ACADEMIA MILITAR

AS TECNOLOGIAS DE INFORMAÇÃO NA ESTRUTURA DE INVESTIGAÇÃO CRIMINAL DAS UNIDADES TERRITORIAIS DA GUARDA NACIONAL REPUBLICANA

Autor: Aspirante de Infantaria da GNR Amílcar da Cunha Pereira

Orientador: Tenente-Coronel de Infantaria da GNR António Duarte Rodrigues Lobo de Carvalho

Coorientador: Capitão de Administração da GNR Luís Carlos Rodrigues Malheiro

Mestrado Integrado em Ciências Militares, na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, maio de 2020

ACADEMIA MILITAR

AS TECNOLOGIAS DE INFORMAÇÃO NA ESTRUTURA DE INVESTIGAÇÃO CRIMINAL DAS UNIDADES TERRITORIAIS DA GUARDA NACIONAL REPUBLICANA

Autor: Aspirante de Infantaria da GNR Amílcar da Cunha Pereira

Orientador: Tenente-Coronel de Infantaria da GNR António Duarte Rodrigues Lobo de Carvalho

Coorientador: Capitão de Administração da GNR Luís Carlos Rodrigues Malheiro

Mestrado Integrado em Ciências Militares, na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, maio de 2020

EPÍGRAFE

"Progress is impossible without change, and those who cannot change their minds cannot change anything."

George Bernard Shaw

DEDICATÓRIA

Aos meus pais e ao meu irmão,

Obrigado por tudo. A caminhada não é minha, é nossa!

AGRADECIMENTOS

O presente Relatório Científico Final do Trabalho de Investigação Aplicada espelha o contributo de diversas pessoas que materializaram um alicerce imprescindível para a sua elaboração. Neste sentido, quero deixar-lhes um agradecimento especial e profundo. Porém, pelo apoio e contributo direto nesta investigação, importa nomear as seguintes:

Ao meu orientador, Tenente-Coronel Lobo de Carvalho, agradeço pela permanente disponibilidade, compreensão, dedicação e entrega na orientação e apoio à realização da presente investigação, bem como por todos os conhecimentos transmitidos sobre as Informações, a Investigação Criminal e os Sistemas e Tecnologias de Informação. Apesar desta fase difícil e com grandes constrangimentos a nível profissional e pessoal, esteve sempre disponível para me aconselhar e transmitir os seus conhecimentos e experiência.

Ao meu coorientador, Capitão Luís Malheiro, pelo seu compromisso, prontidão e rigor ao longo de toda esta etapa. Agradeço por, em todos os momentos, estar totalmente disponível para me acompanhar, aconselhar, dirimir todas as questões e transmitir os seus conhecimentos, que foram fundamentais para o desenvolvimento desta investigação.

A todos os entrevistados, um agradecimento pela disponibilidade e prontidão para colaborar na presente investigação, bem como pelo seu aconselhamento profissional e pessoal fora do contexto das entrevistas.

Aos meus camaradas do XXV Curso de Formação de Oficiais da Guarda Nacional Republicana, pela camaradagem, espírito de corpo, entrega e união, assim como pelo apoio em todas as experiências e dificuldades ultrapassadas.

Aos meus pais e ao meu irmão, a quem tudo devo, pelo apoio incondicional ao longo de toda a minha vida, por estarem sempre presentes para me apoiar, aconselhar e por serem a minha referência e orgulho. Sem eles, os meus sonhos não passariam dessa condição!

À minha família, em especial à minha tia Cristina e ao meu tio Amílcar, pela referência enquanto pessoas e enquanto profissionais, que sempre estiveram presentes com os melhores conselhos, dedicação e que sempre me apoiaram em tudo, com tudo e para tudo.

Por fim, à Sofia, quero deixar uma palavra especial de grande agradecimento e amor. Por todo o companheirismo, cumplicidade, motivação, carinho e por todo o apoio incondicional, sempre ao meu lado.

A todos, o meu profundo e sincero Obrigado!

RESUMO

A presente investigação, subordinada ao tema "As Tecnologias de Informação na estrutura de Investigação Criminal das Unidades Territoriais da Guarda Nacional Republicana", tem como objetivo central analisar os principais contributos da utilização das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da Guarda Nacional Republicana.

Neste sentido, revela-se pertinente analisar as principais Tecnologias e Sistemas de Informação utilizados pelas Unidades Territoriais na resposta aos fenómenos criminais, bem como as potencialidades que lhes estão subjacentes e, por conseguinte, caracterizar as melhorias essenciais a implementar. Para tal, foi seguida uma metodologia assente no modelo hipotético-dedutivo, com recurso a entrevistas exploratórias e consequente elaboração de hipóteses, verificadas através de entrevistas confirmatórias.

Concluída a investigação, é notório que as Tecnologias de Informação materializam um pilar fundamental na atividade de Investigação Criminal. Através destas, a recolha, avaliação, tratamento, análise e difusão das informações traduzem um mecanismo integrador das estratégias de prevenção e Investigação Criminal. Em consequência dos novos ângulos de atuação criminais proporcionados pelas tecnologias, urge a necessidade de antecipação, acompanhamento e adaptação a estes fenómenos, o que exige permanente especialização técnica e científica dos recursos tecnológicos e humanos. Apesar da necessidade de reforço e investimento em ferramentas tecnológicas proporcionais às novas formas de manifestação da criminalidade, o recurso a estas não representa um fim em si mesmo, mas um suporte ao processo de tomada de decisão, no qual o elemento humano é central.

Palavras-chave: Informação; Investigação Criminal; Sistemas de Informação; Tecnologias de Informação; Unidades Territoriais.

ABSTRACT

The present work, entitled "Information Technologies in Criminal Investigation structure of Guarda Nacional Republicana Territorial Units", has the main goal to analyze the major inputs of the use of Information Technologies to enhance the operational organ's efficiency of Criminal Investigation structure of Guarda Nacional Republicana Territorial Units.

In this regard, it is relevant to describe the principal Technologies and Information Systems used by Territorial Units in response to criminal phenomena, as well as the advantages and disadvantages which underlie them and, consequently, to characterize the essential improvements to be implemented. To achieve these goals, a methodology based on the hypothetical-deductive model was followed, using exploratory interviews and consequent elaboration of hypothesis, verified through confirmatory interviews.

Once the research is concluded, it is evident that, increasingly, Information Technologies materialize a key pillar in the Criminal Investigation activity. Through these, the collection, evaluation, treatment, analysis and dissemination of information represents an integrating mechanism for prevention and Criminal Investigation strategies. As a result of the new criminal approaches provided by technologies, there is an urgent need for anticipation, monitoring and adaptation to these phenomena, which requires permanent technical and scientific specialization of resources, both technological and human. However, it was found that, despite the need for reinforcement and investment in technological tools proportional to the emerging criminal nature, this investment does not represent an end, but rather a support to be decision-making processes, in which the human element plays the key role.

Keywords: Information; Criminal Investigation; Information Systems; Information Technologies; Territorial Units.

ÍNDICE GERAL

ÍNDICE DE FIGURAS

ÍNDICE DE QUADROS

ÍNDICE DE TABELAS

LISTA DE APÊNDICES E ANEXOS

APÊNDICES

ANEXOS

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AFIS	*Automated Fingerprint Identification System*
AJ	Autoridade Judiciária
al.	Alínea
AM	Academia Militar
AMA	Agência para a Modernização Administrativa
ANSR	Autoridade Nacional de Segurança Rodoviária
AP	Administração Pública
APA	*American Psychological Association*
ArcGIS	*Aeronautical Reconnaissance Coverage Geographic Information System*
Art.º	Artigo
ASAE	Autoridade de Segurança Alimentar e Económica
BEAV	Boletim Estatístico de Acidentes de Viação
CCCO	Centro de Comando e Controlo Operacional
Cf.	Conforme
CFSIIC	Conselho de Fiscalização do Sistema Integrado de Informação Criminal
CIG	Centro de Informações da Guarda
CNPD	Comissão Nacional de Proteção de Dados
CO	Comando Operacional
COSI	Centro de Operações de Segurança Informática
CP	Código Penal
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
CSIRT	*Computer Security Incident Response Team*
CTer	Comando Territorial
CTIC	Conselho para as Tecnologias de Informação e Comunicação
DCSI	Direção de Comunicações e Sistemas de Informação
DI	Direção de Informações
DIC	Direção de Investigação Criminal
DIKI	*Data-Information-Knowledge-Intelligence*

DR	Decreto Regulamentar
DTer	Destacamento Territorial
DVI	*Disaster Victim Identification*
EUROPOL	Agência da União Europeia para a Cooperação Policial
FSS	Forças e Serviços de Segurança
GA-PIIC	Grupo de Acompanhamento da Plataforma para o Intercâmbio de Informação Criminal
GNR	Guarda Nacional Republicana
GPTIC	Grupo de Projeto para as Tecnologias de Informação e Comunicação
GTTSI	Grupo de Trabalho para as Tecnologias de Sistemas de Informação
H	Hipótese Derivada
HPP	Hipótese da Pergunta de Partida
HUMINT	*Human Intelligence*
IALEIA	*International Association of Law Enforcement Intelligence Analysts*
IBM	*International Business Machines Corporation*
IC	Investigação Criminal
INFOSEC	*Information Security*
LISIOPC	Lei da Interoperabilidade entre Sistemas de Informação dos Órgãos de Polícia Criminal
LMS	*Learning Management System*
LOGNR	Lei Orgânica da Guarda Nacional Republicana
LOIC	Lei de Organização da Investigação Criminal
LPC	Lei de Política Criminal
LPIEFSS	Lei de Programação de Infraestruturas e Equipamentos das Forças e Serviços de Segurança
LSI	Lei de Segurança Interna
MAI	Ministério da Administração Interna
Maj	Major
MP	Ministério Público
n.º	Número
NAIIC	Núcleo de Análise de Informações e Informação Criminal
NAO	Núcleo de Apoio Operativo
NAT	Núcleo de Apoio Técnico

NDF	Núcleo Digital Forense
NEP	Norma de Execução Permanente
NIAVE	Núcleo de Investigação e de Apoio a Vítimas Específicas
NIC	Núcleo de Investigação Criminal
NICAV	Núcleo de Investigação de Crimes em Acidentes de Viação
NICCOA	Núcleo de Investigação de Crimes e Contra-Ordenações Ambientais
NTP	Núcleo Técnico-Pericial
NUIPC	Número Único Identificador de Processo Crime
OE	Objetivo Específico
OG	Objetivo Geral
OLAP	*Online Analytical Processing*
OPC	Órgão de Polícia Criminal
OSCE	*Organization for Security and Cooperation in Europe*
OSINF	*Open Source Information*
OSINT	*Open Source Intelligence*
OTAN	Organização do Tratado do Atlântico Norte
PARR	Projeto de Atualização das Redes Rádio
PCCCOFSS	Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança
PCM	Presidência do Conselho de Ministros
PD	Pergunta Derivada
PGETIC	Plano Global Estratégico para a Racionalização e Redução de Custos com as Tecnologias de Informação e Comunicação
PIGO	Plataforma de Integração e Gestão Operacional
PIIC	Plataforma para o Intercâmbio de Informação Criminal
PJ	Polícia Judiciária
PM	Polícia Marítima
PMDGNR	Patrulhamento Móvel Digital - Guarda Nacional Republicana
PP	Pergunta de Partida
PSP	Polícia de Segurança Pública
PUC-CPI	Ponto Único de Contacto para a Cooperação Policial Internacional
QGIS	*Quantum Geographic Information System*
RAIC	Repartição de Análise de Informação Criminal

RAICO	Relatórios de Análise de Informação Criminal – Operacional
RASI	Relatório Anual de Segurança Interna
RCFTIA	Relatório Científico Final do Trabalho de Investigação Aplicada
RGSGNR	Regulamento Geral do Serviço da Guarda Nacional Republicana
RNSI	Rede Nacional de Segurança Interna
SAMA	Sistema de Apoio à Modernização e Capacitação da Administração Pública
SARS-Cov-2	*Severe Acute Respiratory Syndrome-Coronavirus-2*
SCoT	Sistema de Contraordenações do Trânsito
SEF	Serviço de Estrangeiros e Fronteiras
SEG2APIC	Sistema Estratégico de Gestão e Apoio da Atividade Policial e Informação Criminal
SEPNA	Serviço de Proteção da Natureza e do Ambiente
SG2S	Sistema de Gestão de Salas de Situação
SGSSI	Secretário-Geral do Sistema de Segurança Interna
SI	Sistemas de Informação
SIED	Serviço de Informações Estratégicas de Defesa
SIG-GNR	Sistema de Informação Geográfica da Guarda Nacional Republicana
SIGRI	Sistema Integrado de Gestão de Recursos Internos
SIG-SIRESP	Sistema de Informação Geográfica - Sistema Integrado de Redes de Emergência e Segurança de Portugal
SIIC	Secção de Informações e Investigação Criminal
SIIOP	Sistema Integrado de Informações Operacionais de Polícia
SIIOP-2S	Sistema Integrado de Informações Operacionais de Polícia - Salas de Situação
SIIOP-A	Sistema Integrado de Informações Operacionais de Polícia – Ambiente
SIIOP-D	Sistema Integrado de Informações Operacionais de Polícia – Documental
SIIOP-F	Sistema Integrado de Informações Operacionais de Polícia - Fiscal
SIIOP-G	Sistema Integrado de Informações Operacionais de Polícia – Georreferenciação
SIIOP-O	Sistema Integrado de Informações Operacionais de Polícia - Ocorrências
SIIOP-P	Sistema Integrado de Informações Operacionais de Polícia – Principal
SIIOP-T	Sistema Integrado de Informações Operacionais de Polícia – Trânsito

SIRESP	Sistema Integrado de Redes de Emergência e Segurança de Portugal
SIS	Sistema de Informação *Schengen*
SPD	*Seattle Police Department*
SSI	Sistema de Segurança Interna
STM	Sistema de Transmissão de Mensagens
TI	Tecnologias de Informação
TIA	Trabalho de Investigação Aplicada
TIC	Tecnologias de Informação e Comunicação
UAF	Unidade de Ação Fiscal
UEn	Unidade de Enumeração
UFED	*Universal Forensics Extraction Device*
UNODC	*United Nations Office on Drugs and Crime*
UR	Unidade de Registo
VOIP	*Voice Over Internet Protocol*
ZA	Zona de Ação

INTRODUÇÃO

O presente Relatório Científico Final do Trabalho de Investigação Aplicada (RCFTIA) é desenvolvido no domínio do Mestrado Integrado em Ciências Militares, na especialidade de Segurança, materializando a fase final do ciclo de estudos dos alunos da Academia Militar (AM) (Academia Militar [AM], 2016). Pelo que antecede, o Trabalho de Investigação Aplicada (TIA) apresentado está subordinado ao tema: "As Tecnologias de Informação na estrutura de Investigação Criminal das Unidades Territoriais da Guarda Nacional Republicana".

Uma vez que os instrumentos tecnológicos estão enraizados, cada vez mais, na estrutura, cultura, procedimentos e intervenção das organizações, converteram-se em "necessidades naturais e intrínsecas às mesmas" (Rascão, 2008, p. 97). Deste modo, a escolha e edificação do tema[1] decorre da crescente necessidade de recurso às Tecnologias de Informação (TI) na previsão, adaptação e resposta às exigências criminais atuais.

Assim, a utilização progressiva das ferramentas tecnológicas, ainda designadas como "novas" fruto da sua constante evolução, produz efeitos em múltiplas dimensões, desde logo, no que diz respeito à informação. Uma das principais consequências do uso das TI prende-se com o aumento não só da quantidade, como da qualidade da informação (Castro, 2018).

As informações desempenham um papel decisivo para a eficácia operacional das estruturas de Investigação Criminal (IC)[2] na antecipação e combate aos fenómenos criminais (Soares, 2014) até porque, "sem informações, a Polícia é cega, logo inoperante" (Clemente, 2007, p. 394). Por um lado, possibilitam "a apresentação da prova imprescindível para confirmar ou infirmar a prática de um facto ilícito" e, por outro lado, constitui facto gerador da prevenção criminal (Sousa, 2007, p. 225). Neste sentido, dado que um dos principais desafios que se coloca é "compreender em que consiste a informação, como se gere, interpreta e que decisão(ões) permite tomar" (Rascão, 2008, p. 66), a recolha, tratamento, análise e difusão da informação recorrendo a TI, traduz um mecanismo diferenciador nas estratégias de prevenção e IC (Lopes, 2017).

[1] O tema é o assunto que se pretende estudar e pesquisar. A escolha de um tema compreende a seleção de um assunto segundo "as inclinações, as possibilidades, as aptidões e as tendências" do autor do trabalho científico (Vilelas, 2017, p. 79).

[2] A IC constitui uma das principais áreas para as quais concorre a missão atribuída à Guarda Nacional Republicana (GNR), conforme (Cf.) o disposto na alínea (al.) f) do número (n.º) 1 do artigo (art.º) 6.º do Regulamento Geral do Serviço da GNR (RGSGNR).

Por consequência, um dos princípios orientadores da presente investigação é o de que "se o crime evolui, a resposta ao crime deve evoluir" (Valente, 2019, p. 67). Assim, face ao desenvolvimento de uma criminalidade "cujo perfil assume inúmeras formas de manifestação" (Santos, 2015, p. 39), o acompanhamento, adaptação e inovação dos recursos tecnológicos configura uma exigência atual da IC (Agência da União Europeia para a Cooperação Policial [EUROPOL], 2002), sob pena da sua obsolescência para uma resposta eficaz, pronta e oportuna às novas formas de atuação criminal (Bose & Kabir, 2017).

É a partir do conhecimento da natureza e da evolução da criminalidade, que serão definidas as estratégias para a prevenção e combate aos fenómenos criminais (Braz, 2016). Consequentemente, a informação, "uma vez sujeita a um processo de tratamento sistemático através de sistemas centralizados" (Braz, 2020, p. 70), designadamente, Sistemas e TI que assegurem a sua recolha, avaliação, tratamento, análise e disseminação, em tempo útil, torna-se em conhecimento da criminalidade (Braz, 2020).

Todavia, tal como previsto no Relatório Anual de Segurança Interna (RASI) de 2018, o investimento e reforço das Forças e Serviços de Segurança (FSS) com novas ferramentas tecnológicas para o aumento da eficácia e eficiência da atividade operacional, deve ser acompanhado pela valorização dos recursos humanos (Sistema de Segurança Interna [SSI], 2019). Apesar do recurso às TI se traduzir em vantagens significativas na intervenção operacional das estruturas de IC, importa sublinhar, desde logo que, por si sós, não são suficientes para melhorar o desempenho operacional na redução da criminalidade (Koper, Lum & Willis, 2014). Deste modo, as dificuldades investigatórias deverão ser superadas com base num estreito vínculo entre os recursos tecnológicos e humanos (Carvalho, 2010).

Adicionalmente, acresce considerar que, a presente investigação enquadra o recurso às TI subjacente ao período entre 2015 até à atualidade, a fim de abordar os principais recursos tecnológicos e respetivas ferramentas atualmente empregues.

Por sua vez, dado que "a melhor forma de começar um trabalho de investigação consiste em (…) enunciar o projeto sob a forma de uma pergunta de partida" (Quivy & Campenhoudt, 2017, p. 44), foi definida a seguinte: "Quais os principais contributos das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da GNR?".

A Pergunta de Partida (PP) enunciada concorre para o Objetivo Geral (OG) da investigação (Fortin, Côté & Filion, 2009), traduzindo-se em "Analisar os principais contributos da utilização das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da

GNR". Por conseguinte, a fim de desagregar o OG em "aspetos mais restritos e elementares", de modo a conhecer o grau de cumprimento do OG (Santos & Lima, 2019, p. 58), delinearam-se como Objetivos Específicos (OE) os seguintes: OE1 – Descrever a função das Informações Criminais na resposta aos fenómenos criminais; OE2 – Caracterizar as principais Tecnologias e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades Territoriais da GNR; OE3 – Identificar os pontos fortes e as debilidades subjacentes à estrutura e funcionamento dos Sistemas e Tecnologias de Informação na estrutura de Investigação Criminal das Unidades Territoriais da GNR; e, OE4 – Identificar as melhorias a implementar nos Sistemas e Tecnologias de Informação para reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR.

No cumprimento dos objetivos propostos, o RCFTIA foi desenvolvido em conformidade com a Norma de Execução Permanente (NEP) n.º 522/1.ª, de 20 de janeiro de 2016 (AM, 2016), suportando os critérios omissos na 7.ª edição *American Psychological Association* (APA, 2019). No que concerne à sua estrutura, a presente investigação encontra-se dividida em cinco capítulos fundamentais.

No primeiro capítulo, é realizado um enquadramento concetual da IC e da estrutura orgânica da vertente de IC ao nível dos Comandos Territoriais (CTer) e do Comando Operacional (CO). Este capítulo visa, de igual modo, analisar o regime jurídico subjacente à IC e caracterizar as suas vertentes funcionais. Posteriormente, no segundo capítulo, é elaborado o enquadramento concetual das Informações, a sua caracterização e articulação, a fim de compreender as suas diversas dimensões e a importância da sua utilização para a atividade operacional. Por sua vez, no terceiro capítulo, é realizada uma abordagem concetual aos Sistemas de Informação (SI) e TI. Complementarmente, é analisada a importância dos SI para a cooperação e interoperabilidade, bem como para a atividade operacional da GNR e, por fim, caracterizadas as principais TI utilizadas pela IC.

Relativamente ao quarto capítulo, é apresentado o trajeto metodológico adotado na presente investigação, nomeadamente, a delimitação dos objetivos, o modelo de análise, os métodos e procedimentos metodológicos e as técnicas de recolha, tratamento e análise dos dados. Quanto ao quinto e último capítulo, são apresentados os dados recolhidos nas entrevistas exploratórias e entrevistas confirmatórias para a subsequente análise e discussão verificando, por fim, as hipóteses de investigação formuladas.

Na fase final da investigação desenvolvida, são apresentadas as conclusões juntamente com algumas recomendações e propostas para futuras investigações.

CAPÍTULO 1
A INVESTIGAÇÃO CRIMINAL

1.1. Enquadramento concetual

O vocábulo Investigação provém do latim "*investigatione*" (*in+vestigius+actio*), que compreende a ação orientada para o rasto, para a pegada e que conduziu à tradução de "ato de pesquisar, de indagar, de investigar" (Valente, 2019, p. 471). Remetemos, portanto, para o conceito de investigar enquanto "olhar inquiridor sobre os vestígios deixados e os rastos não apagados" de um determinado acontecimento ou facto, com o fim de atingir o conhecimento, uma verdade (Valente, 2019, p. 472).

É, precisamente, a partir dessa reciprocidade, que emerge o Princípio das Trocas, de *Edmond Locard* (Thompson, 2018). Este princípio postula que, num prisma dinâmico e numa lógica de correlação causa/efeito, "o autor do crime leva, consigo, algo da vítima e/ou do local onde agiu, e dos instrumentos e objetos que utilizou, e deixa nestes, algo de si mesmo" (Braz, 2016, p. 112).

Assim, a IC, de um ponto de vista clássico, tem como finalidade a localização, recolha, conservação, exame e interpretação das provas que nos encaminhem à explicação e demonstração da verdade material dos factos que traduzem a consumação de um determinado ilícito criminal (Lopes, 2017). Porém, não se deve prender só aos fins probatórios descritos, mas também, com todas as provas que possam "corroborar a tese da inocência" (Valente, 2019, p. 491). Uma estrutura eficaz de IC requer estratégia e planeamento (Paiva, 2019). O seu objeto versa não só sobre os factos (ações ou omissões), como sobre o comportamento humano que esteve na sua origem, o que a torna "um processo padronizado e sistemático destinado a atingir o conhecimento" (Mannheim, 1984, p. 118).

Por sua vez, Paulsen e Robinson (2009) defendem que, a interpretação do crime exige a integração de quatro elementos mínimos: a lei, que estabelece quais os comportamentos que consubstanciam o crime; o criminoso, enquanto indivíduo que viola as normas legais; o alvo, seja pessoa ou objeto, sobre o qual o autor do crime atua e, por fim, o local, isto é, a localização espaço-temporal, na qual as três dimensões suprarreferidas se cruzam e se desenvolve o evento criminal. Neste sentido, a IC estrutura e desenvolve um conjunto de princípios, regras e procedimentos próprios, isto é, um "sistema operativo", a partir do qual

é prosseguida a sua atividade, tendo por base três pilares fundamentais: o método, a informação e a cooperação (Braz, 2020, p. 62).

Por um lado, o método traduz as normas básicas e os instrumentos de raciocínio sobre os quais assentam as finalidades da IC, possibilitando a interpretação, ordenação e valorização da informação que possuímos, a fim de obter a que necessitamos, produzindo conhecimento (Hess, 2017). Por seu turno, a informação, enquanto base do conhecimento da criminalidade, pode ter como origem fontes pessoais, documentais ou organizacionais, formais e informais, internas e externas, abertas e fechadas, entre outras (Sintra, 2010). Por outro lado, no que concerne ao terceiro pilar, a cooperação, assenta na ideia de reciprocidade, permitindo a partilha de informação e de experiências (United Nations Office on Drugs and Crime [UNODC], 2010). A cooperação materializa-se, por exemplo, através da criação de Equipas Mistas e Conjuntas[3] que atuam num quadro de resposta operacional a novos desafios criminais (Braz, 2020). De acordo com o RASI de 2015, a estruturação, desenvolvimento e manutenção de Equipas Mistas de Prevenção Criminal representa uma mais-valia à cooperação institucional e à otimização da partilha de informações entre as FSS (SSI, 2016).

Em termos práticos, segundo Soares (2014), é bastante ténue a linha que divide a prevenção criminal, enquanto conjunto de medidas com a finalidade de evitar a criminalidade, da repressão criminal, que abrange, além da proibição do crime, uma resposta atual à sua consumação. Tal como refere Clemente (2006, p. 78), a IC cumpre, num Estado de Direito, um "papel central no processo penal e, logo, promove a prevenção criminal".

De acordo com o n.º 2 do art.º 2.º da Decisão 2009/902/JAI do Conselho da União Europeia, de 30 de novembro de 2009, a prevenção da criminalidade integra o conjunto de medidas que visam diminuir ou contribuir para a diminuição da criminalidade e do sentimento de insegurança, seja por intermédio de medidas diretas de dissuasão da prática de crimes, seja mediante políticas e ações orientadas para a minimização dos fatores que estimulam as causas da criminalidade (Conselho da União Europeia, 2009).

Por conseguinte, uma vez que a prevenção criminal consiste, sobretudo, numa investigação de recolha de informações (UNODC, 2010), "a mesma deve ser efetuada em coordenação com as demais Forças e Serviços de Segurança" (Valente, 2019, p. 557), a fim

[3] As Equipas Mistas decorrem da coordenação de elementos de diversos OPC, sendo constituídas em casos de investigações relativas a crimes violentos e graves, ao abrigo do art.º 15.º da Lei n.º 96/2017, de 23 de agosto (Lei de Política Criminal (LPC) - Biénio de 2017 – 2019). Por sua vez, uma Equipa de Investigação Conjunta compreende "um instrumento de cooperação internacional assente num acordo entre autoridades competentes", quer a nível judicial, quer no âmbito da aplicação da lei, entre dois ou mais Estados, por um período limitado e com um objetivo estabelecido, de modo a prosseguir investigações penais num ou mais Estados (Conselho da União Europeia, 2017, p. 4).

de serem adotadas as "medidas adequadas para certas infrações de natureza criminal" (Canotilho & Moreira, 2010, p. 861). Atendendo à Lei Orgânica da Guarda Nacional Republicana (LOGNR)[4], podemos aferir preceitos que estão enquadrados no plano da prevenção criminal, nomeadamente as alíneas c), d), e) e m) do n.º 1 e as alíneas a), d) e j) do n.º 2, ambos do art.º 3.º da LOGNR.

Com efeito, o principal desafio que se coloca à IC, segundo Braz (2020), é o da eficiência[5]. Assim, a IC "quer-se científica, metódica e integrante" (Valente, 2017, pp. 473-474), o que exige especialização, trabalho em equipa, treino, formação e recurso a equipamentos e meios tecnológicos sofisticados (Braz, 2020), enquanto "contributos para uma maximização operacional" (Pereira, 2012, p. 241).

1.2. A estrutura de Investigação Criminal dos Comandos Territoriais da GNR

A GNR[6] é uma "força de segurança de natureza militar, constituída por militares organizados num corpo especial de tropas e dotada de autonomia administrativa" (Assembleia da República [AR], 2007, p. 8043)[7].

Para cumprimento da sua missão[8], as atribuições da GNR são desenvolvidas na totalidade do território nacional e mar territorial (n.º 1 do art.º 5.º da LOGNR). Atendendo à Componente Territorial da Guarda, a sua estrutura é materializada pela ocupação do território por Unidades, designadamente as Territoriais (CTer)[9], responsáveis pela prossecução da missão da Guarda na respetiva área de responsabilidade, sob dependência direta do Comandante-Geral (n.º 1 do art.º 37.º da LOGNR).

