, 3 e 4 aos quais correspondem as opiniões de discordo, nem concordo nem discordo e concordo, respetivamente.

O questionário foi realizado numa plataforma *online*, nomeadamente no *Google Forms*, com o objetivo de poder abranger o máximo de militares que prestam serviço nos NDF num curto espaço de tempo, com a vantagem de as suas respostas serem guardadas numa base de dados, facilitando assim a sua posterior consulta e tratamento da informação.

Os resultados dos inquéritos por questionário encontram-se no capítulo seguinte da presente investigação.

2.4.2. Inquérito por entrevista

De acordo com Guerra (2006), as entrevistas devem ser gravadas e acompanhadas de notas tomadas pelo investigador e afirma que a transcrição das mesmas é aconselhável, dependendo do tempo disponível. Assim, e tendo em conta que as entrevistas foram

realizadas via plataformas *Microsoft Teams* ou *Zoom*, as mesmas foram gravadas e posteriormente transcritas integralmente pelo autor.

A análise de conteúdo feita a cada uma das entrevistas visou identificar as ideias-chave das respostas dos entrevistados sendo que esta análise pode-se caracterizar como "sínteses dos discursos que contêm a mensagem essencial da entrevista e são fiéis, inclusive na linguagem, ao que disseram os entrevistados" (Guerra, 2006, p. 73).

Os resultados dos inquéritos por entrevista encontram-se no capítulo seguinte da presente investigação.

2.5. Caracterização do contexto de observação

Relativamente aos questionários e tal como já foi referido, estes tiveram como amostra 22 militares que desempenham funções em NDF.

No que concerne às entrevistas, foram entrevistados seis Chefes de SIIC e dois Procuradores do MP com experiência e contacto com a prova digital em sede de inquérito. Os primeiros, por serem deste que, hierarquicamente, dependem os NDF na estrutura de IC da GNR e por terem uma vasta experiência a nível da IC. Os segundos, por serem uma AJ e terem uma vasta experiência no que toca à valoração da prova digital como prova.

Salienta-se ainda que, apesar de as entrevistas terem sido transcritas na sua totalidade por parte do autor, para a presente investigação foram apenas transcritos excertos das respostas dos entrevistados, excertos esses que constituem parte das análises de conteúdo feitas às entrevistas.

Tal como defende 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". Assim, as seis entrevistas realizadas a Chefes das SIIC dos diversos Comandos Territoriais e as duas entrevistas realizadas a Procuradores do MP permitiram que fosse possível atingir não só uma diversidade interna, mas também uma diversidade externa, na medida em que foi possível obter contributos por parte de militares da estrutura de IC da GNR e de elementos externos à GNR que com estes trabalham. Assim, à medida que eram realizadas as entrevistas, notava-se que se estaria a atingir um ponto de saturação que se atinge quando "depois de um certo número de entrevistas, o investigador (…) tem a noção de nada recolher de novo quanto ao objeto de pesquisa" (Guerra, 2006, p. 42).

2.6. Análise SWOT

Por forma a ser feita uma análise aos NDF, recorreu-se à Análise SWOT (*Strengths, Weaknesses, Opportunities, Threats*) materializada numa Matriz SWOT (ver Quadro n.º 2) que numa primeira fase é constituída "no domínio da Análise Interna, o que se reúne sob as designações de Pontos Fortes (S) e Pontos Fracos (W), e na Análise Externa, o que se entende constituir Oportunidades (O) e Ameaças (T)" (Rosado, 2015, p. 119). Ao serem conjugadas estas duas vertentes, ou seja, a interna e a externa, Rosado afirma que "emergem as denominadas Estratégias de Desenvolvimento (SO, WO, ST e WT)" (2015, p. 119).

Quadro 2 - Caracterização dos Entrevistados

Análise Interna (S/W) **Análise Externa (O/T)**	**S (*Strengths*)** **Pontos Fortes**	**W (*Weaknesses*)** **Pontos Fracos**
O (*Opportunities*) **Oportunidades**	**Estratégias SO:** Tirar o máximo partido dos pontos fortes e aproveitar ao máximo as oportunidades detetadas	**Estratégias WO:** Mitigar ou ultrapassar os pontos fracos e simultaneamente aproveitar ao máximo as oportunidades
T (*Threats*) **Ameaças**	**Estratégias ST:** Tirar o máximo partido dos pontos fortes e minimizar os efeitos das ameaças detetadas, evitando-as, tanto quanto possível	**Estratégias WT:** Mitigar ou ultrapassar os pontos fracos e minimizar os efeitos das ameaças detetadas, evitando-as, tanto quanto possível

Fonte: Adaptado de Rosado (2015, p. 119)

CAPÍTULO 3. APRESENTAÇÃO E DISCUSSÃO DE RESULTADOS

No presente capítulo, é realizada a apresentação e discussão de todos os dados obtidos através do trabalho de campo realizado ao longo da investigação. Assim, inicia-se pela análise dos resultados dos inquéritos por entrevista, seguidos da análise dos resultados do inquérito por questionário realizado.

De seguida, será feita uma análise aos dados obtidos através da DIC finalizando com uma análise SWOT.

3.1. Inquéritos por Entrevista

3.1.1. Apresentação, análise e discussão da Questão n.º 1 dos Apêndices D, E e F

Quadro 3 - Apresentação, análise e discussão da Questão n.º 1 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"sim"
E2	"sim; boa formação inicial; capacitados para o desenvolvimento das missões atribuídas; fácil desatualização se não se verificar uma formação contínua a par das novas licenças, funcionalidades e capacidades dos *softwares* especializados; autoformação tem de ter um papel relevante"
E3	"apesar de não termos essa valência no CTer Aveiro, sei que estão devidamente capacitados tecnicamente sendo certo que têm que acompanhar o desenvolvimento tecnológico"
E4	"já se vai produzindo algum bom trabalho nestas áreas; boa formação dos militares e boa preparação do ponto de vista técnico; trabalho de qualidade"
E5	"sim, possuem conhecimentos, quer pela quantidade de equipamentos analisados, quer pelo *feedback* muito positivo que tenho tido de quem solicita o exame"
E6	"de um modo geral sim; os militares que foram escolhidos para estes núcleos já tinham alguma experiência na área por isso o processo não começou totalmente do zero"
E7	"nota-se que a GNR fez um esforço bastante considerável na melhoria das qualificações técnicas"
E8	"só tenho a dizer bem; militares bem preparados; bons conhecimentos técnicos"

Fonte: Elaboração Própria

Em relação à Questão n.º 1 dos Apêndices D, E e F ("Considera que as capacidades técnicas, conhecimentos e qualificações dos militares dos NDF, reveladas no seu contacto com estes militares, são adequadas para as competências que lhes são atribuídas em matéria de prova digital?") foi possível perceber que, do ponto de vista dos entrevistados, os militares encontram-se bem capacitados a nível de conhecimentos técnicos e qualificações para o cumprimento da sua missão nos NDF. Os militares obtiveram a sua formação a nível da

digital forense no Instituto Politécnico de Leiria (IPL) e no Centro de Formação Profissional da Indústria Eletrónica, Energia, Telecomunicações e Tecnologias da Informação (CINEL).

3.1.2. Apresentação, análise e discussão da Questão n.º 2 dos Apêndices D, E e F

Quadro 4 - Apresentação, análise e discussão da Questão n.º 2 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"sim, fruto das formações constantemente recebidas"
E2	"sim; constante formação"
E3	"sim; devidamente capacitados; procedimentos técnicos não só na extração dos dados, mas também no momento das apreensões"
E4	"sim, desde que haja uma constante atualização dos conhecimentos; troca de experiências e novas técnicas com a PJ"
E5	"sim; estão em constante formação; partilha de informação e entreajuda entre os elementos que compõem os NDF; empresas às quais a GNR adquiriu o *software* vão fornecendo formações"
E6	"sim; os próprios magistrados do MP nos pedem para colaborar em processos deles o que demonstra uma ideia positiva do seu funcionamento"
E7	"parece-me que estão constantemente a tentar atualizar, quer os materiais, quer em termos de programação disponíveis; preocupação no sentido de poder efetivamente prestar o melhor serviço possível"
E8	"têm todos os conhecimentos técnicos; preocupados em acautelar e preservar a prova"

Fonte: Elaboração Própria

Em relação à Questão n.º 2 dos Apêndices D, E e F ("Considera que os militares dos NDF revelam, na sua atuação, possuir conhecimentos atualizados e aplicar os melhores métodos e boas práticas em matéria de prova digital?") verificou-se uma resposta afirmativa, visto que os militares dos NDF estão constantemente a receber formação quanto ao *software* utilizado nos NDF por partes das empresas que fornecem esse mesmo *software*. Quando estes militares participam em buscas, sabem exatamente o que têm que fazer no imediato para preservar a prova e para assegurar a sua cadeia de custódia no que toca à prova digital. O trabalho dos militares tem uma qualidade de tal forma reconhecida, que o próprio MP muitas vezes contacta a GNR para solicitar apoio em exames de prova digital. No entanto, para que estes conhecimentos se mantenham atualizados, é da opinião da grande maioria dos entrevistados que os militares devem manter uma contínua formação de reciclagem, devendo ainda verificar-se um esforço dos próprios militares para se manterem atualizados através do acompanhamento das novas tendências. Existe igualmente um sistema de partilha de informações e entreajuda entre os elementos que compõem os NDF a nível nacional e o Laboratório de Polícia Científica (LPC) da PJ, para troca de impressões e experiências.

3.1.3. Apresentação, análise e discussão da Questão n.º 3 dos Apêndices D, E e F

Quadro 5 - Apresentação, análise e discussão da Questão n.º 3 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"conhecimentos a nível do processamento de equipamentos *mobile* (telemóveis, *tablets*) e aplicações *web* (redes sociais, aplicações de pagamento)
E2	"extração de prova digital em equipamentos eletrónicos/digitais mais específicos (centralinas de automóveis, GPS, *clouds*)"
E3	"acompanhamento do desenvolvimento tecnológico"
E4	"formação dos militares com pouca componente prática sobre a extração de conteúdos e análise"
E5	"conhecimentos ao nível de programação"
E6	"formação a nível de *software*, programação, quebra de sistemas de segurança e de *passwords* de acesso"
E7	"conhecimento do regime especial previsto para a prova digital constante da Lei do Cibercrime; jurisprudência; elevado domínio das ferramentas forenses disponibilizadas pela GNR"
E8	"dotar os restantes militares, nomeadamente aqueles que recebem o expediente e as queixas com esses conhecimentos"

Fonte: Elaboração Própria

Relativamente à Questão n.º 3 dos Apêndices D, E e F ("Que capacidades dos militares dos NDF, a nível de conhecimentos teóricos e práticos, entende que deveriam ser melhoradas para um melhor desempenho em matéria de prova digital?") as respostas variam bastante, não sendo possível encontrar uma resposta transversal a todas as entrevistas. No entanto, é de salientar que cada entrevistado tem um ponto de vista diferente visto que são chefes de SIIC com NDF, chefes de SIIC sem NDF e Procuradores do MP. Desta forma, as capacidades que deveriam ser melhoradas seriam os conhecimentos a nível de aplicações *web*, como as redes sociais (*Facebook, Instagram*, etc) e aplicações de pagamento (*MbWay*, *PayPal*, etc), extração de prova digital de equipamentos mais específicos que ainda não são trabalhados na GNR, como centralinas de automóveis, GPS e *clouds* e formação a nível de quebra de sistemas de segurança e de *passwords* de acesso.