Nesta senda, os CTer articulam-se em comando, serviços e subunidades operacionais (Destacamentos Territoriais, de Trânsito e de Intervenção)[10]. No que concerne ao serviço de IC, a prossecução das tarefas de segundo nível compete aos órgãos de IC das Unidades e da Direção de Investigação Criminal (DIC)[11], responsável por apoiar tecnicamente as Unidades[12].

[4] Lei n.º 63/2007, de 6 de novembro.
[5] A eficiência compreende a "medida do nível de utilização dos recursos", ou seja, alcançar os objetivos/finalidades com o menor número de recursos possível (Rosado, 2015, p. 194).
[6] Adiante designada por Guarda ou GNR - Consultar organograma da GNR no Anexo A.
[7] Cf. n.º 1 do art.º 1.º da LOGNR.
[8] Cf. n.º 2 do art.º 1.º da LOGNR.
[9] Cf. al. b) do art.º 20.º e al. b) do n.º 1 do art.º 22.º, ambos da LOGNR.
[10] Cf. art.º 38.º e n.º 1 do art.º 39.º da LOGNR; e n.º 1 do art.º 2.º conjugado com o n.º 1 do art.º 3.º, ambos da Portaria n.º 1450/2008, de 16 de dezembro.
[11] Cf. n.º 3 do art.º 193.º do RGSGNR.
[12] Cf. Despacho n.º 18/14 – OG, de 11 de março de 2014.

De acordo com o Despacho n.º 18/14 – OG, o comando da valência de IC dos CTer está atribuído às Secções de Informações e Investigação Criminal (SIIC)[13]. Uma vez que a atividade de IC na GNR se encontra alicerçada em três pilares fundamentais (IC - Operativa, IC - Criminalística e IC - Análise de informação criminal), as SIIC asseguram o desempenho das funções de IC mediante a articulação da sua estrutura nos seguintes órgãos centrais: a Subsecção de Análise e de Investigação Criminal, a Subsecção de Criminalística e o Núcleo de Investigação Criminal (NIC) do Destacamento Territorial (DTer). No caso das SIIC Tipo I[14], a sua estrutura estabelece a existência de um NIC na dependência direta da SIIC, sendo eventual no caso das SIIC Tipo II/III[15].

Sob dependência da SIIC apresentam-se, igualmente, o Núcleo de Investigação de Crimes em Acidentes de Viação (NICAV), o Serviço de Proteção da Natureza e do Ambiente (SEPNA) e o Núcleo de Investigação de Crimes e Contra-Ordenações Ambientais (NICCOA), conforme o Despacho n.º 18/14 – OG.

1.3. A estrutura do Comando Operacional: Da Investigação Criminal às Tecnologias de Informação

De acordo com o n.º 1 do art.º 21.º da LOGNR, a estrutura de comando da GNR compreende o Comando da Guarda e os Órgãos Superiores de Comando e Direção. O CO, enquanto Órgão Superior de Comando e Direção, é responsável por assegurar o comando de toda a atividade operacional da Guarda, exercendo comando direto, para fins operacionais, sobre as Unidades Territoriais, conforme o n.º 1 e n.º 4 do art.º 32.º da LOGNR.

Ao serviço da IC, o CO exerce, essencialmente, tarefas do terceiro nível[16], pela DIC, no que concerne a "atividades de prospeção, de controlo, de propostas de doutrina e de relacionamento com outras entidades e organismos" (Ministério da Administração Interna [MAI], 2010, p. 33884)[17].

Assegurando o apoio das Unidades Territoriais em diferentes áreas, nomeadamente, ao nível das informações e da IC (n.º 3 do art.º 32.º da LOGNR), a estrutura do CO

[13] Atendendo à Diretiva Operacional n.º 01/14, de 14 de abril de 2014, do CO, verificamos que, as SIIC materializam o centro de gravidade de toda a IC das Unidades Territoriais, com alteração na lógica de funcionamento da IC (dos DTer para os CTer), a fim de reforçar a coordenação da rede de Informações da Guarda e, sobretudo, operacionalizar as sinergias entre as atividades de IC e as informações policiais.
[14] Cf. Informação n.º 05/CO/14, de 20 de março de 2014, do CO. Consultar estrutura da SIIC Tipo I no Anexo B.
[15] Cf. Anexo C – Organograma da SIIC do CTer Tipo II/III.
[16] Tendo em atenção, igualmente, o exercício de tarefas de segundo nível prosseguidas pela DIC, segundo o n.º 3 do art.º 193.º do RGSGNR.
[17] Cf. n.º 4 do art.º 193.º do RGSGNR.

compreende cinco unidades orgânicas nucleares, entre as quais se destacam, na presente investigação: a Direção de Informações (DI)[18], a DIC[19] e a Direção de Comunicações e Sistemas de Informação (DCSI)[20], previsto no n.º 1 do art.º 3.º do DR n.º 19/2008, de 27 de novembro e no Despacho n.º 488/18-OG, de 30 de novembro, do CO.

1.4. Regime jurídico da Investigação Criminal

A IC integra 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[21], no âmbito do processo" (Assembleia da República [AR], 2008a, p. 6038)[22].

Analisando a LOIC, verificamos que, segundo o seu art.º 6.º conjugado com o art.º 7.º e os n.ºs 1, 6 e 7 do art.º 8.º, as competências de IC atribuídas à GNR "se inserem no âmbito de crimes que mais afetam a própria população no seu dia a dia" (Valente, 2019, p. 535). Enquanto Órgão de Polícia Criminal (OPC) de competência genérica[23], compete à Guarda a investigação de crimes cuja competência não esteja reservada a outros OPC e lhes seja delegada pela Autoridade Judiciária (AJ) competente (art.º 6.º da LOIC).

Nos termos processuais, cabe à AJ a direção da investigação, assistida pelos OPC[24] que atuam sob a sua dependência funcional, embora conservem autonomia técnica e tática (n.ºs 1, 2, 4 e 5 do art.º 2.º da LOIC e n.º 1 do art.º 55.º do Código de Processo Penal [CPP]). Segundo Valente (2019, p. 462), a IC "encontra-se subsumida à esfera da ação penal", uma vez que o Ministério Público (MP) e o Juiz devem, no domínio da IC, "defender e promover a legalidade de todos os atos de investigação", bem como promover a ação penal.

Por outro lado, no âmbito da investigação e prevenção criminal, existem fenómenos criminais para os quais, a LPC confere precedência na sua investigação, isto é, os denominados crimes de prevenção prioritária e crimes de investigação prioritária, conforme

[18] Cf. art.º 12.º e art.º 13.º do Despacho n.º 32021/2008, do Comando-Geral da GNR, e o art.º 7.º do Decreto Regulamentar (DR) n.º 19/2008, de 27 de novembro.
[19] Cf. art.º 14.º e art.º 15.º do Despacho n.º 32021/2008, do Comando-Geral da GNR, e o art.º 8.º do DR n.º 19/2008, de 27 de novembro.
[20] Cf. art.º 10.º do DR n.º 19/2008, de 27 de novembro.
[21] De acordo com o n.º 1 do art.º 124.º do CPP, constituem objeto da prova todos os factos com relevância jurídica para a existência ou inexistência do crime, a punibilidade ou não punibilidade do seu agente e a determinação da pena ou das respetivas medidas de segurança.
[22] Cf. art.º 1.º da Lei de Organização da Investigação Criminal (LOIC) – Lei n.º 49/2008, de 27 de agosto.
[23] Cf. al. b) do n.º 1 do art.º 3.º da LOIC.
[24] Segundo o n.º 2 do art.º 55.º do CPP, compete aos OPC, inclusive por iniciativa própria, colher notícia dos crimes, procurando evitar as suas consequências, bem como descobrir os seus agentes e prosseguir atos necessários e urgentes a fim de garantir os meios de prova.

o art.º 2.º e art.º 3.º da LPC, respetivamente. É, portanto, nas leis de política criminal que são definidas as prioridades e orientações de política criminal, sem colocarem em causa o Princípio da Legalidade[25] (Lopes, 2017).

Visando a redução sustentada dos índices de criminalidade, o art.º 14.º da LPC, identifica a partilha de informações, materializada pela cooperação entre os OPC, enquanto orientação para a prevenção e investigação dos crimes anteriormente referidos.

De acordo com o Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança (PCCCOFSS), a atividade de IC é prosseguida no seio do Sistema de Investigação Criminal, ao qual o legislador atribui duas finalidades: a primeira, promover através de ações de recolha da prova, a aplicação da justiça em cada caso em particular. Para tal, é fundamental o reforço das competências de IC da GNR para a criminalidade cuja investigação exige uma eficácia[26] de proximidade; em segundo lugar, contribuir para a prevenção da criminalidade (SSI, 2010).

Assim, a prevenção criminal engloba o conjunto de ações desenvolvidas pelas forças de segurança, a fim de evitar a consumação de factos contrários às finalidades da atividade de segurança interna (n.º 1 do art.º 1.º da LSI).

Por sua vez, atendendo ao n.º 3 do art.º 272.º da Constituição da República Portuguesa (CRP), constata-se que, compete à Polícia[27], "enquanto força de segurança com função de garantia da segurança interna", a prevenção da criminalidade (Soares, 2014, p. 44). Segundo Valente (2019, p. 462), a prevenção criminal concretiza-se, igualmente, na prossecução de atos de IC conduzidos pelos OPC "que se subjugam a este comando constitucional".

Nesta senda, tal como refere Pereira (2005, p. 160), é fundamental evitar a descaracterização dos OPC ou a "perversão da investigação criminal e a sua colocação ao serviço de fins estanhos ao desenvolvimento da política criminal do Estado".

1.5. As vertentes funcionais da Investigação Criminal

Os OPC[28] dispõem de um "saber técnico preciso e profundo" fundamental à prossecução da atividade de IC (Lopes, 2017, p. 19). Remetemo-nos, portanto, para a autonomia técnica dos OPC, prevista no n.º 6 do art.º 2.º da LOIC. Esta autonomia

[25] Segundo Fernandes e Valente (2005, p. 44), o Princípio da Legalidade é "consubstanciado na subordinação da atuação das Forças e Serviços de Segurança aos princípios do Estado de Direito e ao respeito pelos direitos, liberdades e garantias dos cidadãos", ao abrigo do n.º 2 do art.º 266.º da CRP e do art.º 2.º da Lei n.º 53/2008, de 29 de agosto (Lei de Segurança Interna (LSI)).
[26] A eficácia traduz a "medida do grau de concretização dos objetivos" (Rosado, 2015, p. 194).
[27] Cf. n.º 3 do art.º 272.º da CRP.
[28] Cf. al. c) do art.º 1.º do CPP e al. b) do n.º 1 do art.º 12.º da LOGNR.

compreende os procedimentos, conhecimentos e técnicas adequados ao desempenho das suas atribuições[29] (Lopes, 2017). Por outro lado, a possibilidade concedida aos OPC em decidir o tempo, lugar e modo adequados à prossecução dos atos subjacentes ao exercício das suas funções, designa-se por autonomia tática (n.º 6 do art.º 2.º da LOIC).

Nesta conformidade, segundo Paiva (2019, p. 223), "nenhuma lei define a investigação criminal do ponto de vista material, metodológico e epistemológico", ou seja, o investigador não obtém na lei qual o método e/ou estratégias que deverão ser adotadas, de modo a investigar um crime. Neste sentido, Paiva (2019) reforça que, o problema da IC, neste âmbito, consiste na necessidade de estabelecer como se deve resolver cada caso em particular, ou seja, na determinação de uma metodologia ajustada aos factos a investigar. É, neste contexto, que as autonomias técnica e tática se encontram "subordinadas à necessidade de eficácia da investigação criminal" (Valente, 2019, p. 515).

Assim, considerando as alterações à estrutura de IC assumidas no Despacho n.º 18/14 – OG, o reforço da eficácia operacional da IC da Guarda materializa o princípio ativo da sua restruturação. Neste sentido, é estabelecida uma estrutura de IC assente em três vertentes funcionais: IC-Operativa, IC-Criminalística e IC-Análise de Informação Criminal.

1.5.1. IC - Operativa

São múltiplas as fontes que alimentam o sistema das informações, destacando-se, entre elas, o elemento humano (Valacich & Schneider, 2018).

Analisando o Despacho n.º 18/14 - OG, percebe-se que, a vertente operativa da estrutura de IC das Unidades Territoriais, as SIIC, é materializada pelos seguintes órgãos: o NIC[30], o Núcleo de Apoio Operativo (NAO), presente apenas nas SIIC Tipo I, o Núcleo de Investigação e de Apoio a Vítimas Específicas (NIAVE), o NICCOA e o NICAV[31].

Assim, conforme o Apêndice B, a vertente operativa centra as suas atribuições no elemento humano, enquanto agente fundamental na recolha de informações, preocupando-se em "obter dados concretos e com precisão tanto quanto for possível" (Bispo, 2004, p. 89).

[29] A título exemplificativo, apresenta-se a prova pericial que, segundo o art.º 151.º do CPP, tem lugar, em sede processual penal, quando a perceção ou apreciação dos factos requer especiais conhecimentos técnicos, científicos ou artísticos.

[30] Segundo a Informação n.º 05/CO/14, do CO e a Diretiva Operacional n.º 01/14, do CO, os NIC nos CTer Tipo I, foram criados com o intuito de reagir rapidamente a fenómenos criminais de maior complexidade e colmatar, cumulativamente, a extinção das Equipas de Investigação e Inquérito (EII) nos SubDestacamentos Territoriais e dos Postos Territoriais.

[31] Cf. Apêndice B – Vertentes funcionais da IC das Unidades Territoriais da GNR: Despacho n.º 18/14 – OG.

1.5.2. IC - Criminalística

A criminalística compreende uma área do conhecimento científico coadjuvante do Direito e da IC, cujo objeto de análise é o crime e o criminoso. Paralelamente, o seu objetivo traduz-se na "descoberta e na reconstituição da verdade material dos factos penalmente relevantes e a demonstração da sua autoria" (Braz, 2016, p. 38).

Neste sentido, a crescente importância da prova material no plano jurídico-processual e técnico-científico, conduziu ao desenvolvimento das polícias técnica[32] e científica[33] (Machado & Costa, 2013), que exercem um papel íntegro e único no processo de produção probatória (Braz, 2020). Assim, atendendo à realidade operacional, quanto mais rápida for a intervenção policial, maiores serão as probabilidades de salvaguardar e preservar, de forma adequada, o local do crime, a fim de o manter semelhante ao original, no instante posterior ao ato do criminoso (Pinheiro, 2011). Todavia, importa considerar a materialidade da prova[34], já que o recurso a métodos científicos, técnicos ou artísticos, apensados ao processo no domínio probatório, exige que as provas sejam sempre validadas[35] (Lopes, 2017).

Com efeito, através da evolução da ciência e da tecnologia, emergiram diferentes técnicas e metodologias que vieram trazer rigor e eficiência acrescidos ao processo de identificação humana (Braz, 2016). Deste modo, a criminalística intervém em várias áreas forenses, como por exemplo, a fotografia forense, a identificação lofoscópica (U.S. Department of Justice, 2004) e a identificação genética (Machado & Granja, 2020).

De acordo com o Despacho n.º 18/14 – OG, a estrutura de criminalística das Unidades Territoriais da Guarda integra a Subsecção de Criminalística, que se divide em dois órgãos centrais: o Núcleo Técnico-Pericial (NTP) e o Núcleo de Apoio Técnico (NAT) [36].

Ao nível do Despacho n.º 18/14 – OG, em conjugação com o Despacho n.º 488/18-OG, encontra-se, de igual modo, prevista a capacidade forense digital[37], materializada pela

[32] A Polícia Técnica compreende o recurso a múltiplos procedimentos operacionais, técnicas e conhecimentos específicos, com elevados critérios de formação técnica e científica. É responsável, por exemplo, pela localização, identificação e preservação de vestígios, no âmbito da inspeção ao local do crime (Braz, 2020).
[33] A Polícia Científica materializa a retaguarda de apoio e auxílio instrumental à IC, visando assegurar a produção da prova material (Braz, 2020).
[34] A garantia da integridade e da proteção dos vestígios, bem como dos materiais analisados, é determinante no âmbito da Cadeia de Custódia da Prova para que, na esfera jurídico-processual, os vestígios possam ser valorados como prova, apresentando, de modo inequívoco, a veracidade dos factos (Braz, 2016).
[35] No âmbito processual penal, as apreensões estão sujeitas a validação da AJ, num prazo máximo de setenta e duas horas, conforme o disposto no n.º 6 do art.º 178.º do CPP.
[36] Cf. Apêndice B – Vertentes funcionais da IC das Unidades Territoriais da GNR: Despacho n.º 18/14 – OG.
[37] A atividade forense digital traduz o "conjunto de procedimentos científicos relativos ao manuseamento de informação eletrónica, no âmbito das diligências processuais, com o objetivo de identificar, preservar, adquirir, analisar e documentar a prova digital" (Guarda Nacional Republicana [GNR], 2019a, p.1-14).

Repartição de Perícias Digitais Forenses, da Divisão de Criminalística do CO, destacando-se as suas atribuições no âmbito da realização de estudos, exames e perícias de recolha de prova no domínio das Tecnologias de Informação e Comunicação (TIC), bem como a garantia de ações de investigação de crimes perpetuados com recurso às TIC.

1.5.3. IC - Análise de Informação Criminal

À medida que a natureza dos dados criminais evolui, o mesmo acontece com a sofisticação dos métodos analíticos criminais (Pramanik, Lau, Zhang & Li, 2016). Assim, a análise de informação não se baseia somente em elementos históricos, mas, essencialmente, em elementos da atualidade e com base em perspetivas de futuro (Bispo, 2004).

Deste modo, a análise[38] consiste na avaliação e comparação das informações, de modo a compreender o significado dos dados referentes a uma investigação ou avaliação criminal (International Association of Law Enforcement Intelligence Analysts [IALEIA], 2012). Por sua vez, a análise de crimes[39] consiste no estudo sistemático de problemas criminais e de outros aspetos inerentes à missão policial, nomeadamente, fatores sociodemográficos, temporais e espaciais, com o objetivo de apoiar as forças policias no combate, redução, prevenção e avaliação dos crimes (Santos, 2013).

Segundo o Despacho n.º 18/14 – OG, a atividade de Análise de Informação Criminal dos CTer da GNR é assegurada pela Subsecção de Análise e de Investigação Criminal, onde se enquadram os Núcleos de Análise de Informações e Informação Criminal (NAIIC)[40].

Atendendo a esta vertente de IC, o objetivo da análise de informação criminal é transformar dados e notícias disseminadas, em informação processada e integrada. Remete, portanto, para a transformação da matéria prima *Information* no produto final *Intelligence* (Braz, 2020), por intermédio da combinação de múltiplas técnicas, nomeadamente, gráficos, diagramas de associações, matrizes comparativas, entre outros (EUROPOL, 2002).

Contudo, importa concluir que, é o analista quem dirige todo o processo e decide qual a ferramenta que, numa determinada circunstância, melhores soluções poderá extrair do elevado volume de informação (Keay & Kirby, 2018).

[38] Segundo McDowel (2009), a expressão *analysis* traduz tanto o processo analítico, propriamente dito, como também, o seu resultado.
[39] A análise de padrões de crimes é um processo que procura ligações entre crimes e outros incidentes, de modo a encontrar semelhanças e diferenças que podem ser utilizadas na antecipação e prevenção das atividades criminais futuras (Ratcliffe, 2008).
[40] Cf. Apêndice B – Vertentes funcionais da IC das Unidades Territoriais da GNR: Despacho n.º 18/14 – OG.

CAPÍTULO 2
AS INFORMAÇÕES

2.1. Enquadramento concetual

Desde as décadas finais do século XX, as transformações sociais, políticas, económicas, tecnológicas e ambientais emergentes, projetam o alcance da informação e do conhecimento nas múltiplas dimensões da vida em sociedade (Boschele, 2014).

O valor da informação está intimamente relacionado com o modo como esta apoia os responsáveis pela tomada de decisão no cumprimento dos objetivos da organização (Stair & Reynolds, 2016), ou seja, "é fator crítico de sucesso da missão" (Clemente, 2010, p. 158). Assim, dado que a "informação surge como a base de toda a decisão" (Guarda Nacional Republicana [GNR], 2016a, p. 7), a sua função encontra-se latente na prossecução das atividades de diversas instituições, nomeadamente as policiais (Strom, 2017).

Nesta conformidade, uma vez que "a informação favorece a ação" (Clemente, 2010, p. 158), revela-se fundamental a recolha e processamento de notícias úteis para a missão policial, na medida em que permitem "identificar agentes de ameaça, prever acontecimentos e antecipar medidas de segurança" (Alves, 2012, p. 58). Porém, a designação de informação enquanto "resultado do conjunto de atividades de pesquisa, estudo e interpretação de notícias" (GNR, 2016a, p. 13), não pode ser confundida com outros conceitos coexistentes.

Segundo Ratcliffe (2008), a sequência DIKI *continuum* (*Data-Information-Knowledge-Intelligence*) representa uma forma de conceptualizar as informações e as fontes de dados necessárias que estruturam o conhecimento.

Neste sentido, partindo do nível mais elementar, os dados (*Data*)[41] são "factos brutos" (Stair & Reynolds, 2016, p. 5), ou seja, "observações e medições não interpretadas" (Organization for Security and Cooperation in Europe [OSCE], 2017, p.16).

Por seu turno, as notícias dizem respeito a "qualquer facto, documento ou material cujo conhecimento se revele suscetível de ter interesse" permitindo conhecer melhor, quer o adversário, quer a sua área de ação (GNR, 2016a, p. 11). Consequentemente, os dados e as

[41] Segundo a OSCE (2017), são exemplos de dados, os recursos utilizados pelas estruturas de IC que são facilmente quantificáveis, designadamente, os relatórios criminais, as estatísticas de crimes e o conteúdo presente nas bases de dados.

notícias, de acordo com Ferreira (2007, p. 70), não são "tecnicamente informações, embora também não sejam informação sem significado, são informação antes do significado". Considerando os dados individualmente, verificamos que, por si sós, não têm significado (Rascão, 2008). No entanto, quando "colocados num contexto, relacionados com o espaço, o tempo e o cenário de ação" (Bispo, 2004, p. 78), estes convertem-se em informação (*Information)*. Conceptualmente, a informação é o produto da adição aos dados, de um padrão particular de relações que determinam o respetivo formato. Atuar sobre a informação não representa apenas intervir sobre os dados que lhe estão subjacentes, mas também "atuar sobre as relações que se estabelecem, ou seja, sobre os padrões coletivos ou individuais" (Rascão, 2008, p. 68).

Neste seguimento, o processo que permite estabelecer relações entre os dados, a fim de originar informações úteis, exige conhecimento (*Knowledge*) (Stair & Reynolds, 2016). Zikmund (2009, p. 19) define conhecimento como sendo "a mistura de informação, experiência e de entendimento que proporcionam uma estrutura que pode ser aplicada na avaliação de nova informação ou de situações novas". Por outras palavras, o conhecimento passa a existir quando o significado é estruturado (Tomita, Shirasaka, Watanabe & Maeno, 2017), isto é, quando existe a capacidade de associar sistemas complexos de informação para uma nova realidade (Valacich & Schneider, 2018).

Porém, a informação, quando analisada de forma isolada, não permite compreender o modo como os atores irão agir, quais os modelos que serão adotados, os sentidos a alcançar, bem como a oportunidade de emprego do seu esforço (EUROPOL, 2002). Desta forma, quando compreendemos a informação de forma relacionada, contextualizada e organizada, alcançamos um patamar superior, as informações (*Intelligence*) (Bispo, 2004).

Conforme a Figura n.º 1, as informações traduzem-se no "conjunto de notícias, dados e factos, que através de um processo metódico e sistematizado são transformados em informação útil, pertinente" (Sousa, 2007, p. 220) e com fins orientados para a ação (OSCE, 2017).

Em suma, podemos concluir que, enquanto os produtos do conhecimento concorrem para a compreensão, os produtos das informações concorrem para a ação (de Lint, O'Connor & Cotter, 2007).

Figura n. º 1 - Modelo DIKI (*Data - Information - Knowledge - Intelligence*)

Fonte: Elaboração própria, com base em (Liew, 2013, p. 60)

2.2. Caracterização das Informações

A atividade de informações compreende um processo complexo caracterizado pela pesquisa, avaliação, análise, integração e consequente interpretação de informações (Cardoso, 2004). Deste modo, as características da informação estabelecem a sua qualidade e permitem sistematizar o seu tratamento, em virtude de um corpo de critérios que espelham a sua importância, qualidade e valor (Association of Chief Police Officers [ACPO], 2010).

Neste sentido, é fundamental que, a montante da informação, existam dados exatos e pertinentes, de modo a "não exceder a finalidade determinante da sua recolha e, quando aplicável, atuais" (Ministério da Administração Interna [MAI], 1995a, p. 456)[42]. Assim, a utilidade das informações é definida em função da sua adequabilidade[43], oportunidade[44] e precisão[45]. Estas deverão ser devidamente coordenadas, integradas e disseminadas, a fim de apoiarem os responsáveis pelo processo de tomada de decisão (Cardoso, 2004).

Sousa (2007) estrutura o conceito de informações a partir de uma perspetiva tripartida: enquanto produto decorrente do processamento de notícias de índole policial; como um conjunto de atividades que apresentam como finalidade obter o conhecimento e, por fim, enquanto organizações, isto é, elementos responsáveis pelas atividades de

[42] Cf. n.º 1 do art.º 4.º do DR n.º 2/95, de 25 de janeiro.
[43] Segundo Pinochet (2014), devemos ser seletivos nas informações que utilizamos, a fim de descartar as que já não contribuem para nossa atuação, num determinado contexto.
[44] A velocidade de resposta de uma determinada organização decorre da presença, em tempo útil, do fluxo de informação adequado (Gouveia & Ranito, 2004).
[45] A precisão da informação advém do grau de rigor da informação, o que permite uma "caracterização da realidade o mais fiável possível; informação correta, verdadeira" (Gouveia & Ranito, 2004, p. 15).

consecução ou negação do conhecimento. Significa isto que, "podemos entender as informações como um produto, uma atividade ou uma organização" (Sousa, 2007, p. 219).

Pelo que antecede, é na qualidade de produto que a atividade das informações adquire relevo em diversos domínios, nomeadamente, na IC. Contudo, para este produto final ser obtido, é fundamental prosseguir um conjunto de atividades com o intuito de transformar os dados e notícias em informações (Sousa, 2007). A este conjunto de atividades denominamos Ciclo de Produção de Informações[46]. Este ciclo configura um processo "contínuo e dinâmico" (Clemente, 2007, p. 395), constituindo-se o "centro de gravidade[47] de todo o processo analítico" (Paiva, 2019, p. 226).

Neste contexto, o papel primário das informações é o de "reduzir as incertezas e clarificar o que está em jogo", com a finalidade de atingir uma informação "tão depurada quanto possível" (Bispo, 2004, p. 84). Por conseguinte, quando abordamos as informações, "é tradicional estabelecer níveis, consoante o âmbito e a área de aplicação", o que nos conduz à classificação das informações em: Informações Estratégicas, Informações Operacionais e Informações Táticas (Bispo, 2004, p. 91).

Primeiramente, as Informações Estratégicas apresentam horizontes e objetivos de longo prazo, com consequências no desenvolvimento e na prossecução da atividade das forças policiais (EUROPOL, 2002). Estas informações permitem analisar as tendências atuais e emergentes dos fenómenos criminais, ameaças à segurança[48] e ordem públicas, potenciando novas oportunidades e estimulando mudanças nas políticas, programas e legislação (United Nations Office on Drugs and Crime [UNODC], 2011).

Por sua vez, as Informações Operacionais[49] destinam-se ao planeamento e condução das ações no terreno (UNODC, 2011), apoiando os comandantes no planeamento das atividades que visam a redução dos crimes e a implementação de recursos para alcançar os objetivos operacionais (Ratcliffe, 2004). A aquisição destas informações constitui um indicador importante para o "estabelecimento do nível de prontidão desejado e para a avaliação correta das capacidades das nossas forças ou dos nossos sistemas de produção" (Bispo, 2004, p. 94).

[46] Cf. Apêndice C – Ciclo de Produção de Informações.
[47] O centro de gravidade representa o ponto central, onde todo o poder e movimento se encontram mais densamente concentrados, ou seja, do qual tudo depende (Clausewitz, 1982).
[48] Ver conceito de Segurança no Apêndice A - Glossário.
[49] De acordo com a UNODC (2011), as Informações Operacionais envolvem hipóteses e inferências sobre redes criminosas específicas, indivíduos ou grupos envolvidos em atividades ilícitas, discutindo os seus métodos, capacidades, vulnerabilidades, limitações e intenções.

Por fim, mas não menos importantes, as Informações Táticas, representam o suporte para a intervenção na linha da frente, compreendendo as investigações e outras áreas operacionais determinantes na tomada de ações específicas, com o intuito de alcançar os objetivos de execução (Ratcliffe, 2004).

Pelo que antecede, Torres (2005, p. 594) defende que, as FSS podem produzir qualquer tipo de informação, contanto que "revistam uma natureza instrumental e se insiram no âmbito das suas atribuições estatutárias".

2.3. Das Informações Policiais às Informações Criminais

A atividade regular das forças policiais é, em si mesma, "uma excecional fonte de informação" (Sousa, 2011, p. 172), em virtude das "permanentes diligências de vigilância e prevenção levadas a cabo por todo o território nacional" (Oliveira, 2004, p. 90).

Neste sentido, à polícia[50] "cabe a tarefa de previsão, ou seja, antecipar a prevenção" (Clemente, 2010, p. 159). Para tal, recorre à produção de informações e, subsequente, exploração dos produtos, no domínio da manutenção da ordem pública e prevenção da criminalidade inscrevendo-se, neste âmbito, o conceito de informações policiais (Clemente, 2010).

Conceptualmente, as informações policiais[51] são o conjunto de informações destinadas "à prossecução direta das missões legalmente atribuídas a serviços de natureza policial" (Torres, 2005, p. 593), situando-se a um "nível instrumental, mais estratégico-operacional" (Moleirinho, 2009, p. 81). Segundo Alves (2012), as informações policiais compreendem a implementação de medidas de caráter preventivo, bem como a melhoria da eficácia das operações. Neste âmbito, Clemente (2010), divide as informações policiais[52] numa estrutura tripartida, designadamente em: contrainformações, informações de ordem pública e informações criminais.

Primeiramente, as contrainformações designam "o conjunto de medidas de segurança[53] ativas ou passivas de qualquer natureza" (GNR, 2016a, p. 72), com o objetivo de impedir a recolha indevida de informação sigilosa (Földes, 2016).

[50] Cf. art. º 272.º da CRP.
[51] As informações policias não podem ser confundidas com as informações de segurança, uma vez que se situam em planos diferentes (Clemente, 2007). As informações de segurança apresentam um caráter transversal, encontrando-se na base da sua produção, os Serviços Públicos de Informações (Serviço de Informações Estratégicas de Defesa - SIED - e o Serviço de Informações de Segurança – SIS) (Sousa, 2011).
[52] Considerando a Diretiva Operacional n.º 01/14, do CO, compete às SIIC a responsabilidade de coordenação da ação da IC e das informações policiais, bem como a respetiva sincronização.
[53] Cf. Apêndice D e Anexo D – Segurança da Informação: Ficha de procedimentos n.º 1/2020 – GNR (CO/DI).

Por sua vez, as informações de ordem pública destinam-se a prevenir ocorrências de ordem pública e antecipar incivilidades, nomeadamente a produção de delitos criminais, envolvendo o conhecimento decorrente da atividade pré-processual em sede criminal (Clemente, 2010).

Já as informações criminais, "inscrevem-se no âmbito da atividade reportada à investigação criminal" (Clemente, 2010, p. 159). A recolha e processamento de informações criminais constituem uma das ferramentas/técnicas fundamentais na investigação de crimes, pelos OPC (Sousa, 2007). Segundo Moleirinho (2009, p. 152), o processamento das informações criminais "pressupõe que as informações foram adquiridas", através de autos de notícia[54], de denúncia ou de certidão enviada ao Tribunal. A sua importância para a IC é reconhecida pela LOIC ao criar um Sistema Integrado de Informação Criminal previsto no art.º 11.º da LOIC e no art.º 1.º da LISIOPC (Lei da Interoperabilidade entre Sistemas de Informação dos Órgãos de Polícia Criminal)[55] (Fernandes & Valente, 2005).

No que concerne à partilha de informação, designadamente da informação criminal, pode ser realizada mediante as seguintes modalidades: "acesso resultante de pedido em concreto[56]; acesso resultante de determinação ou protocolo[57]; e acesso direto a Sistemas de Informação[58]" (Pereira, 2012, p. 64). Prosseguida por intermédio de acessos a sistemas integrados de informação criminal[59], a partilha de informação criminal representa o "instrumento de cooperação mais qualificado para fins (…) de investigação criminal" (Pereira, 2012, p. 62). Deste modo, as informações de natureza criminal servem de base à condução da IC e auxiliam os OPC na tomada de decisão das táticas e técnicas a adotar (Fernandes & Valente, 2005).

Face ao exposto, seria um equívoco considerar que, "não existe relação alguma entre informações e investigação criminal", dado que "as informações são, em larga medida, instrumentais da investigação criminal" (Pereira, 2005, p. 157).

[54] Cf. art. º 243.º do CPP.
[55] Lei n.º 73/2009, de 12 de agosto.
[56] Cf. al. b) do n.º 1 do art.º 9.º da LISIOPC, por exemplo.
[57] Cf. n.ºs 2, 3 e 4 do art.º 4.º do Decreto-Lei n.º 81/95, de 22 de abril (Brigadas Anticrime e Unidades Mistas de Coordenação).
[58] Cf. al. a) do n.º 1 do art.º 9.º da LISIOPC, por exemplo.
[59] Cf. n.ºs 1, 2 e 5 do art.º 11.º da LOIC e n.º 1 do art.º 14.º da LPC.

CAPÍTULO 3
DOS SISTEMAS DE INFORMAÇÃO ÀS TECNOLOGIAS DE INFORMAÇÃO

3.1. Os Sistemas de Informação

Um Sistema compreende o conjunto de componentes que se relacionam entre si, com a finalidade de alcançar um objetivo comum. Porém, importa considerar que, o conjunto desses componentes edificadores do Sistema, constituem mais do que a mera soma das respetivas partes (Sillitto, *et al.*, 2019).

Partindo desta visão holística, Laudon e Laudon (2018) definem SI enquanto conjunto de elementos interrelacionados, que concorrem entre si, a fim de recolher, armazenar, processar e disseminar informações, que serão um importante instrumento de apoio à decisão, por quem de direito. Por sua vez, Amaral e Varajão (2000, p. 9), afirmam que os SI se traduzem numa "combinação de procedimentos, informação, pessoas e Tecnologias de Informação, organizadas para o alcance dos objetivos de uma organização" colaborando, quer para o planeamento, como para a tomada de decisão e controlo da organização, conforme representado na Figura n.º 2.

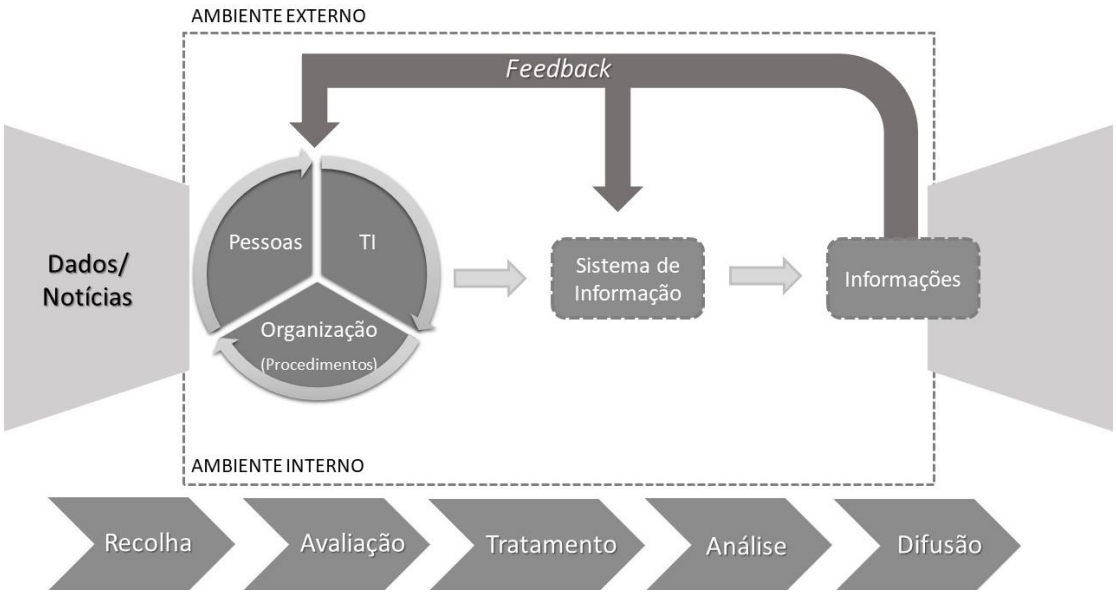


Figura n.º 2 - Enquadramento esquemático de um Sistema de Informação

Fonte: Elaboração própria, com base em (Nunes, 2015a, p. 24) e (Laudon & Laudon, 2018, p. 45)

Assim, os SI configuram o suporte ao fluxo de dados e informação, de modo a satisfazer as necessidades das pessoas que prosseguem atividades no domínio das operações de uma organização (Rainer, Prince & Watson, 2015). A sua conceção assenta numa articulação eficiente e eficaz dos múltiplos componentes integrantes, designadamente, as pessoas, o conjunto de dados, o *hardware*, o *software*, sistemas de comunicação e procedimentos organizacionais, estruturados num critério de valor estabelecido pelos seus utilizadores (Hevner, 2010).

Primeiramente, as pessoas compreendem todos os indivíduos que executam ou apresentam um vínculo com as atividades organizacionais, incluindo os destinatários, os recursos humanos da organização e as respetivas competências (Johnson, 2018). Por outro lado, o *hardware* diz respeito aos sistemas de computação, computadores pessoais, estações de trabalho, entre outros (Wasson, 2015). No que concerne ao *software*, caracteriza-se como sendo todos os programas que possibilitam ao computador[60] a concretização de uma determinada tarefa, sendo constituído por um conjunto de instruções ou comandos sistematizados numa sequência lógica, de modo a instruir o computador (Laudon & Laudon, 2018). Quanto aos sistemas de comunicação, estes materializam todas as redes e comunicações que permitem a conexão entre os computadores geograficamente distribuídos, a fim de garantir a comunicação entre os mesmos, bem como a troca de informações e o respetivo processamento (Ferreira, 2017). Por fim, os procedimentos organizacionais traduzem o conjunto de regras, ações e políticas que devem ser adotados, por forma a alcançar os objetivos organizacionais (Johnson, 2018).

Deste modo, a evolução dos SI assenta os seus pilares na palavra "simplificar" recorrendo, para tal, às TI (Ramos, López & Abreu, 2017). A partir da integração e incorporação das potencialidades provenientes da utilização das TI, os SI tornam-se recursos estratégicos determinantes no alcance de vantagens organizacionais (Rascão, 2012).

3.2. As Tecnologias de Informação

A evolução das TI constitui um fator potenciador da reestruturação, bem como da dinamização da flexibilidade, autonomia e qualidade das tarefas organizacionais (Sequeira & Serrano, 2002). Um estreito alinhamento dos objetivos de uma organização com as

[60] Um computador é todo o dispositivo eletrónico, estruturado com o intuito de processar dados de entrada (*input*), transformando-os através da realização de instruções armazenadas, em informação de saída (*output*), para diversos dispositivos (Gouveia & Ranito, 2004).

capacidades dos Sistemas e TI traduz um dos critérios fundamentais para um bom desempenho de uma organização (Baptista, Varajão & Moreira, 2013).

Neste sentido, segundo Rascão (2008, pp. 72-73), as TI são um "conjunto complexo de conhecimentos, de meios e de *know-how*, organizados com vista a uma produção" impulsionando, de forma determinante, o "aparecimento de novas formas e perspetivas de encarar as questões". Por sua vez, numa perspetiva estritamente tecnológica, Gouveia e Ranito (2004, p. 22) definem TI como sendo o conjunto de "dispositivos de computador (*hardware* e *software*), técnicas de processamento e tecnologias de comunicação de dados e de informação".

Assim, podemos distinguir três grupos principais de elementos que integram as TI, designadamente, o *software*, o *hardware* e as infraestruturas (Rainer, Prince & Watson, 2015). Tal como definido anteriormente, o *software* engloba os sistemas operativos, as ferramentas de desenvolvimento, os sistemas de gestão de bases de dados, entre outros (Ferreira, 2017). Já o *hardware*, envolve os equipamentos de entrada, armazenamento, processamento e saída da informação (Stair & Reynolds, 2016). Por fim, as infraestruturas dizem respeito, quer às instalações e meios de transmissão/telecomunicações, como ao respetivo *hardware* (por exemplo, as placas de rede) e *software* (por exemplo, os protocolos de comunicação) (Rainer, Prince & Watson, 2015).

Por seu turno, Laudon e Laudon (2018) consideram que a infraestrutura das TI, paralelamente aos dispositivos físicos e aplicações de *software*, integra o conjunto de serviços de toda a organização, geridos e compostos pelos recursos humanos e técnicos. Tal como representado na Figura n.º 2, os recursos humanos são significativamente importantes para o sucesso das finalidades para as quais as TI foram concebidas (Neto & Leite, 2015).

Progressivamente, adicionando às TI "as preocupações com a comunicação de informação", designadamente, conteúdos de gestão de base digital entre os utilizadores, suporte a grupos, apresentação e observação dos dados e informação, somos conduzidos ao conceito de TIC (Gouveia & Ranito, 2004, p. 22). Segundo Rascão (2008, p. 73), as TIC compreendem o "conjunto de conhecimentos, de meios materiais (infraestruturas) e de *know-how*", indispensáveis para a produção, utilização de bens e serviços, bem como para o armazenamento (provisório ou definitivo), processamento e comunicação dos dados.

Deste modo, as TI, além da recolha, armazenamento, processamento, acessibilidade e difusão da informação, permitem o aumento, quer da quantidade, quer da qualidade da informação (Castro, 2018), imprimindo acrescidas eficácias e eficiências aos SI e superior robustez nas infraestruturas tecnológicas (Nunes, 2015b).

3.3. A interoperabilidade e o dever de cooperação

Múltiplas são as expressões, com previsão normativa, que definem o conceito ou traduzem atividades instrumentais da cooperação, entre as quais: "Exercício em comum"[61]; "Conjugar Esforços"[62]; "Colaboração"[63]; "Partilha de Informação"[64]; "Intercâmbio de dados e informações"[65]; "Pontos de contacto"[66]; "Comunicação"[67] e "Articulação"[68].

Como referido por Rascão (2008, p. 107), uma vez condicionada a comunicação entre os sistemas, a informação "perde qualidade e precisão, apresenta um custo elevado [e] não é transmitida em tempo útil". Assim, reforçar a articulação e a respetiva cooperação entre as FSS, nomeadamente, através do intercâmbio de informação, recursos, experiências e boas práticas, constituem orientações estratégicas previstas no RASI referente a 2018 (SSI, 2019).

Atendendo ao PCCCOFSS, importa salientar três princípios subjacentes ao desenvolvimento do sistema de IC, especificamente: o Princípio da Coordenação, o Princípio da Cooperação e Dever de Comunicação e o Princípio da Partilha de Informação (SSI, 2010).

Tomando como ponto de partida o Princípio da Coordenação, importa considerar que, a coordenação entre os OPC, de acordo com o n.º 1 do art.º 15.º da LOIC e o art.º 16.º da LSI, é regulada pelo Secretário-Geral do Sistema de Segurança Interna (SGSSI), segundo as orientações genéricas enunciadas pelo Conselho Coordenador dos OPC.

Por sua vez, o Princípio da Cooperação e Dever de Comunicação[69] encontra-se consagrado no n.º 1 e n.º 2 do art.º 10.º da LOIC. Assim, o dever de cooperação determina que os OPC devem cooperar mutuamente no exercício das suas funções, sob pena de violação do pressuposto no art.º 381.º do Código Penal (CP) - Recusa de Cooperação. Igualmente, o n.º 2 do art.º 6.º da LSI, prevê que as FSS cooperam entre si através da "comunicação de informações que, não interessando apenas à prossecução dos objetivos específicos de cada um deles, sejam necessários à realização das finalidades de outros" (Assembleia da República [AR], 2008a, p. 6135). Por fim, o Princípio da Partilha de Informação, estabelecido no n.º 1 do art.º 11.º da LOIC, define que o dever de cooperação é

[61] Cf. n.º 6 do art.º 7.º da CRP.
[62] Cf. Preâmbulo da Carta das Nações Unidas.
[63] Cf. art.º 46.º do Tratado sobre o Funcionamento da União Europeia.
[64] Cf. n.º 1 do art.º 23.º da LSI; n.º 1 do art.º 11.º da LOIC e n.º 1 do art.º 14.º da LPC.
[65] Cf. n.º 3 do art.º 9.º da LISIOPC.
[66] Cf. al. b) do n.º 2 do art.º 17.º, n.º 3 do art.º 23.º e art.º 23.º-A, da LSI.
[67] Cf. n.º 3 do art.º 2.º e n.º 2 do art.º 10.º, ambos da LOIC e n.º 2 do art.º 6.º e n.º 1 do art.º 33.º, ambos da LSI.
[68] Cf. al. a) do n.º 1 do art.º 14.º da LOIC e n.º 3 do art.º 16.º e art.º 35.º ambos da LSI.
[69] Segundo Valente (2019), o Princípio da Cooperação assenta, por um lado, na partilha de dados e informações relativos aos diversos crimes, sempre que seja solicitado por uma das polícias ou seja da sua competência específica e, por outro lado, traduz o dever de comunicação de um OPC.

assegurado por um Sistema Integrado de Informação Criminal que garante a partilha de informação entre os OPC, assente nos princípios da necessidade e da competência[70].

Deste modo, as FSS são fontes essenciais de alimentação dos SI, pelo elevado volume de dados resultantes da sua intervenção no terreno, encontrando-se subordinadas aos deveres de coordenação e cooperação, por intermédio da comunicação recíproca de dados, não enquadrados no regime especial de reserva ou proteção (SSI, 2010).

Em suma, tal como refere Pereira (2012, p. 27), a "investigação criminal é, em si mesma, uma atividade de cooperação". Neste sentido, as TI melhoram a comunicação entre as unidades, principalmente quando articuladas com o objetivo comum de reduzir a criminalidade (Koper, Lum & Willis, 2014).

3.4. Os Sistemas de Informação na GNR: SIIOP e PIIC

As FSS, nomeadamente a GNR, "jamais podem viver sem um Sistema de Informações estruturado, perene e operativo, capaz de fazer a previsão e o acompanhamento dos fenómenos" (Clemente, 2007, p. 385).

No domínio operacional, o sistema com estrutura legal de suporte ao registo das ocorrências de índole operacional, dados pessoais[71] e análise de informação proveniente das múltiplas valências e especialidades institucionais é, numa perspetiva holística, o Sistema Integrado de Informações Operacionais de Polícia (SIIOP)[72] (Agência para a Modernização Administrativa [AMA], 2017). Conforme a NEP/GNR – 8.80, de 16 de maio, o SIIOP[73] constitui uma "base de dados heterogénea distribuída, que tem por finalidade organizar e manter atualizada a informação" (Guarda Nacional Republicana [GNR], 2016b, p.1). Este SI dá corpo a um "repositório único, centralizado e alargado a todo o dispositivo", suportando a prevenção e antecipação, em informação operacional (GNR, 2016b, pp. 1-2).

Atendendo às diversas áreas de especialidade, o SIIOP contém diferentes submódulos aplicacionais destacando-se, na presente investigação, o submódulo Principal (SIIOP-P)[74].

[70] De acordo com Lopes (2017, p. 89), ainda que, com competências muito específicas e próprias, são impostos a todos os agentes que participam na esfera da investigação e prevenção, "graus de confiança elevados com vista à troca de informações entre todas, ainda que bilateralmente".
[71] A manutenção da base de dados pessoais da GNR está prevista no DR n.º 2/95. De acordo com o n.º 1 do art.º 1.º, a base de dados da Guarda é concretizada pelo SIIOP, tendo como objetivo organizar e manter atualizada a informação necessária ao exercício das respetivas atribuições (n.º 2 do art.º 1.º do DR n.º 2/95).
[72] A implementação do SIIOP está regulamentada na NEP/GNR – 2.20 da DI, de 12 de dezembro de 2011.
[73] Segundo o Manual de Intercâmbio de Informações entre Autoridades Policiais, do Conselho da União Europeia, o SIIOP consiste num "repositório de informações sobre pessoas, objetos, veículos, locais, organizações, factos (específicos e não específicos), relações, documentos e armas" (Conselho de União Europeia, 2016, p. 296).
[74] Consultar outros submódulos do SIIOP no Apêndice E.

O SIIOP-P tem como finalidade o registo e a gestão das ocorrências subjacentes à tramitação em sede de auto de notícia, a fim de ser posteriormente enviado para Tribunal, assegurando a rastreabilidade processual, a proteção de dados pessoais e a segurança dos acessos à informação apenas por quem tem a necessidade de saber e está devidamente autorizado. O SIIOP-P destina-se, ainda, à partilha de informação com outras FSS, com as quais a Guarda articula uma estreita relação institucional, quer nacional, quer internacional (AMA, 2017).

Paralelamente, existem ainda diversos sistemas e plataformas externas com as quais a Guarda coopera, interage, consulta e troca dados, para efeitos de IC, nomeadamente, a Plataforma para o Intercâmbio de Informação Criminal (PIIC) (AMA, 2017). Segundo o n.º 2 do art.º 2.º da LISIOPC, a PIIC tem como objetivo garantir um nível elevado de segurança na partilha de informação criminal entre os OPC, no âmbito da prevenção e da IC.

Materializado pela implementação da PIIC (n.º 1 do art.º 1.º da LISIOPC), o Sistema Integrado de Informação Criminal (art.º 11.º da LOIC), embora tenha por base na sua arquitetura a independência dos SI dos OPC[75], a sua implementação, coordenação, supervisão, segurança e intercâmbio de informação são assegurados pelo SGSSI[76], sob controlo do Conselho de Fiscalização do Sistema Integrado de Informação Criminal (CFSIIC) [77] (n.º 1 e n.º 5 do art.º 8.º da LISIOPC) (Valente, 2019).

Pelo que antecede, a fim de reforçar a proximidade entre os SI e as TI, prevenir a criminalidade com uma eficácia acrescida, otimizar os recursos humanos, desmaterializar processos e garantir maior interoperabilidade entre os SI (AMA, 2017), têm vindo a ser desenvolvidas diversas medidas, quer a nível interno, atendendo aos Planos de Atividades e à Estratégia 2020[78] da GNR, como no domínio da Administração Pública (AP) (Estratégia TIC 2020 da AP), para a modernização digital da GNR e desenvolvimento das TIC[79]. Este investimento na transformação digital da GNR tem como suporte o investimento nas TIC decorrente da Lei de Programação de Infraestruturas e Equipamentos das Forças e Serviços de Segurança (LPIEFSS) (Lei n.º 10/2017, de 3 de março).

Deste modo, a difusão de sistemas de apoio à decisão, alicerçados em TI constituem, cada vez mais, uma exigência para a caracterização da autoria e do espaço criminal. A sua adoção possibilita, em tempo real, a gestão do conhecimento referente à prática de crimes (Clemente, 2006). Trata-se, portanto, de trabalhar e produzir informação que se traduz

[75] Cf. n.º 1 do art.º 3.º da LISIOPC.
[76] Cf. n.º 1 do art.º 5.º da LISIOPC e n.º 1 e n.º 2, ambos do art.º 15.º da LOIC.
[77] Cf. Apêndice F – Sistema de Partilha de Informações (PIIC).
[78] Cf. Apêndice G – Medidas no âmbito das TIC - GNR (2015 - 2020).
[79] Cf. Apêndice H - Estratégia TIC 2020: Estratégia para a transformação digital na AP.

determinante no "enorme conjunto de informação estatística sobre pessoas, suspeitos ou arguidos de crimes, sobre determinados fenómenos criminológicos", bem como sobre as respetivas tendências criminais, riscos sociais, entre outros (Lopes, 2017, p. 86).

3.5. As Tecnologias de Informação na Investigação Criminal

Um dos erros mais decisivos para a inviabilização de uma atuação eficiente por parte das FSS prende-se com a implementação de métodos convencionais e obsoletos na resolução de crimes, inseridos num novo contexto social em modificação constante (Souza, 2016).

Assim, a condução de uma investigação eficaz e eficiente na "descoberta e na recolha de indícios suficientes, no exame e interpretação dos mesmos, conseguindo obter em tempo útil as provas reais" (Valente, 2019, p. 135) que garantam uma confirmação da ocorrência de um facto criminal, permitirá uma célere localização e contacto com os seus autores, aumentando as oportunidades de responsabilização e punição dos mesmos (Valente, 2019).

Neste sentido, uma vez que "o *timing* para a tomada de decisões é cada vez menor" (Rascão, 2008, p. 96), é imprescindível, face a esta exigência, o recurso às TI para uma deteção e resposta aos crimes mais célere, bem como na melhoria da recolha de evidências e desenvolvimento de novas estratégias de prevenção e de IC (Koper, Lum & Willis, 2014).

A fusão entre a IC e as TI produz efeitos, desde logo, no âmbito da recolha de indícios criminais. Uma vez que a comunicação ocorre, maioritariamente, por intermédio de meios de comunicação como os telemóveis e a *Internet*, a sua interceção[80], recolha e leitura, materializam peças fundamentais na investigação dos crimes. Falamos, portanto, de meios de recolha de informação utilizados, essencialmente, pela vertente operativa da IC, ou seja, as escutas telefónicas (Custers, 2008). Através de determinados *softwares*, é possível efetuar a recolha das comunicações, o seu armazenamento e a posterior leitura, mediante a gravação[81], em tempo real, do conteúdo das informações comunicadas entre os intervenientes, sob investigação num determinado processo crime (Kusac, 2016). Por conseguinte, a recolha de dados, som e imagem, possibilitam uma recuperação da informação e reconstituição dos acontecimentos passados, bem como o acompanhamento e registo, em tempo útil, do desenvolvimento da atividade criminosa (Braz, 2016).

[80] A interceção consiste na "interrupção do curso de uma conversação ou comunicação telefónica ou na apropriação de uma conversa ou comunicação telefónica dirigida a outrem" (Rodrigues, 2008, p. 91).
[81] A interceção e a gravação de conversações ou comunicações em telemóveis ou outros meios técnicos, como o correio eletrónico, exigem ordem ou autorização do Juiz de Instrução, mediante requerimento do Ministério Público, em certos tipos de crimes, para efeitos probatórios em sede do processo (art.ºs 187.º e 189.º do CPP).

No âmbito da recolha de prova, são utilizadas ferramentas digitais forenses com a capacidade de aceder às informações contidas em dispositivos móveis. Uma das soluções tecnológicas mais utilizadas é o *UFED Ultimate (Universal Forensics Extraction Device)*, que permite o acesso ao conteúdo de, por exemplo, *smartphones*, extraindo e descodificando, quer os dados de fácil acesso presentes na memória interna do dispositivo (por exemplo, as conversações do *WhatsApp*), como também, todos os dados ou ficheiros apagados, restaurando-os (por exemplo, mensagens, fotografias ou vídeos) (Khan & Mansuri, 2018).

Por sua vez, existem provas que, pela sua natural perecibilidade, exigem uma garantia absoluta da integridade e inalterabilidade dos seus elementos, a fim de preservar a Cadeia de Custódia da Prova (Braz, 2016). Consequentemente, uma das vantagens decorrentes da utilização das TI consiste em "produzir provas materiais que futuramente irão corroborar os factos relatados" (Costa & Machado, 2012, p. 130). Remetemo-nos, deste modo, para a identificação lofoscópica que, segundo Braz (2020, p. 55), traduz, de forma inequívoca, "o principal processo de produção probatória". Neste sentido, a força e o valor da prova pericial, para além da forma e do método como são obtidas, dependem de equipamentos tecnológicos que preservam a sua qualidade, garantem o seu armazenamento e promovem a validade das conclusões periciais. Uma das principais TI utilizadas pela vertente de Criminalística, neste domínio, é o sistema AFIS (*Automated Fingerprint Identification System*) (Braz, 2016).

O sistema AFIS materializa uma das tecnologias-chave no armazenamento e tratamento de impressões digitais, quer das dez impressões dos dedos das mãos, como palmares (Girelli, 2014). A partir deste sistema é possível indexar, ordenar e classificar, na sua base de dados, as impressões lofoscópicas recolhidas (Braz, 2016), assim como identificar e comparar as impressões digitais recolhidas das cenas do crime com as impressões digitais do seu repositório[82] (Moses, 2010). Esta tecnologia, de acordo com Braz (2020, p. 55), permitiu um "decisivo aumento de resultados probatórios" contribuindo, quer para identificação dos autores dos crimes, como para deteção de falsas identidades.