3.1.4. Apresentação, análise e discussão da Questão n.º 4 dos Apêndices D, E e F

Quadro 6 - Apresentação, análise e discussão da Questão n.º 4 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"sim, em virtude de todo o processo ser regulado através desta norma"
E2	"sim; só assim podem conhecer os limites e formalidades essenciais para o sucesso da sua atuação"
E3	"meramente secundário pois quem tem que promover a apreensão do meio de obtenção de prova é o militar investigador"

E4	"sim; parte legal acautelada pelo investigador, mas os militares têm que garantir que o equipamento vem acompanhado do despacho judicial da autoridade judiciária que autoriza a extração"
E5	"devem possuir conhecimentos legais suficientes para o desempenho do serviço que executam; saberem o que podem fazer, o que têm que fazer e com que base é que podem fazer"
E6	"sim, mas de uma forma geral"
E7	"muita confusão a nível da terminologia"
E8	"conhecem bem a lei; preocupação em cumprir tudo o que a lei determina"

Fonte: Elaboração Própria

No que se refere à Questão n.º 4 dos Apêndices D, E e F ("Considera que os militares dos NDF devem aprofundar os seus conhecimentos relativos às normas processuais da Lei do Cibercrime?") todas as respostas apontam para um mesmo caminho. Todos os entrevistados concordam que os militares dos NDF devem ter um certo nível de conhecimento relativamente à Lei do Cibercrime nomeadamente naquilo que podem fazer e que trâmites é que devem cumprir, no entanto, esse conhecimento não tem necessidade de ser profundo visto que os militares apenas precisam de saber algumas partes da Lei do Cibercrime para o cumprimento da sua missão.

3.1.5. Apresentação, análise e discussão da Questão n.º 5 dos Apêndices D, E e F

Quadro 7 - Apresentação, análise e discussão da Questão n.º 5 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"utilização de bases de dados com capacidade de reconhecimento e comparação de dados extraídos"
E2	"*hardware*, *software* e ferramentas de eletrónica; o mais relevante é o *software* por ser o mais dispendioso e que está em contante atualização"
E3	"como não temos essa valência no CTer Aveiro, não sei que tipo de aparelhos é que os NDF estão munidos"
E4	"em termos de equipamentos, considero que estamos bem"
E5	"computadores com grande capacidade de processamento de dados; programas para análise de equipamentos eletrónicos; evolução de *hardware* e *software* ao mesmo tempo"
E6	"*software* e *hardware* evoluído para leitura e extração de dados ocultos; computadores topo de gama"
E7	"mais programas forenses certificados; menos recurso a fontes de *open source* por serem mais facilmente atacáveis por parte dos arguidos e por parte das suas defesas; criação de um regime que se diferencie do atual regime das escutas telefónicas"
E8	"disponibilizar todos os meios necessários para que possam cumprir o seu trabalho eficazmente"

Fonte: Elaboração Própria

No que concerne à Questão n.º 5 dos Apêndices D, E e F ("Quais os recursos tecnológicos que entende deverem passar a ser disponibilizados aos militares dos NDF para que estes possam relevar um melhor desempenho, em matéria de prova digital?") concluiu-se que se deveria passar a disponibilizar melhor *software*, não só por uma perspetiva de extração de dados dos diversos equipamentos e por uma constante atualização dos programas mas também por uma questão de certificação dos mesmos; e melhor *hardware*, ou seja, computadores topo de gama com grande capacidade de processamento de dados.

3.1.6. Apresentação, análise e discussão da Questão n.º 6 dos Apêndices D, E e F

Quadro 8 - Apresentação, análise e discussão da Questão n.º 6 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"sem dúvida, uma vez que os meios digitais estão ligados ao ser humano (pegada digital)"
E2	"fundamental; grande parte das nossas interações deixam rasto digital; erro grave não darmos o devido valor a este meio de prova"
E3	"sim, porque em muitos crimes (furtos, violência domésticas, tráfico de estupefacientes), a prova está apenas em mensagens que são trocadas"
E4	"sim; nos dias de hoje passa tudo um pouco pela prova digital; áudios, fotografias, mensagens, são tudo aspetos que são relevantes no decorrer de uma investigação"
E5	"sim; cada vez mais casos nos quais se vê a presença de prova digital"
E6	"cada vez mais porque muitas vezes já se vai buscar provas ao meio digital"
E7	"muitas das vezes é a única forma que temos de obter outros elementos de prova que nos permitam chegar ao autor dos crimes"
E8	"cada vez mais recorremos à prova digital; arguidos cada vez mais dotados; meio digital é utilizado para a prática de crimes"

Fonte: Elaboração Própria

Acerca da Questão n.º 6 dos Apêndices D, E e F ("Considera que a prova digital é uma mais-valia para a fase de inquérito de um processo?") todos os entrevistados, por uma razão ou por outra, responderam afirmativamente. De uma forma geral, a importância da prova digital prende-se com a facto de os meios digitais estarem ligados ao ser humano (rasto digital, pegada digital), em alguns tipos de crimes a prova está apenas em mensagens que são trocadas e porque cada vez mais se verifica a presença da prova digital em casos judiciais sendo que esta por vezes é a única forma de chegar ao autor do crime em causa.

3.1.7. Apresentação, análise e discussão da Questão n.º 7 dos Apêndices D, E e F

Quadro 9 - Apresentação, análise e discussão da Questão n.º 7 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"sim, embora careça de muito trabalho na sua análise fruto do grande volume de dados dos equipamentos analisados"
E2	"sim; não há conhecimento de qualquer alegação da falta de qualidade de recolha da prova digital efetuada por este órgão"
E3	"sim"
E4	"sim; não tivemos nada que tenha sido posto em causa"
E5	"pelo *feedback* positivo dado pelos magistrados, sem dúvida"
E6	"nos casos que tenho tido contacto, sim"
E7	"sim sem dúvida"
E8	"sim; cumprem exatamente o procedimentos que a Lei do Cibercrime impõe; a ajuda e orientação destes militares para ver o que é relevante para o processo (a nível da prova digital) é bastante útil"

Fonte: Elaboração Própria

No que concerne à Questão n.º 7 dos Apêndices D, E e F ("Considera que o trabalho realizado pelos militares dos NDF tem contribuído de forma eficaz para que a prova digital seja admitida e devidamente valorada em sede processual?") todos os entrevistados responderam afirmativamente, adicionando que não houve nenhuma alegação da falta de qualidade na recolha da prova digital e que os magistrados dão um *feedback* muito positivo em relação ao trabalho realizado pelos militares dos NDF.

3.1.8. Apresentação, análise e discussão da Questão n.º 8 dos Apêndices D, E e F

Quadro 10 - Apresentação, análise e discussão da Questão n.º 8 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"sim, embora os mesmos sejam tão extensos que carecem de uma maior e melhor análise para se poder aproveitar toda a prova carreada no processo"
E2	"sim; intuitivos e disponibilizam os dados necessários para a sua eficaz interpretação em sede judicial"
E3	"sim"
E4	"sim, mas penso que deve haver logo a incorporação no processo daquilo que se entende ter realmente interesse para o processo em causa"
E5	"sim"
E6	"sim, porque são a garantia de que aquele ficheiro foi efetivamente retirado de um certo equipamento que por sua vez pertencia ao arguido; garantia de uma cadeia de custódia"
E7	"são essenciais; no entanto são demasiados extensivos; existência de programas forenses que permitam afinar as pesquisas para que saia um relatório mais específico"
E8	"o relatório é essencial; nunca vi ser colocado em causa por nenhuma das partes"

Fonte: Elaboração Própria

Relativamente à Questão n.º 8 dos Apêndices D, E e F ("Considera que os relatórios de resultados da prova digital elaborados pelos militares dos NDF contribuem de forma eficaz para a admissibilidade e valoração da prova digital?"), todos os entrevistados responderam afirmativamente, acrescentando ainda que são essenciais. Os relatórios de resultados são a garantia de que um certo ficheiro, informação ou dado foi efetivamente retirado ou extraído de um certo equipamento que por sua vez pertence ao arguido do processo em causa garantindo assim uma cadeia de custódia. No entanto, estes relatórios de resultados são demasiado extensos, porque não têm apenas a informação relevante para o processo, mas sim toda a informação extraída de um certo equipamento.

3.1.9. Apresentação, análise e discussão da Questão n.º 9 dos Apêndices D, E e F

Quadro 11 - Apresentação, análise e discussão da Questão n.º 9 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"sim, como testemunhas. Como peritos, só quando nomeados"
E2	"não tem sido frequente, mas os militares estão cientes e preparados para tal"
E3	"poderão ser chamados a depor em tribunal como testemunhas; tem que ser nomeado perito pelo juiz no âmbito do CPP"
E4	"chamados durante o inquérito para explicar certos pormenores aos Procuradores, sempre de forma informal; não quer dizer que não venha a acontecer"
E5	"poderão ser ouvidos na qualidade de peritos; o militar já foi chamado, de forma informal, para explicar ao magistrado do MP a análise efetuada"
E6	"tenho ideia que não, nem como peritos, nem como testemunhas; serão ouvidos caso haja alguma dúvida relativamente ao exame"
E7	"não é comum, mas já aconteceu: já indiquei 3 ou 4 militares, e nessa situação indiquei-os como peritos; não são testemunhas dos factos, são os peritos que permitiram obter a prova e essa é a forma adequada de os ouvir; de forma informal, já contactei os militares para que me possam prestar esclarecimentos"
E8	"têm sido poucas vezes chamados; a serem ouvidos, acho que como peritos"

Fonte: Elaboração Própria

No que se refere à Questão n.º 9 dos Apêndices D, E e F ("Os militares dos NDF são ouvidos em tribunal em aspetos relacionados com prova digital?") todas as respostas apontam num mesmo caminho. Os militares dos NDF só serão ouvidos nos processos como peritos caso sejam nomeados com essa qualidade. Por outro lado, são ouvidos muitas vezes informalmente para explicar certos pormenores sobre a análise efetuada a magistrados ou procuradores, caso haja alguma dúvida relativa ao exame ou prestar outros esclarecimentos relativos ao exame ou extração de dados que tenham feito.