Por outro lado, as novas TI alicerçadas por poderosas soluções informáticas, possibilitam o alcance de elevados desempenhos no cruzamento e na correlação de dados aumentando, de forma significativa, a capacidade de tratamento da informação e, principalmente, a respetiva análise (Marolla, 2018). O recurso às TI pela vertente de Análise de Informação Criminal manifesta vantagens, fundamentalmente, a dois níveis na IC: a nível operacional através da projeção de diretrizes de intervenção e hipóteses de trabalho baseados

[82] A correlação das impressões recolhidas com as armazenadas no AFIS é concretizada através da identificação de 12 pontos mínimos convencionados, conforme o n.º 3 do art.º 12.º da Lei n.º 67/2017, de 9 de agosto.

em diagramas, fluxogramas de conexões, cronogramas e matrizes de probabilidade e, a nível estratégico, mediante o apoio ao planeamento e gestão de polícia, através da previsão da "criminalidade e da identificação de tendências e padrões evolutivos" (Braz, 2020, p. 71).

Deste modo, uma das principais vantagens do recurso às TI consiste "no processamento automático para apoio do analista" (Bispo, 2004, p. 99) permitindo, consequentemente, o processamento de um manancial de informação recorrendo a tecnologias, como é o caso do *software i2 Analyst´s Notebook* da *International Business Machines* (IBM) (Gorbanov, Ismailov & Zaiets, 2019). A partir deste *software*, a IC, na sua vertente de Análise de Informação Criminal, dispõe de uma ferramenta que permite a "análise de vínculos, orientado à associação de elementos, identificação de relações e compilação de dados" (Machado & Vilalta, 2018). Por conseguinte, o *i2 Analyst´s Notebook,* permite aos analistas a utilização de recursos de visualização e análise, a fim de apoiar na identificação de redes, padrões e tendências, o que conduz a uma tomada de decisão mais rápida e informada (International Business Machines Corporation [IBM], 2017). Assim, é possível abrir uma janela que resume um conjunto de informações básicas sobre o suspeito, analisar o seu histórico criminal, interligar cada um dos seus contactos, identificar possíveis indivíduos associados ao suspeito, entre outros (Seattle Police Department [SPD], 2017).

Importa, portanto, salientar que a difusão de sistemas e tecnologias de apoio à decisão decorre da necessidade de caracterizar, não só a autoria dos crimes, mas também do espaço criminal (Clemente, 2006, p. 78). Face a esta exigência, é fundamental o recurso a ferramentas tecnológicas que permitam aos analistas mapear o crime, a fim de "realizar análises espaciais de problemas de crimes e desordens" (Santos, 2013, p. 5). Um dos principais recursos tecnológicos de IC utilizados no mapeamento e análise de crimes é a ferramenta *Quantum Geographic Information System* (QGIS). Possibilitando visualizar, navegar, trabalhar e analisar conjuntos de dados de crimes geográficos (Sivaranjani & Sivakumari, 2015), a utilização desta ferramenta permite, igualmente, obter análises visuais e estatísticas da natureza espacial do crime, permite conceder aos analistas diversas fontes de dados baseadas em variáveis geográficas comuns e, também, compreender não apenas onde os problemas criminais estão localizados (Kumar & Game, 2016), mas qual a sua variação espacial ao longo do tempo (Paulsen & Robinson, 2009).

Pelo que antecede, podemos concluir que, os Sistemas e TI tornaram-se um suporte fundamental ao desenvolvimento de qualquer atividade de IC permitindo, desde a recolha e avaliação, ao tratamento, análise e difusão das informações, desenvolver e gerar uma eficácia e eficiência acrescidas nos mecanismos de prevenção e IC (Lopes, 2017).

CAPÍTULO 4
METODOLOGIA, MÉTODOS E MATERIAIS

4.1. Introdução

O presente capítulo destina-se a apresentar a metodologia, métodos e materiais adotados, para o desenvolvimento e condução do presente TIA[83].

De acordo com Sarmento (2013, p. 6), a investigação consiste no "diagnóstico das necessidades de informação e seleção das variáveis relevantes sobre as quais se irão recolher, registar e analisar informações válidas e fiáveis", ou seja, traduz "algo que se procura" (Quivy & Campenhoudt, 2017, p. 31). Assim, a investigação científica[84] diferencia-se das demais pelo seu "caráter sistemático e rigoroso" (Fortin, Côté & Filion, 2009, p. 4), tendo de seguir todo um processo que envolva a "utilização de métodos e técnicas", ou seja, uma metodologia (Oliveira, 2011, p. 19).

4.2. Desenho de investigação

Segundo Fortin, Côté e Filion (2009, p. 214), o desenho de investigação compreende o conjunto de decisões para edificar a estrutura da investigação, permitindo "explorar empiricamente as questões de investigação ou verificar as hipóteses". A investigação deve, portanto, dar resposta a determinados "princípios estáveis e idênticos" seguindo, para tal, um conjunto de etapas do procedimento científico (Quivy & Campenhoudt, 2017, p. 25).

Face ao exposto, o presente TIA segue, como linha de orientação, as etapas do procedimento científico[85] propostas por Quivy e Campenhoudt (2017). É a partir deste procedimento que se torna possível "circunscrever, delimitar, fragmentar e analisar o que se constitui objeto da pesquisa" (Marconi & Lakatos, 2003, p. 79), de modo a "progredir em direção a um objetivo" (Quivy & Campenhoudt, 2017, p. 25). Na primeira etapa deste procedimento, foi estruturada a PP, a fim de direcionar a investigação para "o fenómeno em análise, desempenhando o papel guia na investigação" (Coutinho, 2018, p. 49).

[83] Segundo Fortin, Côté e Filion (2009, p. 18), a Investigação Aplicada compreende "um processo científico, que visa encontrar aplicações para os conhecimentos teóricos", isto é, adquirir "novos conhecimentos, (…) orientados por objetivos práticos determinados" (Carvalho, 2009, p. 42).
[84] A investigação científica traduz toda a atividade orientada para a obtenção de "conhecimentos científicos, ou seja, conhecimentos objetivos, sistemáticos, claros, organizados e verificáveis" (Vilelas, 2017, p. 41).
[85] Cf. Anexo E – Etapas do procedimento científico.

Subsequentemente, a fase seguinte, a Exploração (Quivy & Campenhoudt, 2017), visa uma "apreciação profunda do contributo dos diferentes textos para a resolução do problema de investigação" (Fortin, Côté & Filion, 2009, p. 87). Para tal, foram realizadas leituras de obras literárias, legislação e artigos de referência e, paralelamente, aplicadas entrevistas exploratórias a entidades com experiência na matéria.

Após a Exploração, segue-se uma nova fase, a partir da qual é decidida a abordagem ou perspetiva teórica para tratar do problema enunciado pela PP, isto é, a Problemática (Quivy & Campenhoudt, 2017), circunscrita aos Capítulos 1 a 3 da presente investigação.

Uma vez que "a montante, a problemática só chega realmente ao fim com a construção do modelo de análise", foi edificada a quarta etapa, desenvolvida no Subcapítulo 4.3. Esta fase tem em vista traduzir as ideias apresentadas na fase anterior "numa linguagem e em formas que as habilitem a conduzir o trabalho sistemático de recolha e análise dos dados de observação ou experimentação que deve seguir-se", formulando-se, consequentemente, as hipóteses de investigação (Quivy & Campenhoudt, 2017, p. 109).

Por sua vez, decorre a quinta etapa, ou seja, a Observação (Quivy & Campenhoudt, 2017), onde são recolhidas informações que permitirão "conhecer os fenómenos e extrair deles informação" (Vilelas, 2017, p. 287), isto é, através do qual o modelo de análise será "confrontado com dados observáveis" recolhidos (Quivy & Campenhoudt, 2017, p. 155).

Dado que o objetivo principal da investigação consiste em dar resposta à PP, a sexta etapa, a Análise das Informações, tem por base a verificação empírica permitindo, por consequência, comparar os "resultados observados com os resultados esperados a partir da hipótese" (Quivy & Campenhoudt, 2017, p. 211) e, deste modo, o aperfeiçoamento, quer da PP, como do modelo de análise (Santos & Lima, 2019).

Por fim, a sétima e última etapa, compreende as conclusões do TIA. Segundo Quivy & Campenhoudt (2017), esta fase é estruturada em três critérios: a retrospetiva das principais guias do procedimento seguido; a demonstração criteriosa dos contributos para o conhecimento decorrente da investigação e, por último, as considerações de cariz prático[86].

4.3. Modelo de análise

O modelo de análise[87], enquanto elemento instrumental em relação ao trabalho de campo, emerge no processo de investigação como resultado da revisão da literatura e de

[86] Cf. Apêndice I – Desenho de investigação.
[87] Cf. Apêndice J – Modelo de análise.

"todos os elementos essenciais ao estudo, designadamente no domínio conceptual e no domínio metodológico" (Santos & Lima, 2019, p. 61).

Deste modo, a PP, apresentada no Quadro n.º 1, constitui "verdadeiramente a pergunta central da investigação, na qual se resumirá o objetivo do trabalho" (Quivy & Campenhoudt, 2017, p. 102). Por sua vez, a partir da PP, decorrem as denominadas Perguntas Derivadas (PD), responsáveis por circunscrever os "setores respetivos onde o investigador incidirá o seu esforço, muito ligados naturalmente aos objetivos da investigação" (Rosado, 2015, p. 79). Atribuindo uma "visão global e abrangente do tema" (Marconi & Lakatos, 2003, p. 219), o OG da investigação, posteriormente detalhado através da formulação de OE (Oliveira, 2011), relaciona-se com o "conteúdo intrínseco, quer dos fenómenos e eventos, quer das ideias estudadas" (Marconi & Lakatos, 2003, p. 219).

Assim, a organização e condução de uma investigação assente em hipóteses "constitui a melhor forma de a conduzir com ordem e rigor" (Quivy & Campenhoudt, 2017, p. 119), visto que traduzem um "elemento útil para justificar o estudo e garantir-lhe orientação" (Freixo, 2012, p. 193). As hipóteses de investigação compreendem "proposições conjeturais ou suposições que constituem respostas possíveis às questões de investigação", passíveis de ser confirmadas ou infirmadas durante a investigação (Sarmento, 2013, p. 13).

Quadro n.º 1 – Objetivos e perguntas de investigação

N.º	Objetivo Geral (OG)		Pergunta de Partida (PP)	
	Analisar os principais contributos da utilização das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da GNR.		Quais os principais contributos das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da GNR?	
1	**OE**	Descrever a função das Informações Criminais na resposta aos fenómenos criminais.	**PD**	Qual a função das Informações Criminais na resposta aos fenómenos criminais?
2	**OE**	Caracterizar as principais Tecnologias e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades Territoriais da GNR.	**PD**	Quais as principais Tecnologias e Sistemas de Informação utilizados pelas Unidades Territoriais da GNR na vertente de Investigação Criminal?
3	**OE**	Identificar os pontos fortes e as debilidades subjacentes à estrutura e funcionamento dos Sistemas e Tecnologias de Informação na estrutura de Investigação Criminal das Unidades Territoriais da GNR.	**PD**	Quais as vantagens e desvantagens decorrentes do funcionamento e utilização dos Sistemas e Tecnologias de Informação pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?
4	**OE**	Identificar as melhorias a implementar nos Sistemas e Tecnologias de Informação para reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR.	**PD**	Quais as melhorias a implementar nos Sistemas e Tecnologias de Informação, por forma a reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?

Fonte: Elaboração Própria, com base em (Quivy & Campenhoudt, 2017)

Atendendo à PP e às PD apresentadas no Quadro n.º 1, foram elaboradas quatro hipóteses derivadas (H) e uma hipótese para a PP (HPP), designadamente:

HPP: "O recurso às TI pela estrutura de IC permite a análise e sintetização da informação, a análise do histórico criminal e identificação de padrões e tendências criminais, a extração, armazenamento e leitura das informações armazenadas em dispositivos móveis, bem como a identificação e a preservação de vestígios em suporte digital, garantindo a sua integridade e inalterabilidade."

H1: "As informações criminais destinam-se a cumprir as finalidades da IC, sendo utilizadas pelos NAIIC na produção de relatórios de informações contribuindo, consequentemente, para determinar a existência de um crime, identificar e responsabilizar os seus agentes, bem como descobrir e recolher prova, no âmbito da investigação."

H2: "As Tecnologias e SI utilizados são a PIIC, na partilha de informação com outros OPC homólogos, e o SIIOP. Adicionalmente, é utilizado o *i2 Analyst´s Notebook* na análise da informação e o *UFED Ultimate* da *Cellebrite* para a extração e análise de prova em suporte eletrónico."

H3: "As principais vantagens decorrentes da utilização das TI são a centralização da informação, bem como a sua supervisão e verificação, em tempo real, aumentando a respetiva qualidade e reduzindo o tempo de resposta às necessidades operacionais. Quanto às desvantagens, as TI exigem uma contínua atualização dos conhecimentos técnicos para a utilização das mesmas e têm por base custos elevados para a sua aquisição e manutenção."

H4: "As principais melhorias a implementar, neste âmbito, são o desenvolvimento da capacidade de armazenamento e análise de grandes quantidades de informação, o que permitiria, de forma automatizada, correlacionar informação proveniente de diversas fontes, assim como investir na formação técnica dos militares."

4.4. Métodos e tipo de abordagem

O método é "um conjunto de procedimentos e normas que permitem conduzir o conhecimento" (Sarmento, 2013, p. 7), determinando o "sentido orientador de uma investigação" (Rosado, 2015, p. 77).

Neste sentido, no cumprimento dos objetivos definidos no TIA, foi adotado o método hipotético-dedutivo (Carvalho, 2009). O modelo hipotético-dedutivo ou de verificação de hipóteses tem por base a formulação de hipóteses ou conjeturas que "melhor relacionam e explicam os fenómenos" (Sarmento, 2013, p. 9). Segundo Oliveira (2011, p. 23), o problema

"deve ser investigado de maneira crítica e racional através de conjeturas e hipóteses", para uma melhor interpretação dos fenómenos observáveis (Quivy & Campenhoudt, 2017).

Pelo que antecede, partiu-se do enquadramento concetual e das entrevistas exploratórias realizadas para a construção da problemática (Capítulos 1 a 3) permitindo, consequentemente, definir o modelo de análise, a partir do qual foram formuladas cinco hipóteses de investigação, designadamente, uma hipótese de partida (HPP), que responde provisoriamente à PP, e quatro hipóteses derivadas (H) que procuram dar resposta às PD. As hipóteses formuladas na presente investigação (Subcapítulo 4.3) serão confrontadas com os dados recolhidos na etapa da Observação e testadas, posteriormente, na fase de Análise das Informações, a fim de confirmar ou refutar a sua validade (Subcapítulo 5.3).

No que concerne ao tipo de abordagem, foi privilegiada a abordagem qualitativa[88], que se traduz num "processo de reflexão e análise da realidade através da utilização de métodos e técnicas para compreensão detalhada do objeto de estudo" (Oliveira, 2011, p. 28). Para tal, foram realizadas duas entrevistas exploratórias e quinze entrevistas confirmatórias (Subcapítulo 4.5) permitindo dar resposta, de forma aprofundada, ao modelo de análise.

4.5. Técnicas de recolha de dados

A recolha de dados compreende um "processo organizado posto em prática para obter informações junto de múltiplas fontes" (Freixo, 2012, p. 220). Por consequência, dado que os modos de investigação fixam "o quadro instrumental da apreensão dos dados e devem (…) harmonizar-se com as técnicas de recolha" (Guerra, 2006, p. 35), foram utilizados como instrumentos de recolha de dados a pesquisa documental e pesquisa bibliográfica[89] (Capítulos 1 a 3) e a realização de entrevistas (Capítulo 5) (Marconi & Lakatos, 2003).

Enquanto instrumento prático de recolha de dados, foram realizadas entrevistas exploratórias e entrevistas confirmatórias[90] (Sarmento, 2013). Por um lado, foram realizadas entrevistas exploratórias, uma vez que explorando o conteúdo da investigação, permitirá "obter conhecimentos exploratórios, que facilitarão a elaboração do inquérito e, posteriormente a interpretação dos resultados" (Sarmento, 2013, p. 33). Por consequência, utilizando como ponto de partida o conhecimento resultante do enquadramento concetual e das entrevistas exploratórias realizadas, foi possível construir um modelo de análise

[88] Anexo F – Relação concetual da abordagem qualitativa.
[89] A pesquisa documental assenta nas fontes primárias (Fortin, Côté & Filion, 2009) como relatórios institucionais e diplomas legais. Por sua vez, a pesquisa bibliográfica, assente em fontes secundárias, traduz as obras literárias e artigos científicos, de autores reconhecidos (Prodanov & Freitas, 2013).
[90] Cf. Apêndice K – Relação entre perguntas de investigação e questões das entrevistas confirmatórias.

suportado em hipóteses de investigação com fundamentação de cariz teórico articulado com a componente prática das entrevistas exploratórias, o que permitiu conduzir uma investigação mais "aproximada dos objetos de estudo" [91] (Vilelas, 2017, p. 177).

Por sua vez, as entrevistas confirmatórias visam "obter informações que validem as suas fontes" (Sarmento, 2013, p. 33). Tanto as entrevistas exploratórias como as entrevistas confirmatórias seguiram uma estrutura semidiretiva, ou seja, através do "uso coerente do guião da entrevista" (Flick, 2005, p. 95) existia a possibilidade de "falar sobre assuntos relacionados com as perguntas", por meio de esclarecimentos adicionais (Sarmento, 2013, p. 34), possibilitando uma investigação mais profunda (Freixo, 2012).

Atendendo às entrevistas, foram elaborados os respeitos Guiões de Entrevista, quer para as entrevistas exploratórias, quer para as entrevistas confirmatórias (Apêndice N e Apêndice O, respetivamente), acompanhados por uma Carta de Apresentação (Apêndice M). As entrevistas foram realizadas por videoconferência e por contacto telefónico e, em casos pontuais, por correio eletrónico, sendo pedida autorização aos entrevistados para proceder à gravação das mesmas. Posteriormente, realizou-se a transcrição das entrevistas, sendo remetidas aos entrevistados, a fim de obter a sua validação.

4.6. Caracterização do contexto de observação

A amostragem, segundo Fortin, Côté e Filion (2009), traduz um processo através do qual um grupo de pessoas ou uma porção da população (amostra) é selecionada, por forma a representar a totalidade de uma população.

Consequentemente, foi adotada a modalidade de amostragem criterial, ou seja, foi selecionada uma amostra "segundo um critério pré-definido" (Coutinho, 2018, p. 95). A seleção da amostra foi sustentada em dois critérios principais: por um lado, o desempenho de funções diretamente ligadas à IC e/ou Sistemas e TI e, por outro lado, não desempenhando atualmente essas funções, foi considerada a experiência profissional neste domínio.

Deste modo, no âmbito das entrevistas exploratórias, foram selecionados dois militares da categoria de Oficial que, dado o seu percurso profissional, possuem profundos conhecimentos ao nível das TI e da IC, no domínio das Unidades Territoriais da GNR. Por um lado, o Major (Maj) Tiago Lopes, dada a sua experiência no âmbito das TI e na IC, tendo desempenhado funções de Chefe da Repartição de Análise Digital Forense e, por outro lado, o Maj Hugo Carneiro, com funções de Chefe da Repartição de Sistemas Operacionais.

[91] Cf. Apêndice L – Procedimento científico: Da pergunta de partida às hipóteses de investigação.

No âmbito das entrevistas confirmatórias, foram selecionados Oficiais da GNR pertencentes ao CO e às SIIC[92]. No caso do CO, foram escolhidos os Diretores e Chefes das estruturas diretamente interligadas com a problemática da investigação. Quanto às Unidades Territoriais, foram entrevistados oito Oficiais Chefes de SIIC e um Oficial com função de Adjunto do Chefe da SIIC, em Unidades Territoriais do Norte, Centro e Sul do país.

4.7. Tratamento e análise de dados

A análise de conteúdo é, segundo Coutinho (2018, p. 217), "um conjunto de técnicas que permitem analisar de forma sistemática um corpo de material textual". Assim, para o tratamento e análise de dados, foi seguido o modelo proposto por Sarmento (2013, p. 53), assente na "categorização dos dados brutos da entrevista", organizando-os e atribuindo-lhes significado (Freixo, 2012).

Após a transcrição das entrevistas, procedeu-se à sua leitura vertical, isto é, adotando o critério da ordem cronológica da realização das entrevistas, foram lidas sequencialmente todas as respostas concedidas. Seguidamente, realizou-se a leitura transversal de cada questão adotando, nesta fase, uma linha de leitura horizontal. Posteriormente, procedeu-se à diferenciação dos segmentos do texto das entrevistas respeitantes a uma determinada característica ou atributo comum, isto é, a uma subcategoria[93] constituindo, assim, as Unidades de Registo (UR)[94]. Estas unidades estão associadas a Unidades de Contexto[95], segundo uma codificação numérica e cromática das entrevistas[96].

Adicionalmente, foram criadas Unidades de Enumeração (UEn), que quantificam o número de vezes que a UR é repetida. Procedeu-se, ainda, à elaboração de matrizes de Unidades de Contexto e de Registo, por cada questão de entrevista, conforme o Apêndice S. As Unidades de Contexto foram "escritas a cores diferentes, para uma melhor identificação", sendo que as UR correspondentes, apresentam a mesma cor da Unidade de Contexto (Sarmento, 2013, p. 64) (Apêndice S). Por fim, foram discutidos os resultados obtidos, mediante a análise das respostas às entrevistas e confrontados com a análise desenvolvida nos Capítulos 1 a 3, como definido no desenho de investigação elaborado no Apêndice I.

[92] Cf. Apêndice P – Caracterização dos entrevistados.
[93] As subcategorias são conjuntos de UR, "agregadas segundo as particularidades comuns, que contribuem para caracterizar as categorias, a que o investigador atribui uma designação" (Sarmento, 2013, p. 54).
[94] As UR são "fragmentos mínimos de conteúdo, que exprimem uma caraterística ou atributo e fazem parte de uma dada subcategoria" (Sarmento, 2013, p.54).
[95] As Unidades de Contexto compreendem segmentos do texto que integram as UR e que permitem "compreender o significado das unidades de registo" (Sarmento, 2013, p. 54).
[96] Cf. Apêndice R – Codificação das respostas às entrevistas confirmatórias.

CAPÍTULO 5
APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS

5.1. Apresentação, análise e discussão das entrevistas exploratórias

As entrevistas exploratórias (Apêndice Q) foram realizadas com o fim de desenvolver e orientar a investigação num suporte empírico e conhecimento mais aprofundado e, por consequência, apoiar a elaboração do modelo de análise e das entrevistas confirmatórias.

Quanto às debilidades da estrutura de IC das Unidades Territoriais da GNR, o Maj Hugo Carneiro salienta limitações ao nível das ferramentas tecnológicas disponíveis, bem como em termos da quantidade de recursos humanos. Por sua vez, o Maj Tiago Lopes defende que "o atual conceito das vertentes funcionais da IC (…) estão desajustadas à realidade funcional", não existindo total capacidade de investigação em determinadas áreas.

Quanto ao elemento base das TI, as informações, ambos os entrevistados afirmaram que estas são fundamentais na IC, tanto no combate/repressão da criminalidade, como no âmbito da prevenção. Partindo da dualidade entre informações policiais e criminais, os entrevistados afirmam que as informações policiais são destinadas, essencialmente, a antecipar e planear operações, prever fenómenos específicos e orientar o policiamento nas suas diferentes vertentes o que permite, consequentemente, uma elevada capacidade de proatividade policial. Quanto às informações criminais, os dois entrevistados referiram que estas informações são fundamentais na componente da repressão criminal, sendo que a sua centralização e análise, com base em fontes humanas (interrogatórios e inquirições, por exemplo), prova documental e/ou acesso a bases de dados é fundamental, uma vez que permite, no âmbito de uma investigação em curso e cumprindo as finalidades do inquérito penal, averiguar a existência de um crime, identificar os seus autores e recolher as respetivas provas, mediante uma estreita colaboração com as AJ.

Neste sentido, o Maj Hugo Carneiro referiu a importância do SIIOP-P, enquanto ferramenta de recolha e registo de informação, que permite "uniformizar, padronizar e sistematizar a recolha de informação", bem como a sua supervisão e verificação, aumentando a respetiva qualidade. Por sua vez, o Maj Tiago Lopes suporta as potencialidades das TI em ferramentas de análise de informação criminal, como o *i2 Analyst´s Notebook*, utilizado pelos NAIIC, assim como em ferramentas digitais forenses,

como o *Cellebrite UFED Ultimate*, para a recolha e análise de prova, em suporte eletrónico ou em redes, utilizado pelos Núcleos Digitais Forenses (NDF).

Como proposta de melhoria da utilização dos Sistemas e TI pela estrutura de IC das Unidades Territoriais, o Maj Hugo Carneiro defende a importância do desenvolvimento de uma ferramenta central, com capacidade de armazenamento e análise de grandes quantidades de informação. Por seu turno, o Maj Tiago Lopes acrescenta o investimento na formação dos militares da estrutura de IC, bem como a aquisição de novas ferramentas tecnológicas.

5.2. Apresentação, análise e discussão das entrevistas confirmatórias

O presente Subcapítulo integra a apresentação, análise e discussão dos dados recolhidos no trabalho de campo, tendo como base o conhecimento resultante das fases de Exploração (Leituras e Entrevistas Exploratórias), da Problemática (Revisão da Literatura), do Modelo de Análise e da Observação (Entrevistas Confirmatórias). Os aspetos fulcrais subjacentes às respostas de cada entrevistado, estão vertidos nas matrizes cromáticas (Apêndice S), nas quais se enquadram as UR e as Unidades de Contexto correspondentes.

Em virtude de não se encontrarem a desempenhar funções na estrutura de IC, os Entrevistados 7 e 8 (E7 e E8) consideraram, em questões pontuais, não dispor de elementos suficientes para dar resposta às mesmas.

5.2.1. Apresentação, análise e discussão da Questão n.º 1

A Questão n.º 1 tem como finalidade compreender as principais debilidades da estrutura de IC das Unidades Territoriais da GNR.

Atendendo à Tabela n.º 1, compreendemos que 69% dos entrevistados entendem que, uma das limitações a destacar, diz respeito à quantidade de recursos humanos disponíveis no quadro orgânico das Unidades Territoriais. Nas palavras de E6, "o principal problema da Investigação Criminal prende-se com a falta de recursos humanos", nomeadamente na sua vertente operativa (E2, E12, E15), sendo que deveria existir um reforço e gestão das Unidades (E12) utilizando como critério a sua realidade criminal (E4) e o "seu volume de trabalho" (E5). De acordo com E2, "não se trata da existência de corte de efetivo", mas de um desvio dos recursos humanos existentes para dar resposta a novas exigências que conduziram ao aparecimento de novas valências. Esta limitação vem condicionar, por exemplo, a capacidade dos NIAVE para cumprir a exigência de, "em todas as situações que sejam consideradas de risco elevado, o inquérito seja elaborado e entregue à AJ em setenta

e duas horas", dificultando a capacidade de resposta a esta necessidade de celeridade processual (E2). Por conseguinte, com o Despacho n.º 18/14 - OG (E1, E2), além da extinção das Equipas de Investigação e Inquérito dos Postos Territoriais, veio trazer condicionalismos em termos de efetivo dos NAO, comprometendo a recolha de prova para o Inquérito (E2).

De igual modo, E1, E4, E5, E12, E13, E14 e E15 apontam a falta de investimento na formação, quer em termos da "formação base" (E14), quer ao nível da "formação de atualização" (E5, E14). E4 afirma, inclusivamente, que assistimos a "estruturas altamente debilitadas em termos de efetivo formado". Assim, 54% dos entrevistados consideram que, como refere Lopes (2017), os OPC devem desenvolver o seu conhecimento técnico, uma vez que é determinante para a "eficácia da investigação criminal" (Valente, 2019, p. 515).

Por sua vez, a IC carece de investimento nos seus recursos tecnológicos (54%), visto que uma das principais condicionantes de uma investigação eficiente, se prende com a utilização de equipamentos convencionais e obsoletos (Souza, 2016).

No que concerne à "Partilha de Informação" (38%), E1, E4, E5 e E10 salientam a falta de ligação entre as Unidades Territoriais, em resultado da organização estrutural atualmente implementada na IC. Como refere E4, "não existe, efetivamente, uma centralização do que é a Investigação Criminal". Assim, uma vez que, progressivamente, os crimes praticados como "furtos de residências, furto de interior de veículos, entre outros" (E10) ultrapassam a zona de ação do próprio Comando Territorial, é necessária uma estreita coordenação e partilha de informação entre as SIIC (E1, E4, E10), para uma "rápida perceção e combate" destes fenómenos criminais (E10). Por consequência, E4 salienta a necessidade de recurso a "conhecimentos próprios, por via informal" para dirimir esta descentralização.

No que diz respeito às entrevistas exploratórias, foram igualmente apontadas limitações quanto à quantidade de recursos humanos e TI disponíveis.

Tabela n.º 1 - Matriz de análise de conteúdo da Questão n.º 1

Questão n.º 1																		
Categoria	**Subcategorias**	**UR**	**Entrevistados**														**UEn**	**Resultado (%)**
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**		
Debilidades da estrutura de IC das Unidades Territoriais da GNR	Normativa	**1.1**	X															1	1/13 (8%)
	Partilha de Informação	**1.2**	X			X	X				X	X						5	5/13 (38%)
	Formação	**1.3**	X			X	X							X	X	X	X	7	7/13 (54%)
	Investimento Tecnológico	**1.4**	X		X	X	X						X		X		X	7	7/13 (54%)
	Recursos Humanos	**1.5**		X	X	X	X	X						X	X	X	X	9	9/13 (69%)
	Organização/Gestão Estrutural	**1.6**				X	X				X							3	3/13 (23%)

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

5.2.2. Apresentação, análise e discussão da Questão n.º 2

A Questão n.º 2 tem como finalidade identificar os principais contributos das informações, utilizando como referência as informações policiais e as informações criminais, na prossecução das atividades de IC.

Analisando a Tabela n.º 2, concluímos que, a totalidade dos entrevistados (100%) considera que as informações desempenham um papel essencial, por um lado na prevenção dos fenómenos criminais e, por outro lado, na sua repressão, interligando a função das informações policiais, genericamente, ao domínio da prevenção e das informações criminais à repressão da criminalidade. Contudo, foi considerado que, tanto as informações policiais, como as informações criminais produzem efeitos nos dois domínios, isto é, na prevenção e na repressão criminal (E8, E9, E10, E12, E13, E14, E15), visto que se "encontram separadas por uma linha ténue" (E10), apoiando os decisores nos seus diversos níveis, "sejam eles estratégico, operacional ou tático", tal como referido por E13, à semelhança de Bispo (2004).

Em conformidade com a hierarquia subjacente à sequência DIKI *continuum (Data-Information-Knowledge-Intelligence)* (Ratcliffe, 2008), E2 começa por referir que a informação policial é "toda aquela notícia que depois de ser trabalhada torna-se informação" e para a qual não foi elaborado um auto de notícia, ou seja, atribuído um Número Único Identificador de Processo Crime (NUIPC), mas que pode produzir efeitos na sua elaboração e na prossecução das respetivas diligências (E8). Estando intimamente ligadas à prossecução direta das missões legalmente atribuídas a serviços de natureza policial (E5, E8, E15), as informações policiais permitem antecipar e/ou acompanhar ações ou eventos criminais (E6, E10, E12), realizar estudos comparativos (E2), caracterizar os *modus operandi* (E1, E15), determinar as suas causas (E6, E7) e agilizar medidas de segurança (E1, E3, E12, E13). Esta abordagem traduz o conceito de informações policiais definido por Alves (2012), enquanto conjunto de informações determinantes na implementação de medidas preventivas.

Por seu turno, E1, E3, E6 e E8 caracterizam as informações criminais como o conjunto de elementos inseridos no domínio de um processo crime, materializando prova de investigação, ou seja, "estão diretamente relacionadas com a atividade de IC" (E5). Neste sentido, em conformidade com Sousa (2007), as informações criminais constituem ferramentas/técnicas fundamentais na investigação, pressupondo que foram adquiridas com base nas diligências realizadas em sede de autos de notícia (Moleirinho, 2009).

Contudo, segundo E2, E4, E5, E12 e E15, as informações policiais e as informações criminais, apesar das suas funções distintas, complementam-se. Como afirma E2, "só é

possível ter bons resultados quando, efetivamente, existe (…) uma complementaridade". E4 reforça esta ideia acrescentando que, "ao nível dos Comandos Territoriais, tudo se articula", ou seja, as SIIC agrupam, tanto as informações policiais, como as informações criminais.

Por consequência, aludindo ao PCCCOFSS, E8 suporta que, na atividade de IC, devem ser consideradas estas duas dimensões, isto é, a dimensão da prevenção criminal, a "primeira das suas dimensões" (E8) e, em concreto, a dimensão da IC (SSI, 2010), dado que a prevenção se concretiza, igualmente, na prossecução de atos de IC (Valente, 2019).

Quanto às entrevistas exploratórias, os contributos das informações bifurcaram-se, de igual modo, nos dois domínios centrais: a prevenção e a repressão da criminalidade.

Tabela n.º 2 - Matriz de análise de conteúdo da Questão n.º 2

Questão n.º 2																		
Categoria	Subcategorias	UR	Entrevistados														UEn	Resultado (%)
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Contributos das Informações na IC	Repressão	2.1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	15	15/15 (100%)
	Prevenção	2.2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	15	15/15 (100%)

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

5.2.3. Apresentação, análise e discussão da Questão n.º 3

A análise da Questão n.º 3 tem como objetivo interpretar como são utilizadas as informações criminais pela estrutura de IC, na resposta aos fenómenos criminais.

De acordo com os entrevistados (50%), as informações criminais destinam-se a cumprir as "Finalidades do Inquérito", dando corpo a todas as diligências efetuadas no decurso de uma investigação, isto é, de um processo crime em concreto. Tal como referido por E1, "passamos a ter um grupo, (…) um suspeito e vamo-nos focar naquele grupo, naquele indivíduo". Deste modo, vamos ao encontro da interpretação do crime proposta por Paulsen e Robinson (2009), a partir da qual, o criminoso, enquanto indivíduo que viola as normas, integra um dos quatro elementos centrais da sua classificação.

Assim, uma vez que as informações criminais se inscrevem no "âmbito da atividade reportada à investigação criminal" (Clemente, 2010, p. 159), 50% dos entrevistados reforçam esta ideia, salientando que estas informações estão na base daquilo que são as finalidades da IC, previstas no art.º 1.º da LOIC e, de igual modo, as finalidades do inquérito (n.º 1 do art.º 262.º do CPP), ou seja, permitem determinar a existência de um crime,

identificar e responsabilizar os seus autores e recolher provas, no âmbito do processo, como referido pelo Maj Tiago Lopes e pelo Maj Hugo Carneiro nas entrevistas exploratórias.

Por sua vez, as informações criminais são utilizadas para efeitos de "Análise" (64%), por um lado, pela DIC, ao nível do CO (E4, E10, E13) e, por outro lado, pelos NAIIC, ao nível das Unidades Territoriais (E1, E3, E4, E5, E6, E9, E10, E13), na identificação, estudo e acompanhamento dos fenómenos criminais, permitindo estabelecer associações, isto é, "criar relações entre diversas entidades (pessoas, documentos, veículos, locais, processos, etc.)" (E6) e, a jusante, servir de base para conhecer "novos modos de atuação dos suspeitos por tipologia criminal" (E6, E9, E15). Para este fim, os NAIIC são responsáveis pela elaboração de relatórios de informações com origem, por vezes, em pedidos de pesquisa dos órgãos operativos (E1, E5) permitindo, como referido por Fernandes e Valente (2005), suportar a condução da IC e apoiar os OPC na decisão das táticas e técnicas a adotar.

Por consequência, a recolha, análise e difusão das informações criminais estão na base da "Coordenação/Articulação" (64%) entre os órgãos da estrutura de IC das Unidades Territoriais (E1, E3, E4, E5), bem como na partilha e cooperação com outras entidades (E6).

É com base nesta reciprocidade que, os relatórios de informações são disseminados aos órgãos operativos, orientando o "Planeamento e Intervenção" (64%), ou seja, permitindo aos investigadores direcionar a investigação (E6, E12, E13, E15), "antecipar movimentos, locais e datas" (E12), estabelecer os procedimentos e estratégias de atuação, de recolha de informação e de investigação a adotar (E3), bem como os meios necessários a alocar (E3, E6, E13, E15) e, desejavelmente, "efetuar detenções em flagrante" (E12). Conforme Paiva (2019), uma estrutura eficaz de IC requer estratégia e planeamento, permitindo "criar novas linhas de investigação" (E6) e suportar o processo de Tomada de Decisão (21%).

Tabela n.º 3 - Matriz de análise de conteúdo da Questão n.º 3

Questão n.º 3																			
Categoria	**Subcategorias**	**UR**	**Entrevistados**															**UEn**	**Resultado (%)**
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**		
Utilização das Informações Criminais	Finalidades do Inquérito	3.1	X		X		X	X		X			X				X	7	7/14 (50%)
	Tomada de Decisão	3.2	X										X		X			3	3/14 (21%)
	Planeamento e Intervenção	3.3	X		X	X	X	X				X		X	X		X	9	9/14 (64%)
	Análise	3.4	X		X	X	X	X			X	X		X	X			9	9/14 (64%)
	Natureza do Crime	3.5		X	X		X	X			X							5	5/14 (36%)
	Coordenação/ Articulação	3.6	X	X	X		X	X				X	X		X	X		9	9/14 (64%)

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

5.2.4. Apresentação, análise e discussão da Questão n.º 4

A resposta à Questão n.º 4 tem como objetivo enumerar os principais Sistemas e TI utilizados e/ou de apoio aos órgãos da estrutura de IC das Unidades Territoriais da GNR.

No âmbito das TI, foram identificados, com maior expressividade, o *i2 Analyst´s Notebook* (53%), o *Cellebrite UFED Ultimate* (40%) e o sistema AFIS (33%). O *i2 Analyst´s Notebook*, enquanto ferramenta utilizada, essencialmente, pelos NAIIC, ao nível do tratamento e análise das informações permite, segundo E1, E2, E4 e E8, estabelecer associações, identificar relações e sintetizar dados, conforme Machado e Vilalta (2018). Por sua vez, de acordo com E1, E2, E4 e E5, o *Cellebrite UFED Ultimate* desempenha um papel único no acesso e recolha dos dados constantes em equipamentos digitais, como o telemóvel ou o computador, tal como referido por Khan e Mansuri (2018). No que concerne ao sistema AFIS, trata-se de uma ferramenta utilizada pela vertente de Criminalística no armazenamento, pesquisa e comparação de dados lofoscópicos (E2, E4, E5, E6).

No domínio dos SI, foram destacados o SIIOP (100%) e os Sistemas dos Serviços Partilhados (67%), nomeadamente, o TMENU, o SISII, o SEGURNET, o SCoT, entre outros, fundamentais no apoio transversal a todas as valências de IC.

Ao nível das entrevistas exploratórias, foram enumerados o *i2 Analyst´s Notebook*, o *Cellebrite UFED Ultimate*, o SIIOP e a PIIC, na partilha de informação com outros OPC.

Tabela n.º 4 - Matriz de análise de conteúdo da Questão n.º 4

Questão n.º 4																			
Categorias	**Subcategorias**	**UR**	**Entrevistados**															**UEn**	**Resultado (%)**
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**		
TI na estrutura de IC da GNR	*i2 Analyst´s Notebook*	**4.1.1**	X	X		X	X	X		X	X						X	8	8/15 (53%)
	QGIS	**4.1.2**	X															1	1/15 (7%)
	PowerBI	**4.1.3**	X															1	1/15 (7%)
	FTK	**4.1.4**	X															1	1/15 (7%)
	Cellebrite UFED Ultimate	**4.1.5**	X	X			X	X			X		X					6	6/15 (40%)
	AFIS	**4.1.6**		X		X	X	X									X	5	5/15 (33%)
	ArcGIS	**4.1.7**	X			X	X											3	3/15 (20%)
	4IQ	**4.1.8**		X														1	1/15 (7%)
	Paragon	**4.1.9**					X										X	2	2/15 (13%)
	NUIX	**4.1.10**						X										1	1/15 (7%)
	PC-Crash	**4.1.11**						X										1	1/15 (7%)
SI na estrutura de IC da GNR	SIIOP	**4.2.1**	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	15	15/15 (100%)
	Serviços Partilhados	**4.2.2**	X		X	X				X	X	X		X	X	X	X	10	10/15 (67 %)
	PIIC	**4.2.3**			X	X	X								X			4	4/15 (27%)

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

5.2.5. Apresentação, análise e discussão da Questão n.º 5

A análise da Questão n.º 5 visa enumerar e caracterizar as potencialidades resultantes da utilização dos Sistemas e TI pela estrutura de IC das Unidades Territoriais da GNR.

Uma das principais potencialidades apresentadas é a capacidade de Análise e Sintetização da Informação, conforme 87% dos entrevistados. O recurso a estas ferramentas permite, para efeitos de análise, a construção de gráficos (E1, E6), estabelecer correlações (E3, E4, E12, E15) através de matrizes de comparação/associação (E13), bem como construir diagramas de conexões (E1, E3, E4, E13), cronogramas e fluxogramas (E13), tendo em vista estabelecer *hotspots* de criminalidade (E1, E5), georreferenciar os fenómenos criminais (E2, E4, E5), compreender os *modus operandi* emergentes (E1, E3) e, por consequência, determinar o respetivo padrão (E3, E12) e tendências criminais (E7). Assim, em analogia com Bispo (2004), o recurso às TI na análise de informação criminal tem por base, não apenas os factos históricos, mas também, os elementos atuais orientados para uma visão prospetiva, contribuindo para compreender, tanto a localização dos problemas criminais, como a sua variação espacial ao longo do tempo (Paulsen & Robinson, 2009).

De acordo com E1, E3, E4, E5, E12 e E15 as múltiplas soluções apresentadas são concretizadas através de ferramentas como o *i2 Analyst´s Notebook* e o QGIS e/ou ArcGIS no mapeamento do crime, cujo produto constituirá a base dos relatórios de informações.

Paralelamente, segundo E2 e E6, os contributos das TI produzem efeitos, de igual modo, ao nível da investigação de acidentes de viação com sinistralidade grave e de elevada complexidade. Através da coordenação entre o NICAV e a DIC, são utilizadas ferramentas como o *PC-Crash*, que permitem a análise e a reconstrução de colisões de veículos.

Por seu turno, mediante a análise, sintetização e centralização da informação, as TI permitem "ampliar os antecedentes dos suspeitos, as associações que possam existir" (E6), estabelecer novas linhas de investigação (E6, E13, E15), bem como direcionar, por um lado, o patrulhamento dos Postos e Destacamentos Territoriais (E5, E13), identificando "locais onde requerem a adoção de medidas preventivas" (E1) e, por outro lado, estabelecer os métodos e meios de recolha de informação pelos órgãos operativos (E1, E3, E5). Assim, tal como refere Braz (2016), a evolução das tecnologias veio dar corpo a diversas técnicas e metodologias que contribuem para uma superior eficácia na investigação.

Todavia, as potencialidades das TI não se esgotam na análise e sistematização da informação. A partir destas, é garantida uma Pesquisa e Recolha da Informação (87%), não só em quantidade, como em qualidade, imprimindo "rapidez e fiabilidade" na recolha da

informação (E9). Segundo E5, a utilização de *softwares* de interceção de comunicações, como é o caso do sistema *Paragon*, sob a tutela da Polícia Judiciária (PJ), além da recolha e leitura do seu conteúdo, permitem "identificar onde está o nosso alvo através do nosso sistema de triangulação, utilizado para vigilâncias, com recurso a escutas telefónicas" (E5).

Em complementaridade, a fim de garantir a vigilância e recolha de informações de indivíduos suspeitos, são utilizados *softwares* que permitem o acompanhamento dos aparelhos de vigilância remota, tanto a locais, como a pessoas (E2, E5, E15), rentabilizando os meios que seriam necessários para efetuar os seguimentos e vigilâncias (E2). Em adição, a pesquisa e recolha de informação é prosseguida através de ferramentas de pesquisa *Open Source Intelligence* (OSINT), como o 4IQ, utilizado pelo Centro de Informações da Guarda (E2) que permitem, com recurso às redes sociais e outras fontes abertas (E9), investigar indivíduos suspeitos, conhecer a sua localização, rotinas e vínculos/ligações pessoais (E3, E5) e comunicar essas informações aos órgãos de IC das Unidades Territoriais, para efeitos de análise e investigação, em coordenação com a AJ competente (E2, E3).

No mesmo sentido, *softwares* como o *Cellebrite UFED Ultimate* (E1, E2, E5, E6, E9, E11) e o *Forensic Toolkit* (FTK) (E1), permitem a recolha/extração de dados de telemóveis e/ou computadores, incluindo dados eliminados/apagados, a fim de serem analisados (E2, E6, E12). Estas ferramentas são utilizadas pelos NDF (E3, E5), por exemplo, em casos de violência doméstica (E5), contribuindo para "aprofundar o seu conteúdo" (E2).

Porém, a aplicação destas ferramentas tecnológicas pelos NDF não se limita à pesquisa ou recolha de informação. Estas desempenham um papel único na aquisição de prova nos processos criminais (UR 5.5) (E2, E4, E6, E11). O recurso a estes *softwares* permite "a correta preservação de dados digitais" (E5), visto que esses dados são recolhidos e armazenados com a finalidade de constituírem prova (E2, E4, E5, E6, E8, E9, E11, E12).

De igual modo, o sistema AFIS, sistema comum aos OPC e gerido pela PJ (E6), é utilizado pela Criminalística, não apenas na pesquisa, armazenamento e comparação dos vestígios lofoscópicos recolhidos, mas também na sua preservação em suporte eletrónico (60%) materializando, segundo E4, o "único método para o qual não existe contra-argumentação". Assim, através de ferramentas como o sistema AFIS, a identificação de vestígios (33%) representa, igualmente, uma das potencialidades das TI, visto que "coloca, inequivocamente, um indivíduo num certo local ou a manusear um certo objeto" (E6). Neste sentido, é reforçada a crescente importância das TI na preservação de "provas materiais que futuramente irão corroborar os factos relatados" (Costa & Machado, 2012, p. 130), dado os "níveis de rigor e de certeza que garante[m] no plano probatório" (Braz, 2020, p. 168).

Para além disso, os Sistemas e TI permitem o Armazenamento e Centralização da Informação (53%) num repositório único (E10), como é o caso do SIIOP, no qual é registada toda a atividade operacional (E5, E7, E8, E10, E11), fornecendo informações detalhadas, quer sobre os dados e notícias resultantes dessa atividade (E8, E11) e sobre a sua estatística criminal (E2), quer sobre as informações vertidas nos autos de notícia e crimes registados ao longo do tempo (E5).

Deste modo, é possível "o arquivo e consulta dos processos" (E12), contribuindo para a sua desmaterialização (40%), fruto da capacidade de armazenamento e centralização de toda a informação recolhida (E11). Assim, como refere Castro (2018), as TI, para além da recolha, armazenamento, análise e difusão da informação, contribuem decisivamente para o aumento, quer da quantidade, quer da qualidade da informação (E9, E11), bem como para a redução do tempo de resposta operacional (E13).

Adicionalmente, a utilização das TI permite identificar, no âmbito de uma investigação, as lacunas processuais (UR 5.2) (27%), dado que através da agregação das diligências recolhidas, é possível reconhecer "os elementos probatórios em falta" (E1).

Atendendo às entrevistas exploratórias, foi sublinhado o papel das TI na análise e sintetização da informação, bem como na recolha e preservação de elementos de prova.

Tabela n.º 5 - Matriz de análise de conteúdo da Questão n.º 5

Questão n.º 5																		
Categoria	**Subcategorias**	**UR**	**Entrevistados**														**UE n**	**Resultado (%)**
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**		
Potencialidades da utilização dos Sistemas e TI na IC	Análise/ Sintetização da Informação	5.1	X	X	X	X	X	X	X	X	X		X	X	X		X	13	13/15(87%)
	Identificação de Necessidades Processuais	5.2	X			X	X			X								4	4/15 (27%)
	Pesquisa/Recolha de Informação	5.3	X	X	X	X	X	X		X	X		X	X	X	X	X	13	13/15(87%)
	Rentabilização dos Meios	5.4		X								X	X	X				4	4/15 (27%)
	Preservação da Prova/Valor Probatório	5.5		X		X	X	X		X	X		X	X			X	9	9/15 (60%)
	Identificação de Vestígios	5.6		X		X	X	X									X	5	5/15 (33%)
	Partilha de Informação	5.7			X		X	X	X	X			X					6	6/15 (40%)
	Armazenamento/ Centralização da Informação	5.8			X	X	X	X	X	X		X	X					8	8/15 (53%)
	Desmaterialização de Procedimentos	5.9				X	X	X		X			X	X				6	6/15 (40%)
	Segurança da Informação	5.10											X					1	1/15 (7%)

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

5.2.6. Apresentação, análise e discussão da Questão n.º 6

A análise da Questão n.º 6 tem como objetivo compreender se, os contributos decorrentes da utilização das TI pelos órgãos da estrutura de IC das Unidades Territoriais da GNR, são suficientes para dar total resposta às exigências criminais atuais.

Atendendo à Tabela n.º 6, concluímos que, 86% dos entrevistados consideram os contributos das TI como "Insuficientes" para dar uma resposta cabal aos fenómenos criminais atuais, sendo esta classificação dividida em dois argumentos principais. Por um lado, os meios tecnológicos atualmente utilizados não acompanham, na mesma proporção, as exigências criminais emergentes. Por outro lado, as TI não poderão ser consideradas de forma isolada, ou seja, o papel do elemento humano é insubstituível (E1, E2, E4, E14).

Considerando as causas tecnológicas, E1 afirma que "temos carências ao nível de um conjunto de tecnologias", uma vez que "alguns recursos a este nível (…) estão obsoletos e a sua utilização não está devidamente regulada internamente" (E12). As necessidades tecnológicas referidas por E1, E2, E4, E8, E9, E12 e E15, resultam da constante evolução tecnológica que está na base, cada vez mais, da criminalidade atual. Assim, a rápida capacidade de reorganização e de rearticulação dos fenómenos criminais, resultante dos avanços tecnológicos (E1, E2, E4, E9), vieram dinamizar as atividades criminais tradicionais viabilizando "a prática de novos crimes" (E9) e a adoção de "providências de contramedidas para a utilização destas tecnologias" (E2). É corroborada, portanto, a premissa de que, "se o crime evolui, a resposta ao crime deve evoluir" (Valente, 2019, p. 67), exigindo um acompanhamento e adaptação dos meios tecnológicos, sob a possibilidade de obsolescência para uma resposta eficaz e oportuna às novas formas de criminalidade (Bose & Kabir, 2017).

Por seu turno, o nível de fiabilidade e qualidade dos dados produzidos pelas TI está dependente do elemento humano, pois é este quem faz todo o trabalho de investigação, recolhe e seleciona a informação que será introduzida e trabalhada nas TI (E1, E4, E14). E2 complementa esta ideia acrescentando que, as tecnologias não substituem o trabalho HUMINT, ou seja, "o trabalho que tem de se fazer no terreno", assim como a natureza determinante da prova testemunhal, em sede jurídico-processual. Neste sentido, de acordo com 86% dos entrevistados, embora o recurso às TI se traduza numa intervenção operacional mais eficaz dos órgãos de IC, por si sós, não são suficientes (Koper, Lum & Willis, 2014), exigindo um estreito vínculo entre os recursos humanos e tecnológicos (Carvalho, 2010).

Por sua vez, E5 e E6 consideram que, apesar de "querermos sempre mais" (E5) e de ser "uma área com tendência para crescer" (E6), as atuais TI utilizadas pela estrutura de IC,

possuem a qualidade e requisitos necessários para dar resposta às atuais exigências criminais. Nos termos das entrevistas exploratórias, as TI foram classificadas como "Insuficientes", na medida em que, como anteriormente referido, o elemento humano é indissociável da vertente tecnológica.

Tabela n.º 6 - Matriz de análise de conteúdo da Questão n.º 6

Questão n.º 6																		
Categoria	**Subcategorias**	**UR**	**Entrevistados**														**UEn**	**Resultado (%)**
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
Aptidão das TI, utilizadas pelas SIIC, na resposta às exigências criminais	Insuficientes	6.1	X	X	X	X				X	X	X	X	X	X	X	X	12	12/14 (86%)
	Suficientes	6.2					X	X										2	2/14 (14%)

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

5.2.7. Apresentação, análise e discussão da Questão n.º 7

A apresentação, análise e discussão da Questão n.º 7 tem como finalidade enumerar as principais debilidades subjacentes, quer à utilização, quer ao funcionamento dos Sistemas e TI, pela estrutura de IC das Unidades Territoriais da GNR.

Conforme a Tabela n.º 7, verificamos que, um dos pontos fracos a destacar se prende com o "Registo e Acesso à Informação" (54%). Neste campo, E1, E2, E4, E5, E6 e E10 afirmam que, ao nível do SIIOP, uma das principais limitações diz respeito à dificuldade de pesquisa e análise da informação que é registada. Por um lado, esta limitação decorre do facto de toda a informação que integra o corpo dos autos de notícia ser dificilmente pesquisável, de forma automática, exigindo uma análise da informação "auto a auto" e a sua extração do sistema, a fim de ser "trabalhada à parte" (E4, E5). Por outro lado, para que todos os dados presentes no descritivo do auto de notícia sejam, posteriormente, pesquisáveis e extraídos, automaticamente, terão de ser criadas no sistema, peças individuais para cada dado inserido. Assim, é fundamental o registo de toda a informação de que se tem conhecimento e que este seja corretamente realizado pelos órgãos de IC o que, para E4, E5 e E10, nem sempre se verifica, dificultando o acesso à informação ou, até mesmo, perdendo-se essa informação (E1, E2, E4, E5, E6). Como referido por E1, "não chega só a informação estar carregada no sistema se não a conseguirmos extrair", dificultando a sua análise (E4).

Por seu turno, além da necessidade de conhecimentos técnicos, carecendo da respetiva formação (23%), e da quantidade de recursos humanos (31%), o leque de

ferramentas tecnológicas disponíveis na estrutura de IC das Unidades Territoriais é, igualmente, um constrangimento neste domínio (54%), conforme mencionado nas entrevistas exploratórias. Esta limitação é levantada, principalmente, no domínio digital forense, no qual, segundo E1, E4, E5, E9 e E15, são necessários equipamentos mais recentes e capazes para dar resposta aos avanços tecnológicos utilizados, atualmente, na prática de crimes. Em complemento, E12 aponta esta limitação ao nível da vertente operativa, no que concerne ao défice de aparelhos de vigilância remota disponíveis. Deste modo, o recurso às TI, converteu-se em "necessidades naturais" (Rascão, 2008, p. 97) na resposta aos fenómenos criminais atuais que, consequentemente, assumem "inúmeras formas de manifestação" (Santos, 2015, p. 39).

Igualmente, E4 e E5 salientam constrangimentos logísticos, por um lado, pelo distanciamento das estações AFIS em relação a determinadas SIIC e, por outro lado, o acesso ao conteúdo das escutas telefónicas, em sede de investigação, carece de deslocação dos militares às instalações da PJ, visto que o sistema *Paragon* se encontra sob a sua tutela (E5).

Por sua vez, E3, E4 e E5 salientam que se verifica uma falta de mentalidade de partilha de informação (UR 7.7), uma vez que nem sempre é introduzido no sistema toda a informação de que se tem conhecimento pois, como afirma E5, "informação é poder".

Por fim, E1, E4, E5, E12, E13 e E15 acrescentam a falta de licenças completas e/ou a utilização de versões desatualizadas (UR 7.4) condicionando, quer o trabalho de análise dos NAIIC, como a capacidade de extração e análise de dados dos NDF.

Tabela n.º 7 - Matriz de análise de conteúdo da Questão n.º 7

Questão n.º 7																			
Categoria	**Subcategorias**	**UR**	**Entrevistados**															**UEn**	**Resultado (%)**
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**		
Debilidades da utilização e funcionamento dos Sistemas e TI	Diversidade Tecnológica	7.1	X			X	X				X	X		X			X	7	7/13 (54%)
	Recursos Humanos	7.2	X			X	X							X				4	4/13 (31%)
	Formação	7.3	X				X				X							3	3/13 (23%)
	Grau de Utilização	7.4	X			X	X							X	X		X	6	6/13 (46%)
	Interoperabilidade entre Sistemas	7.5	X		X		X									X		4	4/13 (31%)
	Registo e Acesso à Informação	7.6	X	X		X	X	X				X				X		7	7/13 (54%)
	Partilha de Informação	7.7	X	X	X	X	X											5	5/13 (38%)
	Gastos Logísticos	7.8				X	X											2	2/13 (15%)
	Custo dos Equipamentos	7.9					X						X					2	2/13 (15%)

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

5.2.8. Apresentação, análise e discussão da Questão n.º 8

A análise da Questão n.º 8 tem como objetivo compreender se, as medidas e objetivos definidos na Estratégia da Guarda 2020 e nos Planos de Atividades entre 2015 e a atualidade, estão ajustados às necessidades da estrutura de IC das Unidades Territoriais da GNR.