3.1.10. Apresentação, análise e discussão da Questão n.º 10 dos Apêndices D, E e F

Quadro 12 - Apresentação, análise e discussão da Questão n.º 10 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"investimento"
E2	"produção de prova digital através de métodos seguros e formalmente corretos de modo a constituir prova sólida em sede judicial; recuperação de dados digitais por terem sido apagados ou por danos no equipamento; recolha de dados em equipamentos atípicos"
E3	"recolha de vestígios nos aparelhos informáticos"
E4	"perspicácia por parte da GNR de ter apostado nesta área; os aparelhos descrevem um pouco da vida da pessoa podendo então conter provas importantes"
E5	"recolha e análise de dados digitais"
E6	"recolha de prova digital; melhoria na qualidade da prova e auxílio à investigação criminal"
E7	"havendo mais criminalidade, mais necessidade há de intervenção; muitos crimes cuja investigação está retirada da GNR podendo chegar a uma altura que têm potencialidade para mais, mas não têm um mecanismo legal que permita fazer mais; recursos humanos vocacionados para esta matéria (especialização); formação dos militares do territorial (patrulheiros, atendimento e militar que recebe as queixas) porque há elementos essenciais para obter prova nessas situações;
E8	"não lhe sei dizer"

Fonte: Elaboração Própria

Relativamente à Questão n.º 10 dos Apêndices D, E e F ("Quais são, no seu entender, as potencialidades dos NDF?") muitas foram as potencialidades apontadas pelos entrevistados, nomeadamente, a produção de prova digital através de métodos seguros e formalmente corretos de modo a constituir prova sólida em sede judicial, recolha e análise de dados digitais em aparelhos informáticos e melhoria na qualidade da prova e auxílio à investigação criminal.

3.1.11. Apresentação, análise e discussão da Questão n.º 11 dos Apêndices D, E e F

Quadro 13 - Apresentação, análise e discussão da Questão n.º 11 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"falta de investimento necessário para acompanhar a evolução das tecnologias da informação"
E2	"crescente procura; elevado custo de *software* especializado; demoras nas aquisições ou renovações de licenças; dificuldades burocrático-financeiras que permitam uma constante renovação das tecnologias disponíveis e da formação dos militares"
E3	"tendo em conta que não tenho um NDF na minha dependência, não consigo indicar nenhum ponto fraco"
E4	"formação que requer investimento; não aproveitamento da especialização, perdendo-se assim conhecimento"
E5	"recursos humanos, materiais e formação"
E6	"estar numa fase embrionária; desprovido tecnologicamente; necessidade de formação"

E7	"falta de recursos humanos; resposta em tempo útil"
E8	"falta de formação nesta área dos militares que não estão nesses núcleos"

Fonte: Elaboração Própria

No que concerne à Questão n.º 11 dos Apêndices D, E e F ("Quais são, no seu entender, os pontos fracos dos NDF?") muitos foram os pontos fracos apontados pelos entrevistados, nomeadamente, a falta de investimento, os elevados custos a nível de *software* e de *hardware*, demoras nas aquisições ou renovações de licenças, falta de militares especialistas na área e falta de formação a nível da prova digital dos militares que não estão nos NDF.

3.1.12. Apresentação, análise e discussão da Questão n.º 12 dos Apêndices D, E e F

Quadro 14 - Apresentação, análise e discussão da Questão n.º 12 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"investimento em *hardware* e *software* adequados"
E2	"formação contínua e especializada através de protocolos com centros universitários; aquisição e renovação constante de licenças com as mais recentes capacidades"
E3	"acompanhamento da evolução tecnológica; formação contínua; atualização dos *softwares* utilizados; parcerias a nível da formação no ensino superior; partilha de conhecimentos não só dentro da GNR, mas também com forças congéneres e no âmbito da EUROPOL"
E4	"dotar cada NDF consoante o volume de trabalho"
E5	"formação"
E6	"formação; especialização; investimento; centralização de NDF's"
E7	"formação técnica dos militares; aquisição de programas forenses; celeridade da resposta sem perda da qualidade"
E8	"mais formação e meios humanos"

Fonte: Elaboração Própria

Relativamente à Questão n.º 12 dos Apêndices D, E e F ("Quais são, no seu entender, os aspetos relativos ao NDF nos quais a GNR poderá apostar para que estes sejam cada vez mais relevantes no tratamento da prova digital?") muitos foram os aspetos relativos ao NDF nos quais a GNR poderá apostar elencados pelos entrevistados, nomeadamente o investimento em *software* e *hardware*, formação contínua e especializada através de protocolos com centros universitários, aquisição e renovação constante de licenças com as mais recentes capacidades, partilha de conhecimentos não só dentro da GNR, mas também com forças congéneres e no âmbito da EUROPOL e mais meios humanos.

3.1.13. Apresentação, análise e discussão da Questão n.º 13 dos Apêndices D, E e F

Quadro 15 - Apresentação, análise e discussão da Questão n.º 13 dos Apêndices D, E e F

Entrevistado	Resposta
E1	"falta de investimento"
E2	"dificuldades burocrático-financeiras para aquisição da tecnologia necessária para manter estes órgãos constantemente atualizados"
E3	"acompanhamento das manobras mais fraudulentas de indivíduos que são mais alertados para estas situações e que tenham outros conhecimentos informáticos mais avançados"
E4	"não consigo referir nenhuma"
E5	"dificuldade na renovação de licenças"
E6	"evolução tecnológica; legislação garantística do lado do cidadão"
E7	"não conseguir acompanhar os desenvolvimentos tecnológicos por força de restrições orçamentais; ter núcleos apenas com 1 militar"
E8	"volatilidade do crime informático"

Fonte: Elaboração Própria

No que se refere à Questão n.º 13 dos Apêndices D, E e F ("Quais são, no seu entender, as principais ameaças relativas à missão dos NDF?") muitas foram as ameaças apresentadas pelos entrevistados, nomeadamente, a falta de investimento, dificuldades burocrático-financeiras para aquisição da tecnologia necessária para manter estes órgãos constantemente atualizados, acompanhamento das manobras mais fraudulentas de indivíduos que são mais alertados para estas situações e que tenham outros conhecimentos informáticos mais avançados, dificuldade na renovação de licenças, não conseguir acompanhar os desenvolvimentos tecnológicos por força de restrições orçamentais e ter núcleos apenas com um militar.

3.1.14. Apresentação, análise e discussão da Questão n.º 14 dos Apêndices D e E

Quadro 16 - Apresentação, análise e discussão da Questão n.º 14 dos Apêndices D e E

Entrevistado	Resposta
E1	"começam a ter algum conhecimento; nem sempre conhecem todos os procedimentos a executar"
E2	"sim; pontualmente ainda se verificam procedimentos que podem ser melhorados; o não acautelamento de algumas medidas poderão inviabilizar o sucesso da prova digital"
E3	"o militar da patrulha não necessita de ter conhecimentos técnicos; tem que manter a prova intacta e salvaguardar a cadeia de custódia da prova"
E4	"existem algumas lacunas; não estão sensibilizados para colocar o telemóvel logo em modo avião para preservar a prova; não tentam pedir os *pins*, *passwords* ou outro código de acesso ao dono do equipamento permitindo assim um ganho de tempo; criação de uma *checklist* com aspetos a ter em conta em situações destas"
E5	"a grande maioria não está e essa lacuna já está identificada pelo Comando; inclusão desta matéria na FCAA; formação em procedimentos básicos"

E6	"pouco sensibilizados e preparados; há militares que têm contacto, mas por interesse pessoal; a prova digital é um meio de prova que nem sequer equacionam; formação aos militares das patrulhas, mas também aos do atendimento"

Fonte: Elaboração Própria

No que diz respeito à Questão n.º 14 dos Apêndices D e E ("As patrulhas do dispositivo territorial da GNR encontram-se sensibilizadas para a presença de prova digital num local de crime e sabem dar resposta ao manuseamento desta prova nessas circunstâncias?"), todas as respostas apontam numa mesma direção, sendo essa o facto de os militares das patrulhas e do atendimento terem pouco ou nenhum conhecimento relativo à prova digital.

3.1.15. Apresentação, análise e discussão da Questão n.º 14 do Apêndice F

Quadro 17 - Apresentação, análise e discussão da Questão n.º 14 do Apêndice F

Entrevistado	Resposta
E7	"elevada qualidade; duas dificuldades: o tempo que demoraram a ser obtidos os resultados das perícias e a forma como os resultados dos exames são apresentados são de muito difícil interpretação; no fundo temos muito bons relatórios, mas de difícil interpretação e análise por parte de um juiz, procurador ou magistrado"
E8	"correu tudo bem; facilmente identificaram o burlão; cumpriram os mandados; muito cautelosos na cadeira de custódia da prova; nada de negativo a apontar"

Fonte: Elaboração Própria

Acerca da Questão n.º 14 do Apêndice F ("Aquando da necessidade da realização de exames forenses relativos à prova digital, já contou com o apoio da IC da GNR? Quão eficaz foi esse contributo?") destaca-se a resposta dada pelo Entrevistado n.º 7 que apontou duas dificuldades apesar de referir que o trabalho dos militares foi de elevada qualidade: em primeiro lugar, o tempo que demoraram a ser realizados os exames e em segundo lugar a forma como os resultados dos exames (o relatório de resultados) é apresentado, pois refere que estes são de elevada qualidade, mas que são de difícil apresentação para quem não trabalha com este tipo de relatórios diariamente.

3.1.16. Apresentação, análise e discussão da Questão n.º 15 dos Apêndices D e F

Quadro 18 - Apresentação, análise e discussão da Questão n.º 15 dos Apêndices D e F

Entrevistado	Resposta
E1	"sim; difícil contorno a esse tempo devido à priorização de certos tipos de crimes levando a atrasos no processamento das provas nos inquéritos"
E2	"o tempo atual não é o desejável; verifica-se incapacidade de cumprir os *timings* dos despachos"
E4	"um pouco, não sendo possível cumprir o prazo de 30 dias para a realização do exame; pedidos de prorrogação"
E5	"não, porque os prazos estão a ser cumpridos"
E7	"visto dessa forma, 67 horas parece pouco. O problema é que são 67 horas a multiplicar pelas centenas de exames que é preciso fazer, atrasando assim todo o processo"
E8	"o desejável era ser o mais rápido possível; o aumento das queixas a nível informático cria mais processos ficando assim mais difícil obter-se o resultado o mais rápido possível"

Fonte: Elaboração Própria

No que diz respeito à Questão n.º 15 dos Apêndices D e F ("Tendo em conta que o tempo médio dos exames (tempo das pendências) das provas digitais do NDF sob o seu comando é de X, considera que esse tempo causa problemas quanto à celeridade desejável da fase dos inquéritos onde se inserem esses exames?") à exceção de um entrevistado (Chefe da SIIC de Viseu), nenhum dos NDF estão a cumprir os prazos devidamente, sendo que não conseguem cumprir os 30 dias do primeiro despacho tendo que ser feitos pedidos de prorrogação do prazo. Por parte dos entrevistados, foram apresentados dois problemas: a priorização de certos tipos de crimes levando a que outros processos fiquem pendentes; e o aumento das queixas a nível informático vai levar a que sejam criados mais processos levando a que haja um maior volume de trabalho, atrasando assim ainda mais o tempo de resposta.

3.1.17. Apresentação, análise e discussão da Questão n.º 15 do Apêndice E~

Quadro 19 - Apresentação, análise e discussão da Questão n.º 15 do Apêndice E

Entrevistado	Resposta
E3	"NDF de Coimbra, caso o processo esteja mais a sul do distrito de Aveiro; NDF do Porto caso o processo esteja mais a norte do distrito de Aveiro"
E6	"NDF de Vila Real; caso seja algo mais complexo, acredito que a DIC forneça apoio"

Fonte: Elaboração Própria

Em relação à Questão n.º 15 do Apêndice E ("Tendo em conta que não possui na sua dependência um NDF, no caso de existir uma situação que envolva prova digital, que NDF é que recebe esse processo?") o entrevistado n.º 3 (Chefe da SIIC de Aveiro) referiu que tanto o NDF do Coimbra como o NDF do Porto podem receber os processos dependendo de quão a norte ou a sul esteja situada a origem desse processo; e o entrevistado n.º 6 (Chefe da SIIC de Bragança) referiu que normalmente é o NDF de Vila Real que recebe os processos, mas caso seja algo mais complexo, a DIC poderia fornecer apoio.

3.1.18. Apresentação, análise e discussão da Questão n.º 16 do Apêndice D

Quadro 20 - Apresentação, análise e discussão da Questão n.º 16 do Apêndice D

Entrevistado	Resposta
E1	"sim, embora o reforço de meios humanos careça de um investimento prévio em *hardware* e *software*"
E2	"o reforço deve ser em função das necessidades de serviço; a avaliação do desempenho não pode ser aferida apenas pelo tempo das pendências; há equipamentos que necessitam de uma intervenção mais aprofundada e mais longa, de certa forma "estragando" a média dos tempos; esta análise terá que ser efetuada através do tempo das pendências a par do número total de equipamentos analisados"
E4	"a maior carência é a nível de recursos humanos; já houve a necessidade de remeter equipamentos para a DIC"
E5	"atualmente este Comando consegue dar resposta a todas as solicitações; militar já prescindiu de dias de descanso e férias para poder dar resposta e cumprir os prazos; com o início da instrução dada aos militares das patrulhas e atendimentos, visto que estes estarão mais alerta para a presença de prova digital, certamente surgirão mais solicitações, logo um maior volume de trabalho, fazendo com que o militar não consiga dar resposta; é uma boa solução o NDF ser comtemplado com mais um elemento, para colmatar situações de ausência (férias, formação ou algo imprevisto)"

Fonte: Elaboração Própria

No que concerne à Questão n.º 16 do Apêndice D ("Considerando que tem X militares no NDF sob o seu comando e que o tempo médio dos exames (tempo das pendências) das provas digitais entre 2018 e 2020 é de X, entende que este NDF deverá receber um reforço a nível de recursos humanos?") as respostas foram bastante diferentes sendo que o entrevistado n.º 1 (Chefe da SIIC de Coimbra) referiu que um reforço de meios humanos deveria ser acompanhado com um reforço a nível de *software* e de *hardware*; o entrevistado n.º 2 (Chefe da SIIC do Porto) referiu que o reforço deve ser feito em função do volume de trabalho que cada NDF tem e não apenas com os tempos das pendências; o entrevistado n.º 4 (Chefe da SIIC de Faro) referiu que a maior carência é a nível dos recursos humanos; o entrevistado n.º 5 (Chefe da SIIC de Viseu) referiu que o NDF consegue dar resposta as solicitações fruto do esforço individual do militar do NDF tendo este prescindindo dos

próprios dias de descanso e de férias para dar andamento aos exames, mas que seria uma boa solução que esse NDF fosse comtemplado com mais um elemento para colmatar situações de ausência.

3.1.19. Apresentação, análise e discussão da Questão n.º 16 do Apêndice E

Quadro 21 - Apresentação, análise e discussão da Questão n.º 16 do Apêndice E

Entrevistado	Resposta
E3	"sim, tendo em conta que é um Comando do tipo 1; temos mais processos e a criminalidade é mais complexa; no entanto, com o apoio do NDF de Coimbra e do NDF do Porto, não temos grandes dificuldades a realizar os processos"
E6	"não; devido ao número reduzido de situações reportadas, não seria devidamente rentabilizado; preferível criar um NDF regional com uma capacidade de resposta para vários Comandos Territoriais e que esteja munido do melhor *hardware* e *software* do que ter um NDF em cada Comando Territorial mais limitado com 1 ou 2 militares"

Fonte: Elaboração Própria

Em relação à Questão n.º 16 do Apêndice E ("Tendo em conta que o número de situações reportadas desde 2018 é de X, considera que deveria ser implementado um NDF neste Comando? Porquê?") as respostas dos entrevistados foram distintas, sendo que também tem que se considerar que são dois NDF com diferentes números de situações reportadas a nível de prova digital. O entrevistado n.º 3 (Chefe de SIIC de Aveiro) refere que sim tendo em conta que Aveiro é um Comando do tipo 1 mas que com o apoio do NDF de Coimbra e do NDF do Porto não têm dificuldade a realizar os processos; o entrevistado n.º 6 (Chefe de SIIC de Bragança) referiu que um NDF nesse Comando não seria devidamente rentabilizado fruto do número reduzido de situações reportadas.

3.2. Inquéritos por Questionário

A numeração das perguntas apresentadas de seguida são referentes ao Apêndice B.

3.2.1. Caracterização sociodemográfica

As perguntas n.º 1 a 5 da caracterização sociodemográfica já têm os seus dados explanados no Capítulo 2. A pergunta n.º 6 foi realizada com o intuito de poder haver um controlo sobre o número de militares que faltavam responder em cada NDF.

3.2.2. Formação

Referente à pergunta n.º 1, 20 militares (90,9%) responderam afirmativamente e 2 militares (9,1%) responderam negativamente. Todos os militares dos NDF têm o Curso de Investigação Criminal (CIC) e o Curso Digital Forense (CDF) no qual está incluída a formação no CINEL e no IPL. Dos 22 militares que responderam ao questionário, 5 militares (22,7%) têm outras formações, nomeadamente o Curso de Formação Avançada de Análise Digital e Computação Forense (GNR), Programação *Web Creation* (Formabase), Eletricidade, Eletrónica Analógica e Digital no Centro Integral de Adestramento Tecno Eletrónico (CIATE), Hardware/Redes (CIATE), Curso Experto Universitário em Informática Forense no Centro Universitário da Guardia Civil e ainda outras formações em faculdades estrangeiras, polícias estrangeiras e em marcas comerciais de ferramentas forenses.

Tratando da pergunta n.º 3, 1 militar (4,5%) discorda, 4 militares (18,2%) não discorda nem concorda, 15 militares (68,2%) concordam e 2 militares (9,1%) concordam totalmente.

As perguntas n.º 4 e 5 foram elaboradas com o intuito de perceber a opinião dos militares em relação à Lei n.º 109/2009 e ao Decreto-Lei n.º 78/87 para que depois fosse possível discutir os resultados com os entrevistados sobre esta mesma questão, não sendo assim necessário proceder à sua análise.

3.2.3. Recursos tecnológicos e humanos

Analisando as respostas à pergunta n.º 1 foi possível perceber que grande parte dos militares concorda que certos equipamentos fazem falta para a realização do seu trabalho. Mesmo os militares que responderam que têm o equipamento necessário, apontaram certos equipamentos que fazem falta. Primeiramente a nível de *hardware* os militares indicaram que faria falta o seguinte: servidores de armazenamento de dados, um computador extra para laboratório, um portátil para ações no exterior (bem como um dispositivo de internet móvel), *pens*, cartões *MicroSD*, cabos, *docking stations*, um computador específico para *brute force* (descoberta de *passwords* ou outros códigos de acesso), um *Unlimited Power Source* (UPS) que funciona como um sistema de alimentação de energia secundário para situações de emergência tal como faltas de luz por exemplo, computadores com processadores potentes de última geração. Em segundo lugar, a nível de *software* os militares indicaram que faria falta o seguinte: sistemas forenses para extração de processadores *Kirin* (frequentemente

usados pela empresa *Huawei*), para recuperação e extração em discos e para extração de dados em veículos, licenças da *Cellebrite* como a *Universal Forensic Extraction Device* (UFED), *Cellebrite Advanced Services* (CAS), *Cellebrite Cloud* e *Cellebrite* UFED *Link Analysis* e ainda a licença da *Oxygen XML Editor*.

Relativamente à pergunta n.º 2, foi fornecida aos militares a Tabela n.º 7 e, de uma forma geral, os militares concordam que é necessário completar o quadro de efetivo para um bom cumprimento da missão dos NDF, sendo possível ver na Tabela n.º 1 que 11 dos 15 NDF é constituído apenas por 1 militar e caso este militar integre alguma escala de serviço, esteja de férias ou de folga, o NDF acaba por estar parado.

3.2.4. Valoração da prova digital

Relativamente à pergunta n.º 1 foi possível perceber que todos os militares têm recebido bom *feedback* em relação ao seu desempenho a nível da prova digital. No entanto, alguns militares referem que nem sempre recebem esse *feedback* e que seria do seu interesse serem informados sobre a conclusão do processo para o qual produziram a prova digital por forma a terem conhecimento da importância da prova produzida em processo. Ainda assim, há militares que referem que, de forma informal, lhes é informado que a prova digital foi fundamental para a condenação e medida de pena. Logo, havendo esta disparidade, a mesma poderá estar relacionada com a forma de trabalhar dos magistrados ou procuradores.

3.2.5. Testemunho em Tribunal

Analisando a pergunta n.º 1, 13 militares (59,1%) referiram que, como membros do NDF, nunca tiveram que prestar declarações em tribunal e 9 militares (40,9%) referiram que, como membros do NDF, já tiveram que prestar declarações em tribunal.

Referindo à pergunta n.º 2, apenas 2 militares foram indicados como peritos para produção de prova para um processo sendo que os restantes 7 apenas prestaram declarações como testemunha, para explicar ou justificar certos procedimentos e ajudar na interpretação dos exames elaborados.

3.2.6. Análise ao trabalho dos NDF

Esta secção teve o intuito de perceber a opinião dos militares em relação a certos processos sobre o seu trabalho para que depois fosse possível discutir os resultados com os entrevistados sobre esta mesma questão, não sendo assim necessário proceder à sua análise.

3.3. Dados da DIC

O presente subcapítulo tem o objetivo de demonstrar todos os dados e informações obtidos juntos da DIC em relação a toda a atividade digital forense desde o ano de 2018 até ao ano de 2020. Tais dados e informações são provenientes da plataforma *Digital Forensic Lab Manager* e dos Mapas Anuais da Digital Forense de 2018, 2019 e 2020.

3.3.1. Número de militares por NDF

O presente subcapítulo pretende demonstrar o número de militares por cada NDF. É de realçar que, no caso da DIC, o NDF encontra-se na Divisão de Criminalística (DC) e no caso da UAF se encontra no Destacamento de Pesquisa (DP).