De acordo com a Tabela n.º 8, 31% dos entrevistados consideram estas medidas adequadas. Segundo E11, atendendo à sincronia destas medidas com a Estratégia TIC 2020 da AP, têm sido realizados esforços significativos na melhoria da interoperabilidade e rentabilização dos recursos TIC, de forma "sinérgica e alicerçada em soluções integradas".

E13 concretiza a ideia anterior afirmando que, apesar das suas limitações pontuais, têm vindo a ser disponibilizadas licenças, adquiridos recursos de parque informático e atualizados os SI. No mesmo sentido, E3 afirma que as medidas dão, genericamente, resposta às atuais necessidades. Contudo, considera que as vertentes de análise de informação criminal e digital forense carecem de um investimento acrescido nas suas ferramentas de análise e ferramentas de extração e tratamento da prova digital, respetivamente (E3, E15).

Por outro lado, 46% dos entrevistados consideram as medidas desadequadas. Segundo E4 e E10, a atual estrutura de IC carece de uma metodologia, de uma estratégia, recorrendo ao *Intelligence Led Policing* para suportar esta ideia. E4 acrescenta que, ao nível do mapeamento do crime, nos encontramos "décadas atrasados", reforçando que a IC ainda não possui "capacidade (…) de começar, efetivamente, a prever". Por sua vez, E1 refere necessidades ao nível do SIIOP-G, dado que possui limitações na disponibilização dos dados geográficos, em tempo oportuno. Por fim, E2 e E4 consideram que é necessário um levantamento, ao nível das Unidades Territoriais, quer das TI utilizadas, quer das perspetivas de evolução das mesmas, a fim de serem centralizadas necessidades e, por consequência, viabilizar as melhores soluções a implementar e uniformizar as TI em uso.

Tabela n.º 8 - Matriz de análise de conteúdo da Questão n.º 8

Questão n.º 8																			
Categoria	**Subcategorias**	**UR**	**Entrevistados**															**UEn**	**Resultado (%)**
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**		
Adequabilidade dos objetivos e medidas da Estratégia e Planos de Atividades da GNR	Parcialmente Adequados	8.1			X										X		X	3	3/13 (23%)
	Desadequados	8.2	X	X		X						X		X		X		6	6/13 (46%)
	Adequados	8.3					X	X			X		X					4	4/13 (31%)

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

5.2.9. Apresentação, análise e discussão da Questão n.º 9

A análise da Questão n.º 9 tem em vista levantar as principais melhorias a desenvolver no domínio da utilização e funcionamento dos Sistemas e TI pelos órgãos da estrutura de IC das Unidades Territoriais da GNR.

Atendendo à Tabela n.º 9, verificamos que, uma das melhorias a destacar diz respeito à "Interoperabilidade". Segundo 73% dos entrevistados, devido à pluralidade de SI existentes, a informação encontra-se dispersa, dificultando o acesso à mesma, bem como a sua partilha para efeitos de análise e de investigação. Segundo E1, E5 e E7 seria fundamental uma interligação entre os Sistemas dos Serviços Partilhados na condição de que, a informação "que fosse reservada, informar apenas que essa informação existia" (E1), carecendo de autorização. Por sua vez, E3, E4 e E10, sublinham a necessidade de uma centralização dos sistemas das diferentes polícias numa plataforma única, "onde todos teriam o dever de alimentar, mas também de aceder, (…) respeitando o princípio da necessidade de saber" (E4), visto que ao nível da PIIC, como refere E2, "aquilo que está a ser colocado (…) são as situações que já terminaram", pois "não existe mentalidade de partilha de informação" (E4). E13 acrescenta que é necessário reduzir o "número de pesquisas e do tempo "perdido" e desburocratizar as trocas de informação". Assim, tal como referem Koper, Lum e Willis (2014), as TI devem ser utilizadas no sentido de melhorar a comunicação entre as unidades, nomeadamente, quando articuladas com o fim comum de reduzir a criminalidade, dado que a IC "é, em si mesma, uma atividade de cooperação" (Pereira, 2012, p. 27).

E7, E8, E11 e E14 acrescentam a importância da centralização, no SIIOP-P, dos vários submódulos do SIIOP, a fim de sistematizar o registo, análise e tratamento da informação "garantindo que, com menos pesquisas, se obtém informação mais célere e fiável" (E14). Para este fim, está em curso o "desenvolvimento do chamado SIIOP 3.0" (E8).

De igual modo, E2, E5, E6 e E15 salientam a falta de uma base de dados de IC, de acesso muito restrito, a partir da qual seria possível não só carregar e elaborar as peças dos inquéritos (E5, E6), como também "todas as diligências, relatórios, exames, perícias e demais meios de obtenção de prova" (E6), assim como, os produtos da análise de informação criminal, cumulativamente com a informação constante nos autos de notícia (E2). Esta evolução permitiria, por um lado, a centralização de todo o expediente de IC (E5, E15) e, por outro lado, a supervisão (E6) e o desenvolvimento da comunicação entre as Unidades (E2) evitando, consequentemente, investigações paralelas por parte dos órgãos de IC (E5). Esta solução, ainda em fase de estudo, assume a designação de "SIIOP-IC" (E2, E6).

Paralelamente, 87% dos entrevistados defendem a necessidade de investimento em "Novas Ferramentas Tecnológicas", designadamente, ferramentas que permitam recolher, armazenar e correlacionar grandes quantidades de dados, de forma automatizada, favorecendo a criação de padrões criminais "que até agora possam estar despercebidos" (E7), bem como otimizar o emprego de meios e suportar a prevenção criminal (E11), como referido pelo Maj Hugo Carneiro nas entrevistas exploratórias.

Em adição, é reforçada a necessidade de investimento na quantidade de recursos humanos (33%), na sua formação (53%), pois as TI estão "sempre a evoluir" (E5), e na sua sensibilização para uma correta introdução dos dados nos sistemas (E1, E4, E5, E7).

Tabela n.º 9 - Matriz de análise de conteúdo da Questão n.º 9

Questão n.º 9																		
Categoria	**Subcategorias**	**UR**	**Entrevistados**															**UE n**	**Resultado (%)**
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**		
Melhorias a implementar nos Sistemas e TI	Interoperabilidade	**9.1**	X	X	X	X	X		X	X		X	X		X	X		11	11/15 (73%)
	Novas Ferramentas Tecnológicas	**9.2**	X		X	X	X		X	X	X	X	X	X	X	X	X	13	13/15 (87%)
	Base de Dados IC	**9.3**		X			X	X									X	4	4/15 (27%)
	Confidencialidade da Informação	**9.4**		X														1	1/15 (7%)
	Formação	**9.5**	X		X	X	X				X				X	X	X	8	8/15 (53%)
	Recursos Humanos	**9.6**	X			X	X		X								X	5	5/15 (33%)

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

5.3. Verificação das hipóteses de investigação

Na continuidade das linhas de investigação propostas por Quivy e Campenhoudt (2017), cabe, no presente Subcapítulo, proceder à verificação das hipóteses de investigação, confirmando-as, total ou parcialmente ou, caso contrário, refutando a sua formulação.

Quanto à HPP: "O recurso às TI pela estrutura de IC permite a análise e sintetização da informação, a análise do histórico criminal e identificação de padrões e tendências criminais, a extração, armazenamento e leitura das informações armazenadas em dispositivos móveis, bem como a identificação e a preservação de vestígios em suporte digital, garantindo a sua integridade e inalterabilidade.", foi totalmente confirmada. Os Sistemas e TI permitem a centralização de toda a informação em repositórios únicos, facilitando o seu armazenamento, análise, e, consequentemente, a sua difusão. São igualmente responsáveis pela identificação de necessidades processuais, no âmbito de uma investigação contribuindo, desta forma, para a segurança da informação, a desmaterialização

de atos e procedimentos, a partilha de informação entre os órgãos de IC e, de igual modo, com entidades externas, assim como a rentabilização dos meios a alocar e a adoção de medidas de prevenção e de IC.

Relativamente à H1: "As informações criminais destinam-se a cumprir as finalidades da IC, sendo utilizadas pelos NAIIC na produção de relatórios de informações contribuindo, consequentemente, para determinar a existência de um crime, identificar e responsabilizar os seus agentes, bem como descobrir e recolher prova, no âmbito da investigação.", foi totalmente confirmada. Porém, foi salientada a indissociação entre as informações criminais e as informações policiais, nomeadamente ao nível das Unidades Territoriais, produzindo efeitos, quer ao nível da prevenção, como ao nível da repressão da criminalidade.

No que concerne à H2: "As Tecnologias e SI utilizados são a PIIC, na partilha de informação com outros OPC homólogos, e o SIIOP. Adicionalmente, é utilizado o *i2 Analyst´s Notebook* na análise da informação e o *UFED Ultimate* da *Cellebrite* para a extração e análise de prova em suporte eletrónico.", foi totalmente verificada. Além destas, foram mencionadas TI como o QGIS e/ou ArcGIS no mapeamento do crime, o sistema *Paragon* na interceção e localização de comunicações e, não só, mas também, o sistema AFIS na pesquisa, identificação e preservação de vestígios lofoscópicos.

A H3: "As principais vantagens decorrentes da utilização das TI são a centralização da informação, bem como a sua supervisão e verificação, em tempo real, aumentando a respetiva qualidade e reduzindo o tempo de resposta às necessidades operacionais. Quanto às desvantagens, as TI exigem uma contínua atualização dos conhecimentos técnicos para a utilização das mesmas e têm por base custos elevados para a sua aquisição e manutenção.", foi totalmente confirmada. A utilização das TI constituem um importante suporte ao nível do planeamento e intervenção dos órgãos de IC, permitindo identificar e decidir as técnicas e táticas de investigação a adotar, assim como racionalizar os meios a empregar. Contudo, a constante evolução tecnológica produz efeitos nas dinâmicas criminais e na sua capacidade de organização e articulação, o que exige adaptação e acompanhamento pela estrutura de IC.

Por fim, a H4: "As principais melhorias a implementar, neste âmbito, são o desenvolvimento da capacidade de armazenamento e análise de grandes quantidades de informação, o que permitiria, de forma automatizada, correlacionar informação proveniente de diversas fontes, assim como investir na formação técnica dos militares.", foi totalmente confirmada. Todavia, a melhoria identificada com maior expressividade foi ao nível da interoperabilidade entre os sistemas, bem como ao nível do registo e acesso à informação, causando constrangimentos na capacidade de análise, sintetização e partilha da informação.

CONCLUSÕES E RECOMENDAÇÕES

A presente investigação procurou dar resposta à questão de investigação: "Quais os principais contributos das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da GNR?". Segundo o método seguido, esta questão foi desagregada em questões derivadas, cuja resposta se identifica em seguida.

Relativamente à PD1: "Qual a função das Informações Criminais na resposta aos fenómenos criminais?" importa destacar que, as informações criminais se inscrevem no âmbito da atividade de IC. Neste sentido, a utilização das informações criminais destina-se a cumprir as finalidades da IC, ou seja, determinar a existência de um crime, identificar e responsabilizar os seus agentes, bem como descobrir e recolher as provas, em sede de um processo crime, constituindo prova de investigação. Assim, a recolha, avaliação, tratamento, análise e difusão destas informações materializam técnicas/ferramentas essenciais para a investigação de crimes pelos OPC. A análise destas informações é prosseguida, ao nível das SIIC, pelos NAIIC, produzindo relatórios de informações que serão difundidos aos órgãos operativos, a fim de suportar o seu planeamento e intervenção operacional. Por conseguinte, as informações criminais permitem direcionar a investigação, estabelecer procedimentos e técnicas de atuação, de recolha e de investigação, identificar, estudar e acompanhar fenómenos criminais, bem como determinar os meios necessários a empregar.

Deste modo, as informações criminais apoiam o analista no seu processo de decisão e no desenvolvimento de estratégias de investigação, em coordenação com os órgãos operativos. Consequentemente, a partilha de informação criminal, constitui um instrumento de cooperação único na resposta aos fenómenos criminais. Contudo, devemos considerar que, ao nível da estrutura de IC das Unidades Territoriais da GNR, as informações criminais não se encontram dissociadas das informações policiais, uma vez que estas se complementam, produzindo efeitos, tanto no domínio da repressão, como da prevenção.

Definida a sua base estruturante, afirma-se enunciar os principais Sistemas e TI utilizados pela estrutura de IC, respondendo à PD2: "Quais as principais Tecnologias e Sistemas de Informação utilizados pelas Unidades Territoriais da GNR na vertente de Investigação Criminal?". No âmbito da análise de informação, uma das principais TI utilizadas pelos NAIIC é o *i2 Analyst´s Notebook*, no tratamento e análise da informação,

permitindo determinar associações, identificar relações, assim como centralizar e sintetizar dados, servindo de base para a produção de relatórios de informações.

Por sua vez, são utilizadas ferramentas que permitem o mapeamento e georreferenciação do crime, como o QGIS e/ou ArcGIS e, ao nível da recolha de indícios criminais, *softwares* como o *Paragon* permitem, por um lado, a recolha, armazenamento e leitura das informações comunicadas entre elementos em processo de investigação e, por outro lado, a sua localização. Adicionalmente, através do recurso a ferramentas digitais forenses como o *Cellebrite UFED Ultimate*, é possível aceder, recolher e preservar dados digitais contidos em dispositivos móveis, que constituirão elementos de prova. De igual modo, o sistema AFIS materializa uma solução tecnológica única na identificação, armazenamento e preservação das características dos vestígios lofoscópicos recolhidos, garantindo a sua inalterabilidade e integridade.

No que concerne aos SI, a PIIC é utilizada enquanto base de registo e partilha de informação entre os diversos OPC. Por fim, na qualidade de sistema transversal a todas as vertentes de IC, assim como a toda a atividade operacional da Guarda, é utilizado o SIIOP, enquanto repositório centralizado, destinado a organizar e manter atualizada toda a informação. A partir deste, é possível aceder a outros sistemas, nos quais é registada a informação resultante da prossecução da missão de outras valências operacionais.

Identificados os principais Sistemas e TI, resulta analisar a PD3: "Quais as vantagens e desvantagens decorrentes do funcionamento e utilização dos Sistemas e Tecnologias de Informação pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?". Considerando, em primeiro lugar, as suas principais vantagens, verificamos que o recurso às TI permite a recolha, armazenamento, tratamento, análise e difusão da informação, em tempo útil, garantindo a centralização num repositório único, de toda a informação dispersa em múltiplas fontes. Paralelamente, além da acessibilidade e, consequentemente, da difusão da informação, as TI são fundamentais para garantir a autenticidade, fiabilidade, confidencialidade e integridade da informação, quer armazenada e/ou preservada, quer partilhada entre os OPC, para fins da prevenção e IC, articulando uma estreita relação e comunicação entre os mesmos.

Neste sentido, as TI constituem ferramentas de apoio à IC, produzindo efeitos a múltiplos níveis. Por um lado, ao nível da informação, enquanto produto, aumentando, quer a quantidade, como a sua qualidade, precisão e segurança. Por outro lado, permitem encurtar e apoiar todo o processo de tomada de decisão, rentabilizar meios, identificar e definir metodologias e técnicas que conduzem a um maior rigor e otimização do processo de

investigação e, por fim, numa perspetiva transversal, imprimir uma eficácia e eficiência acrescidas na intervenção operacional da estrutura de IC das Unidades Territoriais da GNR.

Contudo, o funcionamento e utilização dos Sistemas e TI pelas SIIC manifestam, igualmente, debilidades. Uma vez que as atividades criminosas têm vindo a ser, cada vez mais, dinamizadas pelos avanços tecnológicos, é exigido um acompanhamento e adaptação das ferramentas tecnológicas utilizadas pela IC, sob pena de obsolescência para uma resposta oportuna, eficaz e competente. Na mesma linha de pensamento, visto que as TI se encontram em permanente evolução, sofrem constantes modernizações e alterações, o que exige uma adequação aos respetivos avanços, por intermédio de licenças e/ou versões atualizadas. Destacam-se, de igual modo, limitações ao nível do registo e acesso à informação, dado que se verificam condicionalismos na pesquisa automática de todos os dados constantes no repositório do SIIOP e, consequentemente, nos descritivos dos autos de notícia. Para além disso, assiste-se à necessidade de acesso a múltiplos sistemas para a obtenção e análise da informação, gerando redundância e inoportunidade.

Por fim, em adição aos gastos logísticos e custos dos equipamentos, importa verificar que, as TI não poderão ser consideradas isoladamente. Estas materializam um suporte a toda a atividade desenvolvida pelo elemento humano. Porém, verificam-se limitações em termos da quantidade de recursos humanos na estrutura de IC, bem com ao nível da sua formação, condicionando a rentabilização da utilização dos Sistemas e TI e, por consequência, a qualidade da informação, quer inserida, quer produzida a partir dos mesmos.

Atendendo à última PD, isto é, à PD4: "Quais as melhorias a implementar nos Sistemas e Tecnologias de Informação, por forma a reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?", concluímos que deverão ser implementadas melhorias ao nível da interoperabilidade entre os sistemas utilizados, a fim de centralizar toda a informação individualizada nos diversos repositórios, facilitando a sua sintetização, cruzamento e correlacionamento e, por conseguinte, a respetiva partilha e análise, cumprindo o princípio da necessidade de saber.

Com efeito, tendo em vista a gestão e condução da atividade de IC com maior eficácia, seria igualmente essencial, a criação de uma base de dados reservada à estrutura de IC, a partir da qual seria possível, não só carregar e elaborar as peças dos inquéritos, como todas as diligências recolhidas no âmbito das investigações, nomeadamente, relatórios, perícias, exames, meios de obtenção de prova, entre outros, cumulativamente com os autos de notícia. Neste sentido, é garantida a supervisão das investigações prosseguidas em cada

Unidade, evitando a sua replicação, fomentando a partilha de informação e, por consequência, o cruzamento da informação recolhida em cada SIIC.

Finalmente, em complemento ao reforço da quantidade de recursos humanos e da respetiva formação, seria essencial investir em novos Sistemas e TI, a fim de otimizar todo o ciclo de produção de informações, quer em quantidade, como em qualidade.

Uma vez respondidas as PD, encontram-se reunidas as condições para concretizar a PP: "Quais os principais contributos das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da GNR?". Após a análise dos resultados obtidos, quer a partir das entrevistas exploratórias e do enquadramento teórico, quer por intermédio das entrevistas confirmatórias realizadas, concluímos que são inúmeros os benefícios operacionais resultantes da utilização dos Sistemas e TI pela estrutura de IC, ao nível das SIIC.

Adotando como ponto de partida as potencialidades produzidas ao nível da análise de informação, o recurso às TI possibilita o alcance de elevados níveis de desempenho na centralização e sintetização da informação, dando corpo à projeção de diretrizes e hipóteses de investigação alicerçadas em diagramas, cronogramas, fluxogramas, conexões e matrizes. Por conseguinte, torna-se possível georreferenciar os fenómenos criminais, analisar o seu histórico, interligar relações, identificar tendências criminais, bem como a sua incidência e padrões evolutivos. Por outras palavras, permitem definir novas linhas de investigação, decidir e rentabilizar os meios técnicos, táticos e metodologias a adotar e, por consequência, apoiar o planeamento e intervenção, quer no âmbito da missão geral policial, direcionando o patrulhamento, quer no domínio das investigações prosseguidas pelos órgãos operativos/investigadores.

Por sua vez, o vínculo existente entre a IC e as TI, produz efeitos ao nível da pesquisa e/ou recolha de informação. Através da utilização de *softwares* de recolha e armazenamento de comunicações é possível, por um lado, a reconstituição dos factos e, por outro lado, o acompanhamento e registo, em tempo útil, da atividade criminosa. Por seu turno, a pesquisa e recolha de informações é prosseguida, igualmente, através do recurso a ferramentas OSINT, isto é, ferramentas de pesquisa em redes sociais e outras fontes abertas, possibilitando identificar a localização dos suspeitos e conhecer as suas rotinas e ligações pessoais. Paralelamente, no domínio da recolha de informação, é possível aceder ao conteúdo presente em dispositivos móveis, extraindo e descodificando todos os dados, quer eliminados, quer outros de difícil acesso, permitindo a sua recolha, armazenamento e

preservação, a fim de constituírem prova, fundamentais, por exemplo, nos casos de violência doméstica.

Neste sentido, a preservação da prova, isto é, a garantia do valor probatório dos factos recolhidos, materializa uma das principais potencialidades do recurso às TI. Para este fim, concorrem igualmente, as soluções tecnológicas utilizadas pela criminalística, uma vez que, para além da identificação garantem, de forma absoluta e inequívoca, a integridade e inalterabilidade dos vestígios recolhidos preservando, consequentemente, a Cadeia de Custódia da Prova.

Nesta senda, através da centralização e armazenamento da informação e, portanto, das diligências recolhidas no âmbito da IC, os Sistemas e TI, além da respetiva preservação, permitem a identificação de lacunas processuais. Deste modo, são racionalizados meios (humanos e materiais), desmaterializados atos e procedimentos, agilizadas comunicações, encurtados ciclos de decisão, suprimidas redundâncias e disponibilizadas informações, mediante a sua partilha, numa lógica de cooperação e coordenação.

Pelo que antecede, verificamos que, cada vez mais, é imprescindível o recurso aos Sistemas e TI, uma vez que a evolução da realidade criminal atual é caracterizada pela sua capacidade de reorganização e de rearticulação, dinamizadas pelos avanços tecnológicos, o que exige recursos humanos, formação, especialização e, por consequência, investimento em meios e equipamentos tecnológicos. Assim, podemos concluir que, as TI se converteram num pilar fundamental do desenvolvimento da IC, contribuindo decisivamente para a sua maximização operacional, gerando uma eficácia acrescida nos seus mecanismos de prevenção e de IC.

Como principais limitações na realização do RCFTIA identificam-se os constrangimentos decorrentes da propagação do vírus SARS-CoV-2, condicionando, quer o acesso a espaços de consulta da bibliografia necessária para a construção da problemática da investigação, quer a disponibilidade dos entrevistados para a realização das entrevistas.

Por fim, considera-se pertinente, em investigações futuras, analisar a utilização das TI, em cada fase do processo de Tomada de Decisão, atendendo à missão/função dos diferentes órgãos da estrutura de IC das Unidades Territoriais da GNR. Deste modo, seria possível descrever, faseadamente, o papel das TI no suporte ao Processo de Tomada de Decisão dos órgãos da estrutura de IC. Concomitantemente, seria fundamental, a realização de um estudo comparativo entre a realidade tecnológica da estrutura de IC da GNR e da *Guardia Civil*, permitindo contruir um quadro evolutivo de referência neste âmbito.

REFERÊNCIAS BIBLIOGRÁFICAS

Artigos científicos, obras literárias, relatórios e outros documentos

Agência da União Europeia para a Cooperação Policial [EUROPOL] (2002). Analytical guidelines. In Publications Office of the European Union. In *Publications Office of the European Union*. Acedido a 01 de maio de 2020 em *https://op.europa.eu/en/publication-detail/-/publication/c5abefbc-f9ed-472a-875e-2fe378ba4ba8*

Agência para a Modernização Administrativa [AMA] (2017). *SAMA - Sistema de Apoios à Modernização e Capacitação da Administração Pública.* Lisboa: AMA.

Agência para a Modernização Administrativa [AMA] (2018). In *As Tecnologias de Informação e Comunicação na Administração Pública.* Acedido a 22 de março de 2020 em *https://tic.gov.pt/documents/37177/108997/CTIC_TIC2020_Estrategia_TIC.pdf/e2ea3d32-82a8-ed18-0fbf-9d51dfc24acc*

Alves, C. A. (2012). *Adivinhar Perigos*. Lisboa: Guarda Nacional Republicana.

Amaral, L. A. & Varajão, J. E. (2000). *Planeamento de Sistemas de Informação*. Lisboa: FCA - Editora de Informática.

Association of Chief Police Officers [ACPO] (2010). *Guidance on the Management of Police Information.* Bedfordshire: ACPO.

Baptista, J., Varajão, J., & Moreira, F. (2013). Função Sistemas de Informação nas organizações – realidade, desafios e oportunidades do uso de arquiteturas empresarias. In *RepositoriUM*. Acedido a 30 de março de 2020 em *https://repositorium.sdum.uminho.pt/bitstream/1822/26252/1/ntmi2013-1.pdf*

Bispo, A. (2004). A função de informar. In Moreira, A. (Coord.), *Informações e Segurança: Estudos em Honra do General Pedro Cardoso* (pp. 77-104). Lisboa: Prefácio.

Boschele, M. (2014). The "information society" and the role of knowledge in society. *Academic Journal of Information Technology*, 5(14), 7-14. doi: 10.5824/1309-1581.2014.1.001.x.

Bose, P. K. & Kabir, M. J. (2017). Fingerprint: A Unique and Reliable Method for Identification. *Journal of Enam Medical College*, 7(1), 29-34. doi: 10.3329/jemc.v7i1.30748.

Braz, J. (2016). *Ciência, Tecnologia e Investigação Criminal: Interdependências e Limites num Estado de Direito Democrático*. Coimbra: Almedina.

Braz, J. (2020). *Investigação Criminal: A Organização, O Método e A Prova: Os Desafios da Nova Criminalidade* (5ª edição). Coimbra: Almedina.

Canotilho, G. J. J. & Moreira, V. (2010). *Constituição da República Portuguesa Anotada – Volume II* (4ª Edição). Coimbra: Coimbra Editora.

Cardoso, P. (2004). *As Informações em Portugal* (1ª Edição). Lisboa: Gradiva.

Carvalho, J. Á. (2010). Tecnologias e Sistemas de Informação: uma área científica orientada às necessidades de conhecimento dos profissionais envolvidos na contínua transformação das organizações através das tecnologias da informação. *Revista Eletrónica de Biblioteconomia e Ciência Da Informação*, 1–25. doi: 10.5007/1518-2924.2010v15nesp2p1.

Carvalho, J. E. (2009). *Metodologia do Trabalho Científico* (2ª Edição). Lisboa: Escolar Editora.

Castells, M. (2004). *The network society: a cross-cultural perspective.* Massachusetts: Edward Elgar Publishing.

Castro, C. S. (2018). Novas Tecnologias e Relação Laboral – Alguns Problemas: Tratamentos de dados pessoais, novo regulamento geral de proteção de dados e direito à desconexão. In Centro de Estudos Judiciários (Ed.), *Revista do Centro de Estudos Judiciários* (pp. 271-299). Coimbra: Almedina.

Clausewitz, K. V. (1982). *Da Guerra; Trad. Inês Busse.* Mem Martins: Europa-América.

Clemente, P. J. L. (2006). *A Polícia em Portugal*. Oeiras: INA - Instituto Nacional de Administração.

Clemente, P. J. L. (2007). As Informações Policiais – Palimpsesto. In Silva, G. M. & Valente, M. M. (Coord.), *Estudos de Homenagem ao Juiz Conselheiro António da Costa Neves Ribeiro – In Memoriam* (pp. 381-405). Coimbra: Almedina.

Clemente, P. J. L. (2010). Polícia e Segurança – Breves Notas. *Lusíada. Política Internacional e Segurança.* 1(4), 139-169.

Conselho da União Europeia (2016). *Manual de Intercâmbio de Informações entre as Autoridades Policiais.* Bruxelas: Conselho da União Europeia.

Cortes, B. (2005). *Sistemas de Suporte à Decisão.* Lisboa: FCA – Editora de Informática, Lda.

Costa, S. & Machado, H. (2012). *A Ciência na Luta contra o Crime – Potencialidades e Limites* (1ª Edição). Braga: Edições Húmus.

Coutinho, C.P. (2018). *Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática* (2ª Edição). Coimbra: Almedina.

Custers, B. (2008). Tapping and Data Retention in Ultrafast Communication Networks. *Journal of International Commercial Law and Technology*. 3(2), 94-100.

de Lint, W., O'Connor, D. & Cotter, R. (2007). Controlling the flow: Security, exclusivity, and criminal intelligence in Ontario. *International of the Sociology of Law*. 35(1), 41-58. doi: 10.1016/j.ijsl.2007.01.001.

Dias, M. G. (2006). Segurança Interna. In Valente. M. M. G. (Coord.), *II Colóquio de Segurança Interna* (pp. 155–169). Coimbra: Almedina.

Esteves, P. (2004). A função de informar. In Moreira, A. (Coord.), *Informações e Segurança: Estudos em Honra do General Pedro Cardoso* (pp. 439-458). Lisboa: Prefácio.

Fernandes, L. F. & Valente, M. M. G. (2005). *Segurança Interna – Reflexões e Legislação.* Coimbra: Almedina.

Ferreira, A. M. (2007). O Sistema de Informações da República Portuguesa. In Gouveia, J. B. & Pereira, R. (Coord.), *Estudos de Direito e Segurança* (pp. 67-93). Coimbra: Almedina.

Ferreira, S. C. (2017). *Sistemas de Informação em Segurança*. Brasil: Editora e Distribuidora Educacional S.A.