Tabela 1 - Número de militares por NDF

Núcleo Digital Forense	Número de Militares
NDF Beja	1
NDF Braga	1
NDF Castelo Branco	1
NDF Coimbra	3
DIC/DC	5
NDF Faro	2
NDF Leiria	1
NDF Portalegre	1
NDF Porto	3
NDF Santarém	1
NDF Setúbal	1
NDF Viana do Castelo	1
NDF Vila Real	1
NDF Viseu	1
UAF/DP	1
Total	24

Fonte: Elaboração Própria

3.3.2. Comandos sem NDF e fluxo de vestígios

Apesar de um Comando da GNR não ter constituído na sua estrutura de IC um NDF, tal não significa que não exista a necessidade de serem realizados exames que envolvam prova digital. Assim, neste subcapítulo, são explanados não só os Comandos da GNR que não têm na sua estrutura de IC um NDF, mas também para que NDF é enviado o pedido de exame de prova digital.

Tabela 2 - Comandos sem NDF e fluxo de vestígios

Comando sem NDF	Fluxo de Vestígios
Comando Territorial da Guarda	NDF Coimbra
Comando Territorial da Madeira	DIC/DC
Comando Territorial de Aveiro	DIC/DC
Comando Territorial de Bragança	NDF Porto
Comando Territorial de Évora	DIC/DC
Comando Territorial de Lisboa	DIC/DC
Comando Territorial dos Açores	DIC/DC

Fonte: Elaboração Própria

3.3.3. Tipo de equipamentos examinados

Tabela 3 - Tipo de equipamentos examinados

Tipo de Equipamentos	2018	2019	2020
Computador	221	273	295
GPS	22	14	24
Telefone	1130	1571	1903
Cartão SIM	41	74	78
Unidade de Memória	260	260	316
Disco Rígido	100	48	87
Câmara	9	9	28
Modem/Router	5	5	3
Videovigilância	7	6	13
Diversos	43	73	85
Total	1838	2333	2832

Fonte: Elaboração Própria

3.3.4. Crime associado

Apesar de serem muitos os crimes associados, e segundo os dados fornecidos pela DIC, desde o ano de 2018 até ao ano de 2020 foram associados 100 tipos de crimes no que toca aos exames da prova digital, muitos destes crimes não têm uma incidência relevante. Desta forma, a lista de crimes inframencionada na Tabela n.º 4 é constituída pelos crimes que tiveram um somatório de ocorrências igual ou superior a 20 desde o ano de 2018 até ao ano de 2020.

Tabela 4 - Crime associado

Crime	2018	2019	2020
Ameaça e coação	24	36	27
Burla informática	8	11	7
Devassa da vida privada	4	9	12
Difamação, calúnia e injúria	13	16	5
Fraude Fiscal Aduaneira	8	12	12
Furto em edifício comercial ou industrial com arrombamento, escalamento ou chaves falsas	12	16	34

Furto em residência com arrombamento, escalamento ou chaves falsas	11	19	32
Tráfico de estupefacientes	150	229	333
Violência doméstica conjugal ou relação análoga	82	103	187
Total	312	451	649

Fonte: Elaboração Própria

3.3.5. Número de exames por NDF

Tabela 5 - Número de exames por NDF

Núcleo Digital Forense	2018	2019	2020
NDF Beja	0	30	78
NDF Braga	0	0	280
NDF Castelo Branco	0	0	112
NDF Coimbra	1284	1058	848
DIC/DC	801	702	801
NDF Faro	4	479	253
NDF Leiria	0	23	69
NDF Portalegre	0	0	60
NDF Porto	0	289	392
NDF Santarém	0	0	160
NDF Setúbal	0	0	166
NDF Viana do Castelo	0	0	165
NDF Vila Real	0	0	447
NDF Viseu	0	27	190
UAF/DP	0	0	527
Total	2089	2608	4548

Fonte: Elaboração Própria

3.3.6. Tempo de execução de exames por equipamento

Será importante referir numa primeira fase que, os tempos mencionados na Tabela n.º 6 foram calculados pela data/hora registada no início do exame e fim do exame do equipamento em concreto, tempos os quais incluem tempos de registos, pausas durante o exame, horário fora do horário de trabalho (descanso), pesquisa da solução e são tempos sobrepostos de trabalho com exames de outros dispositivos em simultâneo.

Tabela 6 - Tempo de execução de exames por equipamento

Tipo de equipamento	2018	2019	2020	Média
Computador	91,23	87,18	115,26	97,89
GPS	65,86	81,04	69,21	72,03
Telefone	77,96	109,61	144,91	110,83
Cartão SIM	0,30	0,30	0,30	0,30
Unidade de Memória	74,79	71,47	94,48	80,25
Disco Rígido	103,03	111,03	134,96	116,34
Câmara	81,88	107,83	108,57	99,43
Modem/Router	80,16	84,23	68,13	77,51
Videovigilância	82,45	40,00	41,90	54,78
Média	73,07	76,97	86,41	78,82

Fonte: Elaboração Própria

3.3.7. Tempo de execução de exames por NDF

Será importante referir numa primeira fase que, os tempos mencionados na Tabela n.º 7 foram calculados pela data/hora registada no início do exame e fim do exame do equipamento em concreto, tempos os quais incluem tempos de registos, pausas durante o exame, horário fora do horário de trabalho (descanso), pesquisa da solução e são tempos sobrepostos de trabalho com exames de outros dispositivos em simultâneo.

Tabela 7 - Tempo de execução de exames por NDF

Núcleo Digital Forense	2018	2019	2020	Média
NDF Beja	0	48,88	126,54	87,71
NDF Braga	0	79,33	62,16	70,75
NDF Castelo Branco	0	0	49,13	49,13
NDF Coimbra	74,42	56,89	64,68	65,33
DIC/DC	71,90	77,23	65,10	71,41
NDF Faro	23,23	92,42	86,19	67,28
NDF Leiria	0	59,83	67,08	63,46
NDF Portalegre	0	157,38	105,41	131,40
NDF Porto	14,07	89,91	96,10	66,69
NDF Santarém	0	189	69,51	129,26
NDF Setúbal	0	149,04	126,01	137,53
NDF Viana do Castelo	0	121,52	105,46	113,50
NDF Vila Real	0	55,32	80,89	68,11
NDF Viseu	0	103,19	142,44	122,82

UAF/DP	71,93	93,03	120,22	95,03
Média	51,09	98,07	91,13	

Fonte: Elaboração Própria

3.4. Análise SWOT

Quadro 22 - Matriz SWOT

Análise Interna (S/W)	
S (*Strengths*) **Pontos Fortes**	**W (*Weaknesses*)** **Pontos Fracos**
- Especialização; - Recolha de prova que se tem vindo a mostrar fundamental; - Produção de prova digital, através de métodos seguros e formalmente corretos, de modo a constituir prova sólida em sede judicial;	- Falta de meios para operar no terreno; - Conhecimento autodidata; - Descentralização; - NDF com apenas 1 militar; - Elevado custo de *software* especializado;
Análise Externa (O/T)	
O (*Opportunities*) **Oportunidades**	**T (*Threats*)** **Ameaças**
- Acompanhar o desenvolvimento tecnológico; - Reuniões entre os militares dos NDF para discussão e análise de procedimentos; - Investimento em formação contínua e *software*/*hardware*; - Atualização dos quadros orgânicos; - Criação de um manual com procedimentos técnicos redigidos, aprovados e difundidos, que enquadrem a atuação dos NDF, normalizando, assim, a atividade digital forense;	- Técnicas anti forenses; - Falta de formação do dispositivo territorial; - Crescente evolução dos meios tecnológicos; - Laboratórios sem credenciação a nível de segurança e sem sistema de controlo de acessos;

Fonte: Elaboração Própria

CONCLUSÕES

O presente trabalho de investigação foi desenvolvido com o objetivo de analisar a capacidade de resposta dos militares pertencentes a qualquer NDF da GNR em matéria de tratamento da prova digital. A metodologia utilizada ao longo da investigação, assente na recolha e análise documental, inquéritos por entrevista e inquéritos por questionário, permitiu não só chegar a resultados que conduzem a respostas fundamentadas relativas ao tema, como também permitiu expandir o nosso nível de conhecimento relativamente à temática da prova digital.

Sumarizando os resultados que decorreram da investigação e das respetivas análises documentais, inquéritos por entrevista e inquéritos por questionário, são, assim, apresentadas as respostas fundamentadas a cada uma das perguntas derivadas e à PP, levantadas no início da investigação.

Relativamente à formação dos militares, todos os Chefes de SIIC e Procuradores do MP que participaram consideraram que os militares dos NDF se encontram devidamente capacitados para o cumprimento das suas funções, reforçando ainda que o trabalho dos mesmos é de qualidade e que o *feedback* recebido por quem solicita o exame tem sido muito bom. No entanto, é de salientar que estes resultados têm sido possíveis pelo facto de os militares serem autodidatas, haver troca de impressões com o LPC da PJ e existir partilha de informações entre os elementos que compõem os NDF. Da parte dos militares dos NDF estes concordam que a sua formação é adequada. No entanto, afirmam que com uma formação ainda mais avançada fornecida pela GNR, seria possível obter resultados bastante superiores do seu trabalho.

No que concerne aos recursos tecnológicos, concluiu-se que é de extrema importância a constante formação sobre os programas informáticos utilizados em cada momento, uma vez que estes estão sempre em alteração, nomeadamente através de programas forenses certificados, como sucede em relação às licenças da *Cellebrite* e da *Oxygen*. Conclui-se ainda que, no contexto da prova digital, se devem evitar programas informáticos originários de fontes de *open source*, pois são mais facilmente atacáveis por parte dos arguidos e das suas defesas. A nível de *hardware*, conclui-se que são necessários os seguintes equipamentos mínimos: um computador fixo para laboratório, um computador portátil para ações no exterior (bem como um dispositivo de internet móvel), *pens*, cartões *MicroSD*, cabos, *docking stations*, um computador específico para *brute force* (descoberta de palavras-chave

ou outros códigos de acesso), um *Unlimited Power Source* (UPS) que funciona como um sistema de alimentação de energia secundário para situações de emergência, tal como faltas de luz, por exemplo, e computadores com processadores potentes de última geração para processamento de grandes volumes de dados. Relativamente aos recursos humanos, os entrevistados consideraram que o aumento destes recursos deve ser acompanhado de um reforço a nível de *software* e de *hardware* e que, para apurar da necessidade do aumento de recursos humanos, deverá ser tido em conta o volume de trabalho de cada NDF, atento o tempo das pendências. Por parte dos militares dos NDF, há o entendimento de que é essencial atualizar o quadro de efetivo dos NDF, principalmente daqueles que constituídos apenas por um militar, pois caso este militar integre alguma escala de serviço, esteja de licença de férias ou esteja de folga, esse NDF acaba por ficar parado, aumentando assim o tempo das pendências.