Flick, U. (2005). *Métodos Qualitativos na Investigação Científica.* Lisboa: Monitor – Projectos e Edições, Lda.

Földes, Adam. (2016). *Classified Information: A review of currents legislation across 15 countries & the EU.* London: Transparency International (Defence and Security Programme).

Fortin, M., Côté, J., & Filion, F. (2009). *Fundamentos e Etapas no Processo de Investigação Científica.* Loures: Lusodidacta.

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

Girelli, C. M. A. (2014). Deteção de impressões digitais revertidas em documentos falsos. *Revista Brasileira de Ciências Policiais*. 5(2), 11-29.

Gorbanov, I., Ismailov, K. & Zaiets, A. (2019). Use of Analytical Methods for Protection of Economic Rights, Freedoms and Interests of Persons under Investigation of Criminal Legal Offenses. In Institute of European Integration [IEI] (Ed.), *Social and Legal Aspects of the Development of Civil Society Institutions. Part II* (pp. 126-140). Poland: GESIS.

Gouveia, L. & Ranito, J. (2004). *Sistemas de Informação de Apoio à Gestão.* Porto: Principia, Publicações Universitárias e Científicas.

Guarda Nacional Republicana [GNR] (2014d). *APOTRGNR 22 Regulamento de Utilização das Tecnologias de Informação da GNR*. Lisboa: Direção de Comunicações e Sistemas de Informação.

Guarda Nacional Republicana [GNR] (2014e). Estratégia da Guarda 2020: Uma Estratégia de Futuro. In *Sítio da Guarda Nacional Republicana.* Acedido a 6 de fevereiro de 2020 em *https://www.gnr.pt/estrategia.aspx*

Guarda Nacional Republicana [GNR] (2014f). Plano de Atividades 2015. In *Sítio da Guarda Nacional Republicana.* Acedido a 7 de fevereiro de 2020 em *https://www.gnr.pt/InstrumentosGestao/2015/PAGNR2015.pdf*

Guarda Nacional Republicana [GNR] (2015). Plano de Atividades 2016. In *Sítio da Guarda Nacional Republicana.* Acedido a 7 de fevereiro de 2020 em *https://www.gnr.pt/InstrumentosGestao/2016/PAGNR2016.pdf*

Guarda Nacional Republicana [GNR] (2016a). *Manual de Informações.* Lisboa: Escola da Guarda.

Guarda Nacional Republicana [GNR] (2016c). Plano de Atividades 2017. In *Sítio da Guarda Nacional Republicana.* Acedido a 8 de fevereiro de 2020 em *https://www.gnr.pt/InstrumentosGestao/2017/PA2017.pdf*

Guarda Nacional Republicana [GNR] (2016d). Relatório de Atividades 2015. In *Sítio da Guarda Nacional Republicana.* Acedido a 26 de março de 2020 em *https://www.gnr.pt/InstrumentosGestao/2015/RelatorioActividadesGNR2015.pdf*

Guarda Nacional Republicana [GNR] (2017a). Plano de Atividades 2018. In *Sítio da Guarda Nacional Republicana.* Acedido a 20 de março de 2020 em *https://www.gnr.pt/InstrumentosGestao/2018/PA_GNR_2018.pdf*

Guarda Nacional Republicana [GNR] (2017b). Relatório de Atividades 2016. In *Sítio da Guarda Nacional Republicana.* Acedido a 26 de março de 2020 em *https://www.gnr.pt/InstrumentosGestao/2016/RA2016_APROVADOCMDT.pdf*

Guarda Nacional Republicana [GNR] (2018d). Plano de Atividades 2019. In *Sítio da Guarda Nacional Republicana.* Acedido a 24 de março de 2020 em *https://www.gnr.pt/InstrumentosGestao/2019/PA_GNR_2019.pdf*

Guarda Nacional Republicana [GNR] (2018e). Relatório de Atividades 2017. In *Sítio da Guarda Nacional Republicana.* Acedido a 27 de março de 2020 em *https://www.gnr.pt/InstrumentosGestao/2017/RA2017.pdf*

Guarda Nacional Republicana [GNR] (2019a). *PDGNR 1-04-04: Manual de Investigação de Crimes em Ambiente Digital.* Lisboa: Comando da Doutrina e Formação.

Guarda Nacional Republicana [GNR] (2019b). Relatório de Atividades 2018. In *Sítio da Guarda Nacional Republicana.* Acedido a 27 de março de 2020 em *https://www.gnr.pt/InstrumentosGestao/2018/RA_GNR_2018.pdf*

Guarda Nacional Republicana [GNR] (2019c). Organograma da Guarda Nacional Republicana. In *Sítio da Guarda Nacional Republicana*. Acedido a 17 de março de 2020 em *https://www.gnr.pt/imagens/Organigrama_GNR.pdf*

Guerra, I. C. (2006). *Pesquisa Qualitativa e Análise de Conteúdo – Sentidos e formas de uso* (1ª Edição). Cascais: Princípia Editora.

Hess, K. M., Orthmann, H. C. & Cho, H. L. (2017). *Criminal Investigation* (11th Edition). USA: Cengage Learning.

Hevner A. & Chatterjee S. (2010). *Design Science Research in Information Systems*. USA: Springer.

International Association of Law Enforcement Intelligence Analysts [IALEIA] (2012). *Law Enforcement Analytic Standards* (2nd Edition). USA: IALEIA.

International Business Machines Corporation [IBM] (2017). *IBM i2 iBase: Collaborative database application designed to support intelligence-led operations.* USA: IBM.

Johnson, C. E. (2018). *Organizational Ethics* (4th Edition). Washington: SAGE Publications.

Keay, S. & Kirby, S. (2018). The Evolution of the Police Analyst and the Influence of Evidence-Based Policing. *Policing: A Journal of Policy and Practice*. 12(3), 265–276. doi: 10.1093/police/pax065.

Khan, A. & Mansuri, Z. H. (2018). Comparative study of various Digital Forensics Logical Acquisition Tools for Android Smartphone's internal memory: a case study of Samsung Galaxy S5 and S6. *International Journal of Advanced Research in Computer Science*, 9(1), 357-369. doi: 10.264483/ijarcs.v9i11.5303.

Koper, C.S., Lum, C. & Willis, J.J. (2014). Optimizing the use of technology in policing: Results and implications from a multi-site study of the social, organizational, and behavioral aspects of implementing police technologies. *Journal of Policy and Practice*, 8(2), 212-221. doi: 10.1093/police/pau015.

Kumar, G. & Game, P.S. (2016). Smart Security by Predicting Future Crime with GIS and LBS Technology on Mobile Device. *International Journal of Science and Research*. 5(2), 295-299.

Kusac, M. (2016). *Mutual admissibility of evidence in criminal matters in the EU. A study of telephone tapping and house search.* Belgium: Maklu.

Laudon, K. C. & Laudon, J. P. (2018). *Management Information Systems – Managing the Digital Firm* (15th Edition). New Jersey: Prentice Hall.

Liew, A. (2013). DIKW: Data, Information, Knowledge, Intelligence, Wisdom and their Interrelationships. *Business Management Dynamics*. 2(10), 49-62.

Lopes, J. M. (2017*). Manual de gestão para a investigação criminal no âmbito da criminalidade organizada, corrupção, branqueamento de capitais e tráfico de estupefacientes.* Lisboa: Camões - Instituto da Cooperação e da Língua.

Machado, H. & Costa, S. (2013). Biolegality, the Forensic Imaginary and Criminal Investigation. *RCCS Annual Review,* 5(5), 84-105. doi: 10.4000/rccsar.490.

Machado, H. & Granja, R. (2020). *Forensic Genetics in the Governance of Crime*. Singapore: Springer Nature.

Machado, T. A. & Vilalta, L. A. (2018). Novos Paradigmas da Investigação Criminal. *Revista Brasileira de Ciências Policiais.* 9(1), 13-41.

Mannheim, H. (1984). *Criminologia Comparada*. Lisboa: Fundação Calouste Gulbenkian.

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

Marolla, C. (2018). *Information and Communication Technology for Sustainable Development*. USA: CRC Press.

McDowel, D. (2009). *Strategic Intelligence – A Handbook for Practitioners, Managers, and Users.* UK: The Scarecrow Press.

Ministério da Administração Interna [MAI] (2015). Missão. In *Computer Security Incident Response Team (CSIRT).* Acedido a 17 de abril de 2020 em *https://www.csirt.rnsi.mai.gov.pt/*

Ministério da Administração Interna [MAI] (2018). Rede Nacional de Segurança Interna (RNSI). In *Secretaria Geral do Ministério da Administração Interna*. Acedido a 17 de abril de 2020 em *https://www.sg.mai.gov.pt/Tecnologias/RNSI/Paginas/default.aspx*

Moleirinho, P. (2009). *Da Polícia de Proximidade ao Policiamento Orientado pelas Informações*. Tese de Mestrado em Direito e Segurança. Faculdade de Direito da Universidade Nova de Lisboa, Lisboa.

Moses, K., Higgins, P., McCabe, M., Prabhakar, S. & Swann, S. (2010). *Automated Fingerprint Identification System (AFIS).* Rockville: National Institute of Justice.

Neto, J. F. C. & Leite, J. C. (2015). *Decisões de Investimentos em Tecnologias da Informação*. Brasil: Elsevier Editora.

Nunes, J. (2015a). A Interoperabilidade dos Sistemas de Informação como fator de sucesso. *Pela Lei e Pela Grei - Sistemas de Informação*. 27(108), 24-28.

Nunes, L. (2015b). Estratégia para as Tecnologias e Sistemas de Informação da Guarda. *Pela Lei e Pela Grei - Sistemas de Informação*. 27(108), 17-23.

Oliveira, F. C. (2004). *A Defesa e a Investigação do Crime, Guia Prático para Análise da Investigação Judiciária e para a Investigação pelos Recursos Próprios da Defesa Criminal* (1ª Edição). Coimbra: Almedina.

Oliveira, M. M. (2011). *Como Fazer Projetos, Relatórios, Monografias, Dissertações, Teses*. Rio de Janeiro: Elsevier Editora Ltda.

Organization for Security and Cooperation in Europe [OSCE] (2017). *Guidebook on Intelligence-Led Policing*. Vienna: TNTD/SPMU Publication Series.

Paiva, V. (2019). Apologia da estratégia na investigação criminal (branqueamento e criminalidade económico-financeira). In Sindicato dos Magistrados do Ministério Público (SMMP) (Ed.), *Revista do Ministério Público 158* (pp. 185-236). Lisboa: Sindicato dos Magistrados do Ministério Público.

Paulsen, D. J. & Robinson, M. B. (2009). *Crime Mapping and Spatial Aspects of Crime* (2nd Edition). New Jersey: Pearson Education.

Pereira, A. C. M. (2012). *A Cooperação na Investigação Criminal: Contributos para uma Maximização Operacional* (1ª Edição). Lisboa: EDIUAL.

Pereira, R. (2005). Informações e Investigação Criminal. In Valente. M. M. G. (Coord.), *I Colóquio de Segurança Interna* (pp. 155–169). Coimbra: Almedina.

Pinheiro, M. F. (2011). Identificação genética no âmbito de crimes sexuais. In Associação Sindical dos Funcionários de Investigação Criminal da Polícia Judiciária (Ed.), *Investigação Criminal*. pp. 57-85. Lisboa: ASFIC/PJ.

Pinochet, L. H. (2014). *Tecnologias de Informação e Comunicação*. São Paulo: Elsevier Editora.

Pramanik, M. I., Zhang, W., Lau, R. Y. K., & Li, C. (2016). A Framework for Criminal Network Analysis Using Big Data. *Proceedings.* 17-23. doi: 10.1109/ICEBE.2016.015.

Prodanov, C. C. (2013). *Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Académico* (2ª Edição). Novo Hamburgo: Editora Feevale.

Quivy, R. & Campenhoudt, L. V. (2017). *Manual de Investigação em Ciências Sociais* (7ª Edição). Lisboa: Gradiva Publicações.

Rainer, R. K., Prince, B. & Watson, H. J. (2015). *Management Information Systems* (3rd Edition). USA: John Wiley & Sons.

Ramos, A. (2014). *A Prova Digital em Processo Penal: O Correio Eletrónico.* Lisboa: Chiado.

Ramos, S., López, J. Á. P. & Abreu, R. (2017). Sistemas e tecnologias de informação e comunicação nas forças policiais. In *12th Iberian Conference on Information Systems and Technologies* (pp. 1-5). Lisboa: CISTI. Acedido a 14 de março de 2020 em *https://ieeexplore.ieee.org/abstract/document/7975921?fbclid=IwAR1qScgCgKSLoqtwDjqFYhmyTmTGZfOVfTNgizOIaRDD7aldh65eaiDs2Cw*

Rascão, J. P. (2008). *Novos Desafios da Gestão da Informação* (1ª Edição). Lisboa: Edições Sílabo.

Rascão, J. P. (2012). *Novas Realidades na Gestão e na Gestão da Informação* (1ª Edição). Lisboa: Edições Sílabo.

Ratcliffe, J. H. (2004). *Strategic Thinking in Criminal Intelligence*. Sydney: Federation Press.

Ratcliffe, J. H. (2008). *Intelligence-led Policing*. USA: Willan Publishing.

Rodrigues, B. S. (2008). *Das Escutas Telefónicas – Tomo I. A Monitorização dos Fluxos Informacionais e Comunicacionais* (2ª Edição). Coimbra: Coimbra Editora.

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

Sacramento, A. J. A. (2006). Uma reflexão sobre a segurança nas comunicações. In *Revista Militar*. Acedido a 24 de março de 2020 em *https://www.revistamilitar.pt/artigo/60*

Santos, A. (2015). Investigação Criminal, Processo Penal e Comunicação Social. *Revista de Direito e Segurança*, 3(6), 33-83.

Santos, L.A.B. & Lima, J.M.M. (2019). O*rientações metodológicas para a elaboração de trabalhos de investigação* (2.ª Edição). Lisboa: Instituto Universitário Militar (IUM).

Santos. R. B. (2013). *Crime Analysis with Crime Mapping* (3th Edition). USA: SAGE.

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

Sequeira, B. & Serrano, A. (2002). Influências e efeitos dos SI/TI no desempenho profissional. In *Centro de Investigação de Desenvolvimento e Economia Regional*. Acedido a 30 de março de 2020 em

https://sapientia.ualg.pt/bitstream/10400.1/4443/1/Influ%C3%AAncias%20e%20Efeitos%20dos%20SI%20no%20Desempenho%20Profissional%20.pdf

Sillitto, H., Martin, J., McKinney, D., Griego, R., Dori, D., Krob, D., Godfrey, P., Arnold, E. & Jackson, S. (2019). *Systems Engineering and System Definitions*. USA: INCOSE.

Sintra, A. (2010). Técnicas especiais de investigação criminal: Fator de segurança. *Lusíada. Política Internacional e Segurança*, 1(4), 173-192. doi: 10.34628/s958-7f89.

Sistema de Segurança Interna [SSI] (2010). *Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança.* Lisboa: Sistema de Segurança Interna.

Sistema de Segurança Interna [SSI] (2016). *Relatório Anual de Segurança Interna 2015.* Lisboa: Gabinete do Secretário-Geral do Sistema de Segurança Interna.

Sistema de Segurança Interna [SSI] (2019). *Relatório Anual de Segurança Interna 2018.* Lisboa: Gabinete do Secretário-Geral do Sistema de Segurança Interna.

Sivaranjani, S. & Sivakumari, S. (2015). GIS Based Crime Hotspot Mapping and Analysis Using Radial Basis Function (RBF) and Interpolation Method. *International Journal of Remote Sensing & Geoscience*. 4(5), 43-49.

Soares, P.A.F (2014). *Meios de Obtenção de Prova no âmbito das Medidas Cautelares e de Polícia.* Coimbra: Almedina.

Sousa, P. J. L. (2011). A Partilha de Informação entre as Forças e Serviços de Segurança e os Serviços Prisionais: Uma mais-valia! In Chambel, E. M., Valente, M. G. & Santo, P. E. (Coord.), *Ciências Policiais – Estado, Segurança e Sociedade* (pp. 167-190). Coimbra: Almedina.

Sousa, P. M. L. (2007). A Análise de Informações como um Contributo para que o Ministério Público ultrapasse uma certa passividade durante a Fase Preparatório do Processo. In Silva, G. M. & Valente, M. M. (Coord.), *Estudos de Homenagem ao Juiz Conselheiro António da Costa Neves Ribeiro – In Memoriam* (pp. 197-228). Coimbra: Almedina.

Souza, J. L. C. (2016). Crime, Polícia e Tecnologias da Informação. *Police work and new Technologies*, 22(1), 301-324. doi: 10.5433/2176-6665.2017.1v22n1p301.

Stair, R. M. & Reynolds, G. W. (2016). *Princípios de Sistemas de Informação* (3ª Edição). Brasil: Cengage Learning Edições.

Strom, K. (2017). *Research on the Impact of Technology on Policing Strategy in the 21st Century, Final Report.* Washington: National Criminal Justice Reference Service.

Thompson, W. C. & Scurich, N. (2018). When does absence of evidence constitute evidence of absence? *Forensic Science International*. 291(1), 18-19. doi: 10.1016/j.forsciint.2018.08.040.

Tomita, Y., Shirasaka, S., Watanabe, K. & Maeno, T. (2017). Applying Design Thinking in Systems Engineering Process as an Extended Version of DIKW Model. In *27th Annual INCOSE International Symposium (IS 2017)*. Australia: INCOSE. Acedido a 3 de abril de 2020 em *https://onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2017.00398.x?fbclid=IwAR0NC7OccZgNkZd3_4KeF7PMvDzBEI98yW71RqmvXSyLZpqPH0sHCfYBT0M*

Torres, J. E. (2005). A Investigação Criminal na PSP – O Modelo Atual e Perspetivas de Evolução ao Encontro do Conceito de Polícia Técnica de Proximidade. In Pereira, M. J. & Neves, J. (Coord.), *Estratégia e Gestão Policial em Portugal* (pp. 575-636). Oeiras: INA – Instituto Nacional de Administração.

U. S. Department of Justice (2004). *The fingerprint – Sourcebook*. Washington: National Institute of Justice.

United Nations Office on Drugs and Crime [UNODC] (2010). *Handbook on the Crime Prevention Guidelines: Making them work*. New York: United Nations.

United Nations Office on Drugs and Crime [UNODC] (2011). *Criminal Intelligence – Manual for Analysts*. New York: United Nations.

Valacich, J. S. & Schneider, C. (2018). *Information Systems Today: Managing the Digital World.* (8th Edition). London: Pearson.

Valente, M. M. G. (2017). Investigação Preliminar, Meios Ocultos e Novas Tecnologias. *Revista Brasileira de Direito Processual Penal*, 3(2), 473-482. doi: 10.22197/rbdpp.v3i2.82.

Valente, M. M. G. (2019). *Teoria Geral do Direito Policial* (6ª Edição). Coimbra: Almedina.

Vilelas, J. (2017). *Investigação – O Processo de Construção do Conhecimento* (2ª Edição). Lisboa: Edições Sílabo.

Wasson, C. S. (2015). *System Engineering: Analysis, Design, and Development* (2nd Edition). New Jersey: Wiley.

Zikmund, W. G. (2009). *Business Research Methods* (8th Edition). Orlando: Dryden Press Harcourt College Publishers.

Legislação, Jurisprudência e outros documentos

Academia Militar [AM] (2016). *Normas de Execução Permanente (NEP) n.º 522/1ª/20JAN16/AM: Normas para a redação de trabalhos de investigação.* Lisboa: AM.

American Psychological Association [APA] (2019). *Publication Manual of the American Psychological Association* (7th Edition). Washington: APA.

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

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

Assembleia da República [AR] (2008b). Lei n.º 53/2008, de 29 de agosto: Lei de Segurança Interna. *Diário da República*, 1ª Série, n.º 167, 6135 – 6141.

Assembleia da República [AR] (2009a). Lei n.º 73/2009, de 12 de agosto: Condições e Procedimentos para instituir o Sistema Integrado de Informação Criminal. *Diário da República*, 1ª Série, n.º 155, 5217 – 5220.

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

Assembleia da República [AR] (2015). Lei n.º 38/2015, de 11 de maio: Primeira alteração à Lei n.º 73/2009, de 12 de agosto, que estabelece as Condições e os Procedimentos a aplicar para assegurar a Interoperabilidade entre Sistemas de Informação dos Órgãos de Polícia Criminal, e segunda alteração à Lei n.º 49/2008, de 27 de agosto, que aprova a Lei de Organização da Investigação Criminal. *Diário da República*, 1ª Série, n.º 90, 2335 – 2336.

Assembleia da República [AR] (2017a). Lei n.º 96/2017, de 23 de agosto: Lei de Política Criminal - Biénio de 2017-2019. *Diário da República*, 1ª Série, n.º 162, 4924 – 4928.

Assembleia da República [AR] (2017b). Lei n.º 10/2017, de 3 de março: Lei de programação de infraestruturas e equipamentos das forças e serviços de segurança do Ministério da Administração Interna. *Diário da República*, 1ª Série, n.º 45, 1150 – 1152.

Assembleia da República [AR] (2017c). Lei n.º 67/2017, de 9 de agosto: Identificação Judiciária Lofoscópica e Fotográfica. *Diário da República*, 1ª Série, n.º 153, 4566 – 4570.

Conselho da União Europeia (2009). Decisão 2009/902/JAI do Conselho, de 30 de novembro de 2009, que cria uma Rede Europeia de Prevenção da Criminalidade e revoga a Decisão 2001/427/JAI. In *Publications Office of the European Union*. Acedido a 23 de março de 2020 em *https://op.europa.eu/en/publication-detail/-/publication/8af14487-3553-4a0c-afac-a05d714f3a5c/language-pt*

Conselho da União Europeia (2017). Guia Prático para as Equipas de Investigação Conjuntas. In *European Union Agency for Criminal Justice Cooperation.* Acedido a 26 de março de 2020 em *http://www.eurojust.europa.eu/doclibrary/JITs/JITs%20framework/JITs%20Practical%20Guide/JIT-GUIDE-2017-PT.pdf*

Guarda Nacional Republicana [GNR] (2011). *NEP/GNR – 2.20, de 12 de dezembro: Implementação do Sistema Integrado de Informações Operacionais de Polícia – SIIOP*. Lisboa: Direção de Informações.

Guarda Nacional Republicana [GNR] (2014a). *Despacho n.º 18/14 – OG, de 11 de março.* Lisboa: Comando-Geral.

Guarda Nacional Republicana [GNR] (2014b). *Diretiva Operacional n.º 01/14 - Orientações para a Implementação da Estrutura de Investigação Criminal.* Lisboa: Comando Operacional.

Guarda Nacional Republicana [GNR] (2014c). *Informação n.º 05/CO/14, de 20 de março: Estudo de Alteração Estrutural de Investigação Criminal da GNR – Elaboração dos QOR*. Lisboa: Comando Operacional.

Guarda Nacional Republicana [GNR] (2016b). *NEP/GNR – 8.80, de 16 de maio: Sistema Integrado de Informações Operacionais de Polícia – SIIOP*. Lisboa: Comando Operacional.

Guarda Nacional Republicana [GNR] (2018a). *Despacho n.º 488/18 – OG, de 30 de novembro.* Lisboa: Comando Operacional.

Guarda Nacional Republicana [GNR] (2018b). *Informação n.º I319408-201806-DIC, de 14 de setembro: Plano para Ação de Formação Forense Digital ao abrigo do Fundo de Segurança Interna (FSI) – Critérios de Nomeação de Militares – Ano 2019.* Lisboa: Direção de Investigação Criminal.

Guarda Nacional Republicana [GNR] (2018c). *Informação n.º I060627-201802-DI, de 22 de fevereiro: Projeto Centro de Informações da Guarda Nacional Republicana.* Lisboa: Direção de Informações.

Guarda Nacional Republicana [GNR] (2020a). *Ficha de Procedimentos n.º 1/2020, de 20 de janeiro: Segurança da Informação.* Lisboa: Direção de Informações.

Guarda Nacional Republicana [GNR] (2020b). *Informação n.º I060366-202002, de 5 de fevereiro: Distribuição de Material destinado à Atividade Digital Forense.* Lisboa: Direção de Investigação Criminal.

Ministério da Administração Interna [MAI] (1995a). Decreto Regulamentar n.º 2/95, de 25 de janeiro: Manutenção de uma base de dados pessoais pela Guarda Nacional Republicana (GNR). *Diário da República*, 1ª Série, n.º 21, 456 – 458.

Ministério da Administração Interna [MAI] (1995b). Decreto-Lei n.º 81/95, de 22 de abril: Brigadas Anticrime e Unidades Mistas de Coordenação. *Diário da República*, 1ª Série, n.º 95, 2314 – 2316.

Ministério da Administração Interna [MAI] (2008a). Portaria n.º 1450/2008, de 16 de dezembro. *Diário da República*, 1ª Série, n.º 242, 8845 – 8854.

Ministério da Administração Interna [MAI] (2008b). Decreto Regulamentar n.º 19/2008, de 27 de novembro: Define o número, as competências, a estrutura interna e o posto correspondente à chefia dos serviços de apoio diretamente dependentes do comandante-geral e dos serviços dos órgãos superiores de comando e direção da Guarda Nacional Republicana. *Diário da República*, 1ª Série, n.º 231, 8540 – 8546.

Ministério da Administração Interna [MAI] (2008c). Despacho n.º 32021/2008, de 16 de dezembro: Definir as unidades orgânicas flexíveis do Comando da GNR, bem como as correspondentes atribuições e competências. *Diário da República*, 2ª Série, n.º 242, 50241 – 50248.

Ministério da Administração Interna [MAI] (2010). Regulamento Geral do Serviço da Guarda Nacional Republicana. *Diário da República*, 2ª Série, n.º 119, 33856 – 33891.

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

Ministério da Justiça [MJ] (1995). Decreto-Lei n.º 48/95, de 15 de março: Código Penal. *Diário da República*, 1ª Série, n.º 63, 1350 – 1416.

Presidência da República [PR] (1976). Decreto de aprovação da Constituição: Constituição da República Portuguesa. *Diário da República*, 1ª Série, n.º 86, 738 – 775.

Presidência do Conselho de Ministros [PCM] (1996). Decreto-Lei n.º 183/96, de 27 de setembro: Define os Princípios a que deve obedecer a elaboração do Plano e Relatório Anual de Atividades dos Serviços e Organismos da Administração Pública. *Diário da República*, 1ª Série, n.º 225, 3398 – 3399.

Presidência do Conselho de Ministros [PCM] (2011). Resolução do Conselho de Ministros n.º 46/2011, 14 de novembro: Cria o Grupo de Projeto para as Tecnologias de Informação e Comunicação. *Diário da República*, 1ª Série, n.º 218, 4848 – 4848.

Presidência do Conselho de Ministros [PCM] (2012). Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro: Aprova o Plano Global Estratégico de Racionalização e Redução de Custos com as TIC na Administração Pública, apresentado pelo Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC). *Diário da República*, 1ª Série, n.º 27, 596 – 605.

Presidência do Conselho de Ministros [PCM] (2016). Resolução do Conselho de Ministros n.º 33/2016, de 3 de junho: Constitui o Conselho para as Tecnologias de Informação e Comunicação. *Diário da República*, 1ª Série, n.º 107, 1735 – 1737.

Presidência do Conselho de Ministros [PCM] (2017). Resolução do Conselho de Ministros n.º 108/2017, de 26 de julho: Aprova a Estratégia TIC 2020 e o respetivo Plano de Ação. *Diário da República*, 1ª Série, n.º 143, 3938 – 4201.

União Europeia [UE] (2016). Tratado sobre o Funcionamento da União Europeia (Versão Consolidada). In *Jornal Oficial da União Europeia*. Acedido a 16 de março de 2020, em *https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF*

United Nations [UN] (1945). Carta das Nações Unidas e Estatuto da Corte Internacional de Justiça. In *United Nations*. Acedido a 27 de março de 2020 em *http://dag.un.org/bitstream/handle/11176/387353/PORTUGUESE-1976.pdf?sequence=1&isAllowed=y*

APÊNDICES

APÊNDICE A - GLOSSÁRIO

– ATIVIDADE DE INVESTIGAÇÃO CRIMINAL: Compreende o "conjunto de ações tendentes a descobrir, recolher examinar, interpretar, conservar e formalizar no inquérito, (…) as provas de factos concretos penalmente relevantes, bem como das circunstâncias envolventes e, ainda, as diligências destinadas a identificar, localizar e deter, (…) os responsáveis por tais factos, bem como a determinar o grau de responsabilidade" (Dias, 2006, p. 24).

- *BUSINESS INTELLIGENCE*: "Aplicações e tecnologias que se concentram na recolha, armazenamento e análise de dados e informação" (Gouveia & Ranito, 2004, p. 77), "incluindo *Big Data*" (Laudon & Laudon, 2018, p. 490). Proporcionam o acesso a dados e informação de diferentes fontes, de modo a ajudar os indivíduos a tomarem melhores decisões" (Gouveia & Ranito, 2004, p. 77).