No que diz respeito ao tempo das pendências nos diferentes NDF, este não pode ser analisado de forma isolada, pois existem outros pormenores a ter em conta (para além dos que já anteriormente mencionados) como o número de solicitações feitas a cada NDF, sendo que este pode receber pedidos de exame por parte de um Comando que não disponha de NDF; o número de militares que constituem o NDF e se estes integram ou não serviços de escala; o *software* e o *hardware* disponível em cada NDF, uma vez que a falta de *software* ou *hardware* adequado pode comprometer a realização do exame, tendo este que ser feito num NDF que esteja capacitado para tal; e, por fim, a priorização dos exames que é feita pela seguinte ordem: exames para primeiro interrogatório, processos-crime com arguidos presos, despacho superior, processos relativos a crimes que estejam previstos no art. 5.º da Lei n.º 55/2020, de 27 de agosto, que define os objetivos, prioridades e orientações de política criminal para o biénio de 2020-2022 e, em último, os processos mais antigos. Este facto pode levar à seguinte situação: um exame A relacionado com um processo-crime com um arguido preso entra no NDF, despoletando o início do exame, e, no dia seguinte, entra um exame B relacionado com um primeiro interrogatório, que passa a ser realizado com prioridade em relação ao exame A. Assim, tal como já foi referido, sendo que os tempos das pendências são calculados pela data/hora registada no início do exame e fim do mesmo, o tempo do exame A está a correr simultaneamente ao tempo do exame B. No entanto, apenas este último está a ser realizado, aumentando o tempo das pendências do exame A e levando a um aumento na média do tempo das pendências. O tempo das pendências nem sempre revela efetiva e precisamente o tempo despendido em cada exame, mas antes o tempo entre

a sua entrada no NDF e a sua saída, podendo não ser esta a forma mais correta de cálculo do tempo das pendências.

Em relação à valoração da prova digital como meio de prova, concluiu-se que esta é cada vez mais importante, independentemente do tipo de crime, pois muitas vezes vai-se buscar ao digital um meio de prova importante. Grande parte das nossas interações no dia-a-dia está em *bits*, pelo que deixam rasto digital (pegada digital) nos equipamentos que utilizamos. Atualmente, a criminalidade dita tradicional é também ela muitas vezes praticada através de plataformas digitais, sejam os crimes de injúrias, difamações, ameaça, extorsão e sabotagem, tornando assim a prova digital cada vez mais relevante. As duas tipologias de crime onde a prova digital tem estado cada vez mais presente consistem no tráfico de estupefacientes e na violência doméstica conjugal ou relação análoga (ver Tabela n.º 4).

No que se refere à audição dos militares durante o processo em tribunal, concluiu-se que, em grande parte das situações, os militares são ouvidos como testemunhas e apenas pontualmente como peritos, pois, para terem esta qualidade, têm que ser nomeados como tal. Pese embora serem maioritariamente ouvidos como testemunhas, nessas situações verificou-se que os militares se deslocavam ao tribunal informalmente, a pedido do juiz, procurador ou magistrado, não para falar sobre matéria de facto do processo, mas para explicarem ou justificarem certos procedimentos que tiveram que tomar aquando da execução do exame, ou para ajudar na abertura e interpretação do exame ou para explicar a linguagem que está no relatório de resultados, para que esta seja mais percetível. É da opinião de um dos Procuradores do MP que os militares deveriam ser ouvidos como peritos, porque não são testemunhas dos factos, mas antes peritos que permitiram obter a prova.

Por fim, respondendo à PP: "*Quais as capacidades dos militares dos Núcleos Digitais Forenses da Guarda Nacional Republicana no âmbito do tratamento da prova digital?*" e considerando que a resposta às perguntas derivadas auxilia na resposta à PP, conclui-se que estes militares apresentam muitas capacidades nesse âmbito, destacando-se, de entre estas, a de análise de equipamentos, como computadores, GPS, telefones, cartões SIM, unidades de memória, câmaras, *modem-routers*, câmaras de videovigilância, entre muitos outros. Dependendo do equipamento em causa, e devido às suas características e especificidades, o tempo de análise pode ser diverso. Estas capacidades dos militares dos NDF da GNR no âmbito do tratamento da prova digital devem ser aproveitadas ao máximo, tendo em conta que esta é uma valência relativamente recente na GNR e que, desde 2018, data da sua implementação, tem vindo a mostrar bons resultados.

A GNR deverá procurar fornecer formação contínua, constante atualização de conhecimentos e até novas formações através do estabelecimento de protocolos com instituições de ensino para o desenvolvimento de capacidades e conhecimentos adaptados às necessidades dos NDF, bem como fomentar a partilha de informação, conhecimentos e experiências com forças congéneres e no âmbito da Agência da União Europeia para a Cooperação Policial (EUROPOL) ou da Agência da União Europeia para a Formação Policial (CEPOL). É impreterível que haja um acompanhamento constante das evoluções tecnológicas por parte dos militares dos NDF. Aconselha-se a que, para tal, a GNR crie um grupo de trabalho, que envolva todos os militares dos NDF, com reuniões periódicas e frequentes para que haja uma partilha de conhecimentos e experiências, sobretudo em relação a novas práticas criminais ou novas técnicas que possam ter aparecido.

Paralelamente à formação dos recursos humanos e à sua constante atualização de conhecimento, a GNR deve procurar disponibilizar-lhes o *software* e *hardware* adequados para o exercício das suas funções e compatíveis entre si. De facto, de nada serve ter um programa informático muito evoluído se depois não existem computadores capazes de correr esse programa.

Conclui-se, ainda, que a GNR deveria procurar alterar alguns procedimentos. Em situações de operações de busca, muitas vezes não contam com um militar do NDF. Foi possível perceber através do inquérito por questionário que, em grande parte das situações, o militar investigador da IC Operativa é quem faz a apreensão dos equipamentos. Desta forma, não tendo este último o mínimo de formação a nível da prova digital, poderá contaminar a prova, tornando-a inútil para o processo. Assim, seria de extrema relevância começar a dar valor a estes militares, fruto do conhecimento específico que estes têm, e incluí-los nestas operações.

Formação ao dispositivo territorial, nomeadamente aos militares que fazem patrulha, atendimento e recebimento de queixas. Esta, poderia passar por procedimentos básicos como identificar a presença de prova digital num local e isolar essa mesma para que, após um militar do NDF seja chamado ao local, o mesmo possa realizar o seu trabalho, pois só um militar da IC deverá entrar em contacto com a prova digital e ainda, a simples recolha de *pins, passwords, pattern locks*, verificar o uso de *finger print* e colocar os aparelhos em modo avião. Estes militares, não estando sensibilizados, acabam por nem sequer equacionar a prova digital como um meio de prova, perdendo-se, assim, a oportunidade de ser recolhida prova importante para um processo.

É importante também que a GNR seja capaz de fazer uma gestão de carreira destes militares de uma forma eficaz. Quando haja uma promoção, há que ter em conta que estes militares têm uma formação muito especializada, de difícil e morosa aquisição, não se devendo perder todo o investimento nessa formação nem todo o conhecimento e experiência adquiridos ao longo de anos na realização deste tipo de trabalho, colocando o militar numa área totalmente distinta. É necessário que existam formas diferentes de gerir a carreira dos militares pertencentes a especialidades. Caso contrário, nunca teremos militares com conhecimento profundo sobre determinados assuntos.

RECOMENDAÇÕES

Tendo em conta que a atividade digital forense ainda é relativamente recente na GNR, muitas foram as matérias que foram aparecendo ao longo da execução da presente investigação e que, futuramente, poderão ser alvo de investigação científica por parte dos futuros Aspirantes da GNR no âmbito do TIA. Estas diversas matérias surgiram não só na fase de execução da revisão da literatura, mas também no trabalho de campo, aquando da construção dos inquéritos por entrevista e dos inquéritos por questionário, bem como nas suas respostas. Estas diversas matérias apresentam-se como áreas de especialização dentro da IC, que poderão ser objeto de posteriores investigações. De entre estas, destacam-se as seguintes:

- A prova digital e as redes sociais;
- Recolha de prova digital em equipamentos eletrónicos como *smartTV*, consolas de jogos (*PlayStation*, *Xbox*, etc) ou mesmo em *clouds*;
- A importância da prova digital recolhida em sistemas *closed-circuit television* (CCTV);
- O impacto da pandemia do SARS-CoV-2 na prova digital;
- A argumentação possível dos advogados de defesa, com o objetivo de as ações policiais precaverem eventuais futuros problemas com as provas recolhidas.

REFERÊNCIAS BIBLIOGRÁFICAS

Academia Militar [AM] (2015). *Norma de Execução Permanente n.º 520/4.ª: Trabalho de Investigação Aplicada*. Lisboa: AM.

Academia Militar [AM] (2016). *Norma de Execução Permanente n.º 522/1.ª: Normas para a Redação de Trabalhos de Investigação*. Lisboa: AM.

Almeida, I. F. (2014). *A prova digital*. Dissertação de Mestrado, Mestrado em Ciências Jurídicas, Universidade Autónoma de Lisboa, Lisboa.

Assembleia da República [AR] (2007). Lei n.º 63/2007 de 6 de novembro: Lei Orgânica da Guarda Nacional Republicana. *Diário da República*, 1.ª série, n.º 213, 8043-8051.

Assembleia da República [AR] (2008). Lei n.º 49/2008 de 27 de agosto: Lei de Organização da Investigação Criminal. *Diário da República*, 1.ª série, n.º 165, 6038-6042.

Assembleia da República [AR] (2009). Lei n.º 109/2009 de 15 de setembro: Lei do Cibercrime. *Diário da República*, 1.ª série, n.º 179, 6319-6325.

Branco, C. M. M. (2010). *Guarda Nacional Republicana. Contradições e Ambiguidades*. Lisboa: Edições Sílabo.

Braz, J. A. C. (2017). *Evolução histórica da prova em processo penal – do pensamento mágico à razão. A investigação do crime organizado no Estado de Direito*. Dissertação de Mestrado, Mestrado em Ciências Jurídico-Forenses, Faculdade de Direito da Universidade de Lisboa, Lisboa.

Cancela, A. G. L. (2016). *A prova digital: os meios de obtenção de prova na lei do cibercrime*. Dissertação de Mestrado, Mestrado em Direito na Área de Especialização em Ciências Jurídico-Forenses, Faculdade de Direito da Universidade de Coimbra, Coimbra.

Carrapiço, H. F. (2005). O crime organizado e as novas tecnologias: uma faca de dois gumes. *Nação e Defesa*. 111(3), 175-192.

Fortin, M. (2009). *Fundamentos e Etapas no Processo de Investigação*. Loures: Lusodidacta.

Freixo, M. J. V. (2013). *Metodologia Científica – Fundamentos, Métodos e Técnicas* (4ª Edição). Lisboa: Instituto Piaget.

Guerra, I. C. (2006). *Pesquisa Qualitativa e Análise de Conteúdo – Sentidos e formas de uso*. Parede: Principia.

International Organization for Standardization [ISO] (2012). ISO/IEC 27037. In *site da International Organization for Standardization*. Acedido a 18 de fevereiro de 2021 em https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

Kirk, P. L. (1953). *Crime Investigation: Physical Evidence and the Police Laboratory*. Genebra: Interscience Publishers.

Lessa, B. M. (2009). A invalidade das provas digitais no processo judiciário. In site do *Jus Navigandi*. Acedido a 21 de fevereiro de 2021 em https://jus.com.br/artigos/14555/a-invalidade-das-provas-digitais-no-processo-judiciario/5.

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

Mateus, M. T. (2016). *Crimes em ambiente digital – Investigação da GNR para a obtenção de prova*. Trabalho de Investigação Aplicada, Mestrado em Ciências Militares na Especialidade de Segurança, Academia Militar, Lisboa.

Mendes, P. S. (2014). *Lições de Direito Processual Penal*. Coimbra: Almedina.

Militão, R. L. (2012). A propósito da prova digital no processo penal. *Revista da Ordem dos Advogados*. 72(1), 247-285.

Ministério da Justiça [MJ] (1987). Decreto-Lei n.º 78/87 de 17 de fevereiro: Código de Processo Penal. *Diário da República*, 1.ª série, n.º 40, 617-699.

Prodanov, C. & Freitas, E. C. (2013). *Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico.* Novo Hamburgo: Universidade FEEVALE.

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

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

Ramos, A. D. (2014). *A prova digital em processo penal: o correio eletrónico*. Lisboa: Chiado Editora.

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

Rodrigues, B. S. (2011). *Da Prova Penal – Tomo IV: da Prova-Eletrónico-Digital e da Criminalidade Informático-Digital*. Lisboa: Rei dos Livros.

Rosado, D. P. (2015). *Sociologia da Gestão e das Organizações* (1ª Edição). Lisboa: Gradiva.

Rosado, D. P. (2017). *Elementos Essenciais de Sociologia Geral* (1ª Edição). Lisboa: Gradiva.

Sarmento, M. (2013). *Metodologia científica para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada.

Scientific Working Group on Digital Evidence / Scientific Working Group on Imaging Technology (2010). SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence v2. In site do *Scientific Working Group on Digital Evidence*. Acedido a 19 de fevereiro de 2021 em https://www.swgde.org/documents/published

Scientific Working Group on Digital Evidence [SWGDE] (2016). SWGDE Digital and Multimedia Evidence Glossary v3. In *site do Scientific Working Group on Digital Evidence*. Acedido a 14 de fevereiro de 2021 em https://www.swgde.org/documents/published

Tribunal da Relação do Porto [TRP] (2016). Acórdão do Tribunal da Relação do Porto, de 7 de julho de 2016, Processo n.º 2039/14.0JAPRT.P1. In *site da Direção Geral dos Serviços Informáticos*. Acedido a 19 de fevereiro de 2016 em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/cffe710b2cb8d91e802580050047 5ea9?OpenDocument

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

APÊNDICES

APÊNDICE A – MODELO DE ANÁLISE (ESTRUTURA DA INVESTIGAÇÃO APLICADA)

Objetivo Geral (OG)	Pergunta de Partida (PP)	Objetivos Específicos (OE)	Perguntas Derivadas (PD)
(OG) Analisar a capacidade de resposta dos militares pertencentes a qualquer Núcleo Digital Forense da Guarda Nacional Republicana no âmbito do tratamento da prova digital.	(PP) Quais as capacidades dos militares dos Núcleos Digitais Forenses da Guarda Nacional Republicana no âmbito do tratamento da prova digital?	(OE1) Analisar se a formação que os militares constituintes dos NDF receberam é adequada à sua função (e se esta formação é realizada internamente, externamente ou se há uma complementaridade entre ambas) e se estes possuem os conhecimentos adequados para que possam realizar um bom trabalho.	(PD1) A formação dos militares que integram os NDF em matéria de prova digital é adequada à sua função?
		(OE2) Analisar se os NDF se encontram munidos com os recursos tecnológicos (*hardware* e *software*) e humanos (quer em quantidade como em qualidade) necessários para o tratamento da prova digital.	(PD2) Os recursos tecnológicos e humanos que os NDF têm ao seu dispor são adequados para o bom cumprimento da sua missão?
		(OE3) Determinar o tempo das pendências, ou seja, o tempo que demoram a ser realizados os diversos exames à prova digital.	(PD3) Qual o tempo das pendências nos diferentes NDF?
		(OE4) Analisar, de uma perspetiva do MP se a prova digital é valorada como meio de prova.	(PD4) Qual o valor da prova digital como meio de prova?
		(OE5) Perceber se os militares são ouvidos durante o processo em tribunal e se sim, se são ouvidos como testemunhas ou como peritos.	(PD5) São os militares ouvidos durante o processo em tribunal? Como testemunhas ou como peritos?

Quadro 23 - Modelo de Análise (Estrutura da Investigação Aplicada)
Fonte: Elaboração própria

APÊNDICE B – INQUÉRITO POR QUESTIONÁRIO

Trabalho de Investigação Aplicada - Núcleo Digital Forense da Guarda Nacional Republicana

O presente inquérito, efetuado mediante um questionário, surge no âmbito do Trabalho de Investigação Aplicada (TIA), necessário para a conclusão do Curso de Formação de Oficiais da Guarda Nacional Republicana no curso de Mestrado Integrado em Ciências Militares, na Especialidade de Segurança. Este TIA está subordinado ao tema "Núcleo Digital Forense da Guarda Nacional Republicana" e está a ser elaborado pelo Aspirante de Infantaria da Guarda Nacional Republicana, José Miguel Armada de Matos.

O inquérito é dirigido aos militares da Investigação Criminal da GNR, nomeadamente aos que trabalham nos NDF. Todos os dados presentes neste questionário são anónimos e serão utilizados exclusivamente para a presente investigação do autor, no âmbito do referido TIA.

Para a obtenção de esclarecimentos em relação ao questionário, utilize os seguintes meios de contacto:
E-mail: matos.jma@gnr.pt
Telemóvel: 912 877 961

Carregue em "Seguinte" para iniciar o questionário.

*Obrigatório

Caracterização sociodemográfica

1. 1 - Idade *

2. 2 - Género *

Marcar apenas uma oval.

- ◯ Feminino
- ◯ Masculino
- ◯ Outro

3. 3 - Posto *

Marcar apenas uma oval.

- ◯ Guarda
- ◯ Guarda Principal
- ◯ Cabo
- ◯ Cabo de Curso
- ◯ Cabo Chefe
- ◯ Cabo Mor
- ◯ Segundo Sargento
- ◯ Primeiro Sargento
- ◯ Sargento Ajudante
- ◯ Sargento Chefe
- ◯ Sargento Mor

4. 4 - Anos na Investigação Criminal (coloque apenas o número cardinal em algarismos, sem palavras - por exemplo, "5" e não "5 anos") *

5. 5 - Grau Académico *

Marcar apenas uma oval.

- ◯ Até ao 9.º ano
- ◯ 10.º ano
- ◯ 11.º ano
- ◯ 12.º ano
- ◯ Bacharelato
- ◯ Licenciatura
- ◯ Mestrado
- ◯ Doutoramento
- ◯ Outra: _____

6. 6 - Núcleo Digital Forense onde presta serviço *

Marcar apenas uma oval.

- ◯ NDF Beja
- ◯ NDF Braga
- ◯ NDF Castelo Branco
- ◯ NDF Coimbra
- ◯ DIC/DC
- ◯ NDF Faro
- ◯ NDF Leiria
- ◯ NDF Portalegre
- ◯ NDF Porto
- ◯ NDF Santarém
- ◯ NDF Setúbal
- ◯ NDF Viana do Castelo
- ◯ NDF Vila Real
- ◯ NDF Viseu
- ◯ UAF

Formação

7. 1 - Possui formação técnica e especializada no âmbito da Investigação Criminal vocacionada para lidar com a prova digital? *

8. 2 - Se respondeu que sim à questão anterior, refira onde adquiriu essa formação.

9. 3 - Considero que os cursos/formações de que disponho me habilitam a trabalhar de forma eficiente para o bom cumprimento da minha missão no NDF (Escala de Litker). *

   Marcar apenas uma oval.

   - ◯ 1 - Discordo Totalmente
   - ◯ 2 - Discordo
   - ◯ 3 - Não discordo nem concordo
   - ◯ 4 - Concordo
   - ◯ 5 - Concordo Totalmente

10. 4 - Encontro-me familiarizado com as normas processuais da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime) e do Decreto-Lei n.º 78/87, de 17 de fevereiro (Código de Processo Penal) no que concerne à prova digital (Escala de Litker). *

Marcar apenas uma oval.

- ◯ 1 - Discordo Totalmente
- ◯ 2 - Discordo
- ◯ 3 - Não discordo nem concordo
- ◯ 4 - Concordo
- ◯ 5 - Concordo Totalmente

11. 5 - Considera que os conhecimentos mencionados na última questão são realmente importantes para o seu trabalho? Justifique. *

Recursos Tecnológicos e Humanos

Tempo em horas de execução de exames por NDF. Nota adicional: estes tempos foram calculados pela data/hora registada no início do exame e fim do exame do equipamento em concreto e inclui tempos de registos, tempos de pausa durante o exame, horário fora de trabalho (descanso), pesquisa de solução, incluindo ainda o cálculo da sobreposição de trabalho com exames de mais do que um dispositivo em simultâneo.

Tempo em horas de execução de exame (Média de todos os dispositivos/NDF/Ano)				
Núcleo Digital Forense (NDF)	2018	2019	2020	Média
SSC Beja	----	48,88	126,54	87,71
SSC Braga	----	79,33	62,16	70,745
SSC Castelo Branco	----	----	49,13	49,13
SSC Coimbra	74,42	56,89	64,68	65,33
DIC/DC	71,9	77,23	65,1	71,41
SSC Faro	23,23	92,42	86,19	67,28
SSC Leiria	----	59,83	67,08	63,455
SSC Portalegre	----	157,38	105,41	131,395
SSC Porto	14,07	89,91	96,1	66,69333333
SSC Santarém	----	189	69,51	129,255
SSC Setúbal	----	149,04	126,01	137,525
SSC Viana do Castelo	----	121,52	105,46	113,49
SSC Vila Real	----	55,32	80,89	68,105
SSC Viseu	----	103,19	142,44	122,815
UAF	71,83	93,03	120,22	95,02666667

12. 1 - Tem ao seu dispor o equipamento necessário para a realização do seu trabalho? Refira que outros equipamentos fariam falta. *

13. 2 - Tendo em conta a tabela anexa a esta secção de perguntas, considera que o seu NDF deveria ser reforçado a nível de recursos humanos? Refira outro tipo de reforço que seria conveniente que o seu NDF recebesse. *

Valoração da Prova Digital

14. 1 - O seu trabalho a nível da prova digital tem contribuído para a fase de inquérito dos processos judiciais? Tem tido informação sobre a utilidade desse contributo? *

Testemunho em Tribunal

15. 1 - Como membro do NDF, já teve que prestar declarações em tribunal? *

Marcar apenas uma oval.

- Sim
- Não

16. 2 - Se respondeu que sim na questão anterior, refira se prestou essas declarações como testemunha ou como perito.

Análise ao Trabalho dos NDF

17. 1 - Quando surge uma nova situação a nível da prova digital, existe uma partilha de informação com a estrutura de IC? *

18. 2 - E caso não tenha meios de resolver essa situação, qual é o procedimento a tomar? *

19. 3 - Aquando de um exame, já se deparou com técnicas anti-forenses? *

20. 4 - Desde que se encontra no NDF, já procedeu à apreensão de equipamentos? Se não, essa apreensão foi realizada por quem? E tais intervenientes tinham os conhecimentos mínimos para lidar com esses equipamentos? *

Comentários

26. Caso deseje, refira aqui nesta secção algo que considere que não foi abordado no questionário.

25/04/2021 Trabalho de Investigação Aplicada - Núcleo Digital Forense da Guarda Nacional Republicana

Fim do Questionário

Muito obrigado pelo seu tempo despendido.

Com os melhores cumprimentos,

José Miguel Armada de Matos
Aspirante de Infantaria da Guarda Nacional Republicana

Carregue em "Submeter" para finalizar o questionário.

APÊNDICE C – CARTA DE APRESENTAÇÃO

CARTA DE APRESENTAÇÃO

No último ano do Mestrado Integrado em Ciências Militares na Especialidade de Segurança, os alunos da Academia Militar elaboram um Trabalho de Investigação Aplicada, o qual é submetido à avaliação e posterior defesa pública perante um júri.

Assim, por me encontrar no último ano de formação na Academia Militar e na Escola da Guarda, com vista à obtenção do Grau de Mestre e no âmbito do Trabalho de Investigação Aplicada subordinado ao tema "Núcleo Digital Forense da Guarda Nacional Republicana", venho solicitar a colaboração de Vossa Excelência na realização de uma entrevista que me poderá proporcionar uma visão mais detalhada sobre o meu tema.

A presente investigação tem como principal objetivo efetuar um balanço, identificando os principais pontos fortes e as vulnerabilidades, do funcionamento dos Núcleos Digitais Forenses da Guarda Nacional Republicana (adiante NDF) localizados em diversos pontos do território português, focando-se em particular na formação dos militares, nos recursos tecnológicos que os mesmos dispõem, no tempo despendido em média nos exames relativos à prova digital, na sua admissão e valoração como meio de prova processual, nas maiores ameaças à sua admissibilidade e valoração enquanto prova e na eventual posterior participação dos militares no respetivo processo, nomeadamente como testemunhas ou como peritos.

De modo a garantir a recolha de informações de diversos especialistas e intervenientes sobre o tema em causa, surge a necessidade de realizar entrevistas. Desta forma, estas são realizadas a quem atue profissionalmente na área da investigação criminal e, mais concretamente, na investigação criminal que envolva prova digital.

Face ao exposto, solicito a Vossa Excelência que me conceda uma entrevista sobre o tema em apreço, uma vez que o seu contributo é fundamental para alcançar os objetivos propostos para a presente investigação.

Grato pela sua colaboração e disponibilidade.

Atenciosamente,

José Miguel Armada de Matos

Aspirante de Infantaria da Guarda Nacional Republicana

APÊNDICE D – INQUÉRITO POR ENTREVISTA AOS CHEFES DE SIIC COM NDF

1. Considera que as capacidades técnicas, conhecimentos e qualificações dos militares dos NDF, reveladas no seu contacto com estes militares, são adequadas para as competências que lhes são atribuídas em matéria de prova digital?

2. Considera que os militares dos NDF revelam, na sua atuação, possuir conhecimentos atualizados e aplicar os melhores métodos e boas práticas em matéria de prova digital?

3. Que capacidades dos militares dos NDF, a nível de conhecimentos teóricos e práticos, entende que deveriam ser melhoradas para um melhor desempenho em matéria de prova digital?

4. Considera que os militares dos NDF devem aprofundar os seus conhecimentos relativos às normas processuais da Lei do Cibercrime?

5. Quais os recursos tecnológicos que entende deverem passar a ser disponibilizados aos militares dos NDF para que estes possam relevar um melhor desempenho, em matéria de prova digital?

6. Considera que a prova digital é uma mais-valia para a fase de inquérito de um processo?

7. Considera que o trabalho realizado pelos militares dos NDF tem contribuído de forma eficaz para que a prova digital seja admitida e devidamente valorada em sede processual?

8. Considera que os relatórios de resultados da prova digital elaborados pelos militares dos NDF contribuem de forma eficaz para a admissibilidade e valoração da prova digital?

9. Os militares dos NDF são ouvidos em tribunal em aspetos relacionados com prova digital? Se sim, são ouvidos como peritos ou como testemunhas?

10. Quais são, no seu entender, as potencialidades dos NDF?

11. Quais são, no seu entender, os pontos fracos dos NDF?

12. Quais são, no seu entender, os aspetos relativos ao NDF nos quais a GNR poderá apostar para que estes sejam cada vez mais relevantes no tratamento da prova digital?

13. Quais são, no seu entender, as principais ameaças relativas à missão dos NDF?

14. As patrulhas do dispositivo territorial da GNR encontram-se sensibilizadas para a presença de prova digital num local de crime e sabem dar resposta ao manuseamento desta prova nessas circunstâncias?

15. Tendo em conta que o tempo médio dos exames (tempo das pendências) das provas digitais do NDF sob o seu comando é de X, considera que esse tempo causa problemas quanto à celeridade desejável da fase dos inquéritos onde se inserem esses exames?

16. Considerando que tem X militares no NDF sob o seu comando e que o tempo médio dos exames (tempo das pendências) das provas digitais entre 2018 e 2020 é de X, entende que este NDF deverá receber um reforço a nível de recursos humanos?

Agradeço a sua disponibilidade e colaboração.

José Miguel Armada de Matos

Aspirante de Infantaria da Guarda Nacional Republicana

APÊNDICE E – INQUÉRITO POR ENTREVISTA AOS CHEFES DE SIIC SEM NDF

1. Considera que as capacidades técnicas, conhecimentos e qualificações dos militares dos NDF, reveladas no seu contacto com estes militares, são adequadas para as competências que lhes são atribuídas em matéria de prova digital?

2. Considera que os militares dos NDF revelam, na sua atuação, possuir conhecimentos atualizados e aplicar os melhores métodos e boas práticas em matéria de prova digital?

3. Que capacidades dos militares dos NDF, a nível de conhecimentos teóricos e práticos, entende que deveriam ser melhoradas para um melhor desempenho em matéria de prova digital?

4. Considera que os militares dos NDF devem aprofundar os seus conhecimentos relativos às normas processuais da Lei do Cibercrime?

5. Quais os recursos tecnológicos que entende deverem passar a ser disponibilizados aos militares dos NDF para que estes possam relevar um melhor desempenho, em matéria de prova digital?

6. Considera que a prova digital é uma mais-valia para a fase de inquérito de um processo?

7. Considera que o trabalho realizado pelos militares dos NDF tem contribuído de forma eficaz para que a prova digital seja admitida e devidamente valorada em sede processual?

8. Considera que os relatórios de resultados da prova digital elaborados pelos militares dos NDF contribuem de forma eficaz para a admissibilidade e valoração da prova digital?

9. Os militares dos NDF são ouvidos em tribunal em aspetos relacionados com prova digital? Se sim, são ouvidos como peritos ou como testemunhas?

10. Quais são, no seu entender, as potencialidades dos NDF?

11. Quais são, no seu entender, os pontos fracos dos NDF?

12. Quais são, no seu entender, os aspetos relativos ao NDF nos quais a GNR poderá apostar para que estes sejam cada vez mais relevantes no tratamento da prova digital?

13. Quais são, no seu entender, as principais ameaças relativas à missão dos NDF?

14. As patrulhas do dispositivo territorial da GNR encontram-se sensibilizadas para a presença de prova digital num local de crime e sabem dar resposta ao manuseamento desta prova nessas circunstâncias?

15. Tendo em conta que não possui na sua dependência um NDF, no caso de existir uma situação que envolva prova digital, que NDF é que recebe esse processo?

16. Tendo em conta que o número de situações reportadas é de X, considera que deveria ser implementado um NDF neste Comando? Porquê?

Agradeço a sua disponibilidade e colaboração.

José Miguel Armada de Matos

Aspirante de Infantaria da Guarda Nacional Republicana

APÊNDICE F – INQUÉRITO POR ENTREVISTA AOS PROCURADORES DO MP

1. Considera que as capacidades técnicas, conhecimentos e qualificações dos militares dos NDF, reveladas no seu contacto com estes militares, são adequadas para as competências que lhes são atribuídas em matéria de prova digital?

2. Considera que os militares dos NDF revelam, na sua atuação, possuir conhecimentos atualizados e aplicar os melhores métodos e boas práticas em matéria de prova digital?

3. Que capacidades dos militares dos NDF, a nível de conhecimentos teóricos e práticos, entende que deveriam ser melhoradas para um melhor desempenho em matéria de prova digital?

4. Considera que os militares dos NDF devem aprofundar os seus conhecimentos relativos às normas processuais da Lei do Cibercrime?

5. Quais os recursos tecnológicos que entende deverem passar a ser disponibilizados aos militares dos NDF para que estes possam relevar um melhor desempenho, em matéria de prova digital?

6. Considera que a prova digital é uma mais-valia para a fase de inquérito de um processo?

7. Considera que o trabalho realizado pelos militares dos NDF tem contribuído de forma eficaz para que a prova digital seja admitida e devidamente valorada em sede processual?

8. Considera que os relatórios de resultados da prova digital elaborados pelos militares dos NDF contribuem de forma eficaz para a admissibilidade e valoração da prova digital?

9. Os militares dos NDF são ouvidos em tribunal em aspetos relacionados com prova digital? Se sim, são ouvidos como peritos ou como testemunhas?

10. Quais são, no seu entender, as potencialidades dos NDF?

11. Quais são, no seu entender, os pontos fracos dos NDF?

12. Quais são, no seu entender, os aspetos relativos ao NDF nos quais a GNR poderá apostar para que estes sejam cada vez mais relevantes no tratamento da prova digital?

13. Quais são, no seu entender, as principais ameaças relativas à missão dos NDF?

14. Aquando da necessidade da realização de exames forenses relativos à prova digital, já contou com o apoio da IC da GNR? Quão eficaz foi esse contributo?

15. Tendo em conta que o tempo médio dos exames (tempo das pendências) das provas digitais do NDF da sua área é de X, considera que esse tempo causa problemas quanto à celeridade desejável da fase dos inquéritos onde se inserem esses exames?

Agradeço a sua disponibilidade e colaboração.

José Miguel Armada de Matos

Aspirante de Infantaria da Guarda Nacional Republicana

APÊNDICE G – DECLARAÇÃO DE CONSENTIMENTO

DECLARAÇÃO DE CONSENTIMENTO

Eu, abaixo assinado, _____,
declaro que decido participar de forma voluntária nesta investigação em curso e que me foi explicado o enquadramento e os objetivos a que esta se destina.

Reitero, também, que me foi dada a possibilidade de colocar qualquer questão sobre a investigação e de recusar a resposta a qualquer pergunta que me for dirigida.

Consinto que esta entrevista seja gravada, na condição de, caso o entenda, me ser facultada a transcrição da mesma, bem como o trabalho final, assim que este tiver sido aprovado e caso não tenha acesso restrito.

Permito ainda que as minhas respostas sejam utilizadas e analisadas com o fim de atingir os objetivos da presente investigação.

O Investigador

_____

_____

O/A Entrevistado/a

_____

_____