- *DASHBOARD*: "São ferramentas visuais destinadas a apresentar dados de desempenho", disponibilizando os principais indicadores de desempenho de uma organização através de, por exemplo, gráficos e tabelas sintetizados, a fim de fornecer uma visão global de todas as medidas necessárias a adotar, apoiando o processo de tomada de decisão (Laudon & Laudon, 2018, p. 493).

- *DATA MINING*: "Processo de descoberta de padrões, dependências e relacionamentos com significado semântico que não se encontram explicitamente definidos nos meta-dados (ou nos repositórios analíticos) das organizações" (Cortes, 2005, p. 102).

- *DATA WAREHOUSE*: Trata-se de um "banco de dados que armazena dados atuais e históricos fundamentais para o processo de tomada de decisão. Estes dados são combinados com dados de fontes externas e transformados, corrigindo dados imprecisos e incompletos e restaurando os dados para relatórios e análises de gestão antes de serem introduzidos no repositório de dados. Um sistema de *Data Warehouse* também fornece uma variedade de ferramentas de consulta *ad hoc* e padronizadas ferramentas analíticas e recursos de relatórios gráficos" (Laudon & Laudon, 2018, pp. 255 - 258).

– FORÇAS DE SEGURANÇA: São "organismos policiais armados e uniformizados, integrados por pessoal com estatuto militar (GNR), com estatuto militarizado (PM), ou com estatuto civil (PSP), mas sempre com estrutura organizativa caracterizada pela obediência à hierarquia de comando em todos os níveis" (Dias, 2006, p. 26).

– HUMINT (*Human Intelligence*): Compreende as "informações pesquisadas através de pessoas. Tem a sua maior expressão nas informações internas, embora seja também empregue nas externas. Permite determinar os segredos mais guardados: intenções, planos, datas de ações, inovações tecnológicas, apoios externos, pormenores do equipamento, etc." (Alves, 2012, pp. 91-92).

- OLAP (*Online Analytical Processing*): Compreende uma "técnica de análise e de *reporting* avançado, sobre grandes volumes de dados assentes em estruturas de armazenamento multidimensionais" (Cortes 2005, p. 119), permitindo aos utilizadores "visualizarem os mesmos dados de formas diferentes, utilizando diversas dimensões" (Laudon & Laudon, 2018, p. 260).

– OSINF (*Open Source Information*): "Notícias obtidas através de fontes abertas, documentos não classificados, ou seja, ao alcance do público em geral, especialmente através da comunicação social, *internet* ou outro tipo de publicações" (Alves, 2012, p. 232).

– OSINT (*Open Source Intelligence*): "Processamento de notícias obtidas através de fontes abertas, documentos não classificados, ou seja, ao alcance do público em geral, especialmente através da comunicação social, *internet* ou outro tipo de publicações" (Alves, 2012, p. 232). Estas "fontes exigem, em alguns casos, que se proceda a uma validação da informação em cotejo com outro tipo de informação" (Bispo, 2004, p.90).

– REDE: "Dispositivo espacial, organizado como um tecido emalhado, conjunto de nós interligados, que permite observar e fazer circular informações, de modo mais ou menos abrangente e coordenado. Pode ser aberta ou clandestina" (Alves, 2012, p. 234).

– RISCO: "Probabilidade de a ameaça se concretizar – quantificação com vista a diminuir a incerteza resultante da análise detalhada da situação no alvo" (Alves, 2012, p. 235).

– SEGURANÇA: "Conjunto de medidas destinadas a salvaguardar, contra tentativas não só externa como internas, de obtenção de notícias, subversão e sabotagem, as intenções, potencialidades, atividades, pessoal, material e instalações e ainda fraquezas e vulnerabilidades que desejamos manter confinadas nacional ou que, no âmbito interno, se devem manter restritas em área e em número de pessoas que delas tenham conhecimento" (Cardoso, 2004, p. 266).

– SERVIÇOS DE SEGURANÇA: São "organismos públicos, integrados por agentes com estatuto análogo ao do pessoal da Administração Pública, hierarquicamente estruturados e institucionalmente vocacionados para o desempenho de atribuições específicas de natureza policial (PJ e SEF) ou no domínio das informações (SIS)" (Dias, 2006, p. 26).

APÊNDICE B – VERTENTES FUNCIONAIS DA INVESTIGAÇÃO CRIMINAL DAS UNIDADES TERRITORIAIS DA GNR: DESPACHO N.º 18/14 – OG

Quadro n.º 2 - Vertentes funcionais da Investigação Criminal das Unidades Territoriais da GNR: Transcrição do Despacho n.º 18/14 – OG

VERTENTES FUNCIONAIS DA IC	ÓRGÃOS PRINCIPAIS[97]	ATRIBUIÇÕES	SIIC TIPO I	SIIC TIPO II/III
IC -OPERATIVA	**NIC/CTer** (Núcleo de Investigação Criminal/ CTer)	• Proceder à investigação dos crimes de maior gravidade, complexidade ou dispersão que ocorram dentro da Zona de Ação (ZA) do CTer, ou que justifiquem a gestão concentrada da investigação.		❶ 98
	NIC/DTer (Núcleo de Investigação Criminal/ DTer)	• Proceder à investigação dos crimes que ocorram dentro da Zona de Ação (ZA) do DTer, para os quais a Guarda tem competência, e que não esteja atribuída a outros órgãos; • Outras que, direta ou indiretamente relacionadas com a IC, lhe sejam cometidas.		
	NAO (Núcleo de Apoio Operativo)	• Satisfazer os pedidos dos órgãos de IC do Comando do CTer, através de atividades de vigilância e seguimento e de captação de som e imagem; • Proceder à recolha de informações em fontes humanas (HUMINT) [99]; • Outras que, direta ou indiretamente relacionadas com a IC, lhe sejam cometidas.		
	NICCOA (Núcleo de Investigação de Crimes e Contra-Ordenações Ambientais)	• Assegurar, no âmbito das suas competências técnicas, a supervisão e controlo das investigações de crimes ambientais atribuídas ao órgão SEPNA do CTer; • Outras que, direta ou indiretamente relacionadas com a IC, lhe sejam cometidas.		
	NICAV (Núcleo de Investigação de Crimes em Acidentes de Viação)	• Proceder à investigação e exames de crimes resultantes de acidentes de viação que originem vítimas mortais ou feridos graves, assim como de outros crimes específicos em ambiente rodoviário para as quais a Guarda tem competência;		

[97] Foram considerados, no Quadro n.º 2, apenas os Órgãos com relevância para a presente investigação, sendo transcritas, do Despacho n.º 18/14 – OG, as respetivas atribuições.
[98] No caso das SIIC Tipo II/III, o NIC/CTer é eventual, ou seja, intervém em casos de crimes de maior gravidade, complexidade ou dispersão que ocorram dentro da Zona de Ação do Comando Territorial, ou que justifiquem a gestão concentrada da investigação, conforme o Despacho n.º 18/14 - OG.
[99] Ver conceito HUMINT no Apêndice A.

IC - OPERATIVA	**NICAV** (Núcleo de Investigação de Crimes em Acidentes de Viação)	• Outras que, direta ou indiretamente relacionadas com a investigação criminal, lhe sejam cometidas.
	NIAVE (Núcleo de Investigação e de Apoio a Vítimas Específicas)	• Proceder à investigação dos crimes cometidos, essencialmente, contra as mulheres, as crianças, os idosos e outros grupos de vítimas especialmente vulneráveis e prestar o apoio que, para cada caso, for adequado e possível; • Colaborar com as AJ no acompanhamento dos casos mais críticos, designadamente, através de uma continuada avaliação do risco; • Outras que, direta ou indiretamente relacionadas com a investigação criminal, lhe sejam cometidas.
IC - CRIMINALÍSTICA	**NTP** (Núcleo Técnico-Pericial)	• Realizar estudos e perícias no âmbito da Identificação Humana; • Recolher, tratar e inserir as resenhas[100] no AFIS, bem como gerir o respetivo arquivo; • Efetuar fotografia e recolha de imagem, no âmbito das inspeções técnicas judiciárias de 2º nível ao local do crime em apoio ao NAT, ou o processamento das recolhas efetuadas pelos NAT, para elaboração de Relatórios Fotográficos; • Recolher dados planimétricos no âmbito da inspeção judiciária de 2º nível ao local do crime em apoio ao NAT, ou processar as recolhas efetuadas pelos NAT, para elaboração de Relatórios de Exame Pericial de Planimetria Forense através da DIC; • Efetuar a Fotografia Forense de vestígios, em especial os lofoscópicos e a respetiva Cadeia de Custódia de Prova; • Realizar exames periciais de fotogramas, através das Equipas Técnico Periciais de Tecnologias Informáticas e Criminalísticas; • Assegurar a Cadeia de Custódia da Prova e tratar os vestígios em apoio dos NAT e dos órgãos de IC Operativa; • Efetuar o controlo de qualidade no âmbito das Inspeções Técnicas Judiciárias, elaborados pelos NAT; • Realizar estudos, exames e perícias; • Realizar Inspeções Técnicas Judiciárias Especiais ao local do crime, com recurso a meios técnico-periciais centralizados; • Realizar exames laboratoriais no âmbito da revelação de vestígios lofoscópicos; • Efetuar exames de balística funcional e exames químicos de recuperação de números de série;

[100] De acordo com a al. c) do art.º 2.º da Lei n.º 67/2017, de 9 de agosto (Identificação Judiciária Lofoscópica e Fotográfica), uma resenha lofoscópica compreende o "conjunto de suportes, impressos ou formulários onde são recolhidas as impressões digitais dos arguidos e condenados" (Assembleia da República [AR], 2017c, p. 4567).

IC - CRIMINALÍSTICA	**NTP** (Núcleo Técnico-Pericial)	• Realizar estudos, exames e perícias referentes à área da informática forense e apoio técnico no âmbito das tecnologias informáticas; • Outras que, direta ou indiretamente relacionadas com a investigação criminal, lhe sejam cometidas.		
	NAT (Núcleo de Apoio Técnico)	• Realizar inspeções técnicas judiciárias ao local do crime e a adequada preservação da Cadeia de Custódia da Prova, em apoio aos órgãos de IC – Operativa; • Realizar fotografia e recolha de imagem, no âmbito das inspeções técnicas judiciárias ao local do crime, para elaboração de Relatórios Fotográficos; • Realizar recolha de dados planimétricos no âmbito das inspeções técnicas judiciárias ao local do crime, para elaboração de Relatórios Planimétricos; • Realizar Resenhas/Clichés Fotográficos/Cotejos; • Recolher dados para a identificação humana em cenários de desastres e epidemias, de acordo com as técnicas de identificação DVI (*Disaster Victim Identification*); • Realizar autos de exame direto a armas e munições; • Outras que, direta ou indiretamente relacionadas com a investigação criminal, lhe sejam cometidas.		
	NDF (Núcleo Digital Forense)[101]	• Contribuir para a execução das competências dos órgãos superiores no âmbito da vertente de IC – Criminalística, através das suas secções, a de Recolha da Prova Digital[102] e a de Investigação de Ciberincidentes; • Realizar estudos, pareceres, exames e perícias referentes à recolha de prova em qualquer dispositivo, sistema ou infraestrutura no âmbito das Tecnologias de Informação e Comunicação; • Efetuar análise forense no âmbito da criptografia e de esteganografia; • Apoiar os órgãos da Guarda no âmbito da cibersegurança com atribuições nesta tarefa; • Garantir ações de investigação dos crimes tradicionais que se perpetuam com recurso às Tecnologias de Informação e Comunicação, os relativos à proteção de dados pessoais ou os que estejam relacionados com conteúdos ilícitos;		

[101] O Núcleos Digitais Forenses (NDF) não se encontram previstos no Despacho n.º 18/14 – OG, dado que foram criados posteriormente. Neste sentido, foram utilizadas a Informação n.º I319408-201806-DIC, de 14 de setembro de 2018, da DIC, e a Informação n.º I060366-202002, de 5 de fevereiro de 2020, da DIC.

[102] A Prova Digital, segundo Ramos (2014, p. 86), compreende "toda a informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações".

IC - CRIMINALÍSTICA	**NDF** (Núcleo Digital Forense)	• Organização da atividade forense digital em dois níveis: os *Evidence Specialist* e os *First Responders*. Os *First Responder* no apoio aos Núcleos de Investigação e aos Postos Territoriais e, ainda, os *Digital Evidence Specialist*, concentrados na DIC e em alguns CTer para um apoio direto na própria unidade e comados mais próximos que não têm esta capacidade instalada, destinada a intervir em casos de maior complexidade e /ou nos CTer com falta de recursos; • Outras missões que, direta ou indiretamente relacionadas com a investigação criminal, lhe sejam cometidas.
IC - ANÁLISE DE INFORMAÇÃO CRIMINAL	**NAIIC** (Núcleo de Análise de Informações e Informação Criminal)	• Apoiar os investigadores operativos, através da análise e inter-correlação das informações acedidas através dos Sistemas de Informação ou de estudos de fenómenos criminais; • Colaborar na deteção e caracterização, no âmbito da IC, de novos padrões e perfis criminais, devendo os resultados ser enviados à área das informações; • Realizar as missões inerentes à área de Informações, nomeadamente através de recurso a *Open Source Intelligence* (OSINT)[103]; • Processar as ordens e/ou pedidos de pesquisa que lhe forem dirigidos; • Zelar pela segurança das informações; • Outras que, direta ou indiretamente relacionadas com a investigação criminal, lhe sejam cometidas.

Fonte: Elaboração própria, com base em (GNR, 2014a, pp. 26-41)

[103] Ver conceito OSINT no Apêndice A – Glossário.

APÊNDICE C – CICLO DE PRODUÇÃO DE INFORMAÇÕES

A produção das informações concretiza-se com base num processo, tradicionalmente denominado por Ciclo de Produção de Informações (Alves, 2012).

Segundo as linhas gerais da EUROPOL (2002), o Ciclo de Produção de Informações materializa-se nas seguintes fases: Direção (*Tasking*), Recolha (*Collection*), Avaliação (*Evaluation*), Tratamento (*Collation*), Análise (*Analysis*) e Difusão (*Dissemination*).

No que concerne à Direção da pesquisa ou planeamento (*Tasking*), é fundamental que o analista defina com precisão os objetivos e prioridades a desenvolver. Neste sentido, é determinante que as tarefas ou objetivos estruturados tenham por base dimensões, quer operacionais, quer estratégicas, ao nível local, nacional ou internacional. A edificação deste planeamento pode resultar de requerimentos ou prioridades pré-existentes, relatórios, avaliações de risco ou ameaça, estudos e de conhecimentos adquiridos, com vista a determinar as tendências e padrões criminais, com base em indicadores de referência. Uma vez estabelecidas as prioridades, serão definidos os recursos a alocar, a fim de cumprir o quadro de prioridades e objetivos (EUROPOL, 2002).

O processo de produção de informações baseia-se na forma como são obtidos (*Collection*) e utilizados os dados. Neste sentido, uma vez recolhida a informação, deverá ser assegurado que a mesma é relevante e obtida de forma ordenada. O planeamento da recolha deverá incluir dados específicos, as fontes de informação e a construção de categorias, fundamentais no suporte ao processo de análise (EUROPOL, 2002).

A próxima etapa do Ciclo de Produção de Informações, a Avaliação (*Evaluation*), constitui uma das fases mais complexas deste processo. Deste modo, a fiabilidade das fontes de informação deverá ser cuidadosamente assegurada, o que exige, por parte do analista, a correta interpretação, tanto da qualidade da respetiva fonte, como da própria informação. Por consequência, a fonte e o seu produto deverão ser avaliados de forma independente, sendo imperativo o analista integrar as competências necessárias para a correta análise das informações. Para cumprimento desta finalidade, a presente fase deverá ser concretizada em paralelismo com a etapa anterior (*Collection*), visto que é difícil avaliar as informações sem a sua correta integração. Assim, a etapa da Avaliação encontra-se subordinada a dois princípios fundamentais: por um lado, não deverá ser influenciada pelo elemento subjetivo e pessoal, mas, exclusivamente, pela sua índole profissional e, por outro lado, a avaliação da

fonte deverá respeitar a individualidade entre a mesma e a própria informação (EUROPOL, 2002).

Uma vez disponível e avaliada toda a informação recolhida, a próxima fase, o Tratamento (*Collation*), tem início com a seleção da informação relevante, necessária para o trabalho de análise desenvolvido pelo analista. Contudo, importa considerar que, a utilização das ferramentas tecnológicas deverá ser encarada como um recurso que suporta, quer a capacidade interpretativa do analista no tratamento da informação, quer o trabalho de investigação desenvolvida no terreno (EUROPOL, 2002).

A fase que se segue, a Análise (*Analysis*) é considerada a fase mais importante do Ciclo de Produção das Informações, permitindo a verificação da relevância da informação recolhida, filtrando-a o quanto possível, mediante o recurso a modelos particulares mais adaptáveis ao caso específico. Assim, esta etapa contribui para determinar o valor da informação, a identificação de lacunas e, por conseguinte, direcionar a investigação. A partir da análise, o desenvolvimento das informações permitirão conduzir os objetivos das forças policiais, quer a curto prazo numa dimensão operacional, como a longo prazo numa dimensão estratégica (EUROPOL, 2002).

Na continuidade da fase de Análise, progredimos no sentido da fase final do Ciclo de Produção das Informações que, dada a sua natureza cíclica, poderá nunca ser dado como concluído. Todavia, é incontornável a necessidade de chegada a determinada fase, difundir o seu produto (*Dissemination*). Para tal, poderão ser utilizados relatórios, comunicações orais com base documental, boletins semanais e *briefings*, tratando-se de um passo crucial, uma vez que requer uma cuidada monitorização e controlo (EUROPOL, 2002).

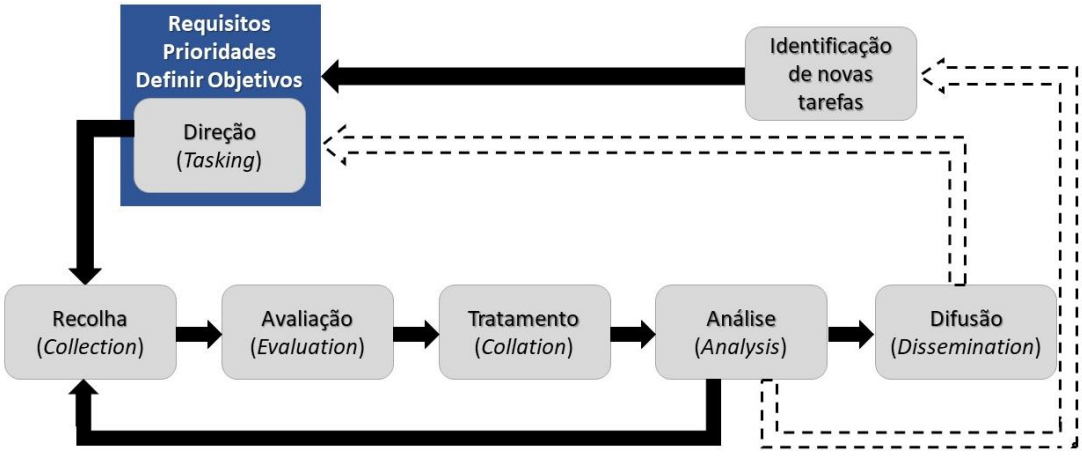


Figura n.º 3 - Ciclo de Produção de Informações *(The Intelligence Process)*

Fonte: Elaboração própria, com base em (EUROPOL, 2002, *Insert* 2)

APÊNDICE D - A SEGURANÇA DAS INFORMAÇÕES

Atualmente, cada "lado" procura transformar a pesquisa de informação do seu opositor o mais difícil possível, adotando medidas de segurança com o objetivo de garantir a segurança das informações, o que constitui um desafio (Cardoso, 2004).

A segurança das informações[104] visa a aplicação de um conjunto de medidas específicas com a finalidade de preservar o conhecimento e garantir "que não haja o descaminho nem o acesso não autorizado a matérias classificadas" (Alves, 2012, p. 88). Por outras palavras, a segurança das informações designada por INFOSEC (*Information Security*), ao abrigo da terminologia OTAN (Organização do Tratado do Atlântico Norte), compreende a aplicação de medidas de segurança, por forma a garantir a "proteção da informação processada, armazenada ou transmitida nos sistemas de informação e comunicação" (Sacramento, 2006, p. 156). O objetivo principal da implementação deste conjunto de medidas consiste na "proteção da informação relativa a matérias consideradas sensíveis" (Bispo, 2004, p. 86), estando somente acessíveis a quem tenha a necessidade de as conhecer[105] (EUROPOL, 2002). Deste modo, é assegurada não só a minimização dos riscos, como a prevenção das quebras de segurança (Cardoso, 2004).

Atendendo ao Relatório de Atividades da GNR de 2018, a garantia da segurança das informações constitui um princípio ativo para a prevenção de falhas de segurança[106] ou acidentes que prejudiquem o correto funcionamento dos SI (Guarda Nacional Republicana [GNR], 2019b). O acesso aos SI, computadores de rede e a própria troca de informação estão subordinados a requisitos de segurança edificados em quatro pilares essenciais: "autenticidade, confidencialidade, integridade e na disponibilidade da informação" (GNR, 2019b, p. 122). Ora, por força do n.º 3 do art.º 3.º da LISIOPC[107] (Lei da Interoperabilidade entre Sistemas de Informação dos Órgãos de Polícia Criminal), alterada pela Lei n.º 38/2015, de 11 de maio, o fornecimento de dados e informações deve reduzir-se ao que for considerado relevante e necessário para o sucesso da prevenção ou da IC.

[104] Cf. Anexo D – Segurança da Informação: Ficha de Procedimentos n.º 1/2020 – GNR (CO/DI).
[105] O Princípio da Necessidade de Conhecer tem como finalidade reduzir a possibilidade da informação operacional ou sensível ser difundida. De modo a garantir a sua minimização, torna-se vinculativo o conhecimento das matérias somente por parte de quem as trabalha diretamente (Esteves, 2004).
[106] Consultar conceito de Segurança no Apêndice A - Glossário.
[107] Lei n.º 73/2009, de 12 de agosto.

Face ao exposto, as unidades de informações que integram as forças policias "jamais se resumem a um mero banco de dados" (Clemente, 2007, p. 394), uma vez que utilizam diversos SI que garantem o armazenamento e processamento de informações, devendo estas ser preservadas, conforme o prefácio do APOTRGNR 22 - Regulamento de Utilização das Tecnologias de Informação da GNR (2014), da DCSI (Guarda Nacional Republicana [GNR], 2014d). No mesmo sentido, a GNR dispõe um SI central, o Sistema Integrado de Informações Operacionais de Polícia (SIIOP)[108]. Tendo em vista garantir a segurança das informações verificamos que, de acordo com as alíneas a) a h) do art.º 12.º do DR n.º 2/95, as principais condições a serem observadas, neste domínio, são o controlo da inserção, acesso, introdução e transporte dos dados, bem como a supervisão da entrada nas instalações, por qualquer pessoa não autorizada.

No entanto, apesar da sofisticação e da crescente evolução técnica das tecnologias e sistemas colocados à disposição da segurança e das matérias classificadas, "é ainda o Homem o elemento preponderante, mas também o mais vulnerável, de todo o sistema de segurança" (Cardoso, 2004, p. 273).

[108] Cf. n.º 1 do art.º 1.º do DR n.º 2/95, de 25 de janeiro.

APÊNDICE E – SUBMÓDULOS ADICIONAIS DO SIIOP

Adicionalmente aos submódulos apresentados no corpo da presente Investigação, deverão ser igualmente considerados os seguintes submódulos aplicacionais que dão corpo ao SIIOP, designadamente (AMA, 2017):

- **SIIOP-A**

  O submódulo Ambiente (SIIOP-A) foi estruturado com o intuito de suportar todas as atividades interligadas com o Serviço de Proteção da Natureza e Ambiente integrando, igualmente, a gestão dos autos de contraordenação, assim como a produção de guias de pagamento com registo Multibanco (AMA, 2017);

- **SIIOP-F**

  O submódulo Fiscal (SIIOP-F) integra o suporte às atividades relativas ao serviço fomentado no domínio Fiscal, pela Unidade de Ação Fiscal (UAF), envolvendo a gestão de autos de contraordenação, estatística e escrituração (AMA, 2017);

- **SIIOP-2S**

  O submódulo Salas de Situação (SIIOP-2S) materializa uma ferramenta fundamental na gestão de meios (humanos, escalas, materiais e viaturas) disponível, em tempo útil, e o seu acompanhamento pelas Salas de Situação até à resolução da ocorrência pelas patrulhas no terreno (AMA, 2017);

- **SIIOP-G**

  No que concerne ao SIIOP-G (Georreferenciação), enquanto componente de Sistema de Informação Geográfico, permite a visualização, em tempo útil, dos diversos rádios, da rede SIRESP (Sistema Integrado de Redes de Emergência e Segurança de Portugal), empregues no terreno e, por consequência, a sua geolocalização (AMA, 2017).

- **SIIOP-D**

  O submódulo Documental (SIIOP-D) é responsável pela garantia, monitorização e controlo dos fluxos de informação, assim como documentos e despachos, de modo centralizado, com origem, quer interna, quer externa à instituição (AMA, 2017).

- **SIIOP-T**

  O submódulo Trânsito (SIIOP-T) tem como finalidade prestar apoio às atividades de fiscalização rodoviária, permitindo o registo de acidentes, assim como também, o controlo de interdição de vias rodoviárias. Paralelamente, este submódulo permite a exportação de dados dos Boletins Estatísticos de Acidentes de Viação (BEAV), em modelo eletrónico, de modo automatizado para a Autoridade Nacional de Segurança Rodoviária (ANSR) (AMA, 2017);

- **SIIOP-O**

  O submódulo Ocorrências (SIIOP-O) tem por base um registo completo e detalhados das ocorrências de índole criminal, assim como de outros factos não classificados como crime, considerados relevantes, a fim de produzir relatórios com utilidades para as informações e para a investigação criminal (AMA, 2017).

APÊNDICE F – SISTEMA DE PARTILHA DE INFORMAÇÕES (PIIC)

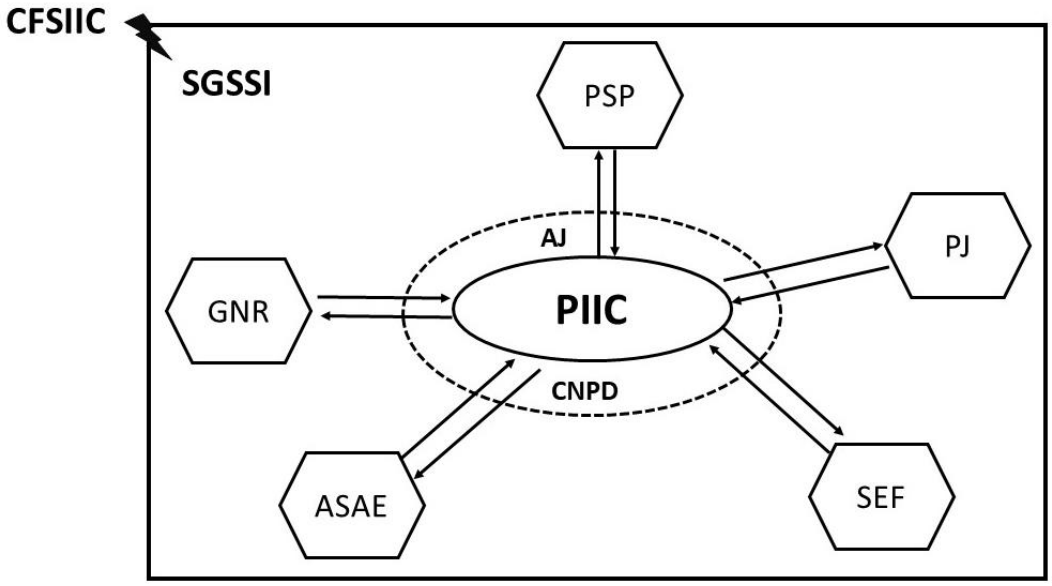


Figura n.º 4 - Sistema de Partilha de Informações (PIIC)

Fonte: Elaboração própria, com base em (Valente, 2019, p. 563)

APÊNDICE G – MEDIDAS NO ÂMBITO DAS TIC - GNR (2015 - 2020)

1. Estratégia da Guarda 2020

Tal como definido no Enquadramento Legal da Estratégia da Guarda 2020, a CRP, a LSI e a LOIC materializam três das principais traves mestras do enquadramento jurídico-constitucional da Guarda (Guarda Nacional Republicana [GNR], 2014e).

A prevenção da criminalidade e da prática de atos que infringem a lei e os regulamentos, bem como fomentar ações de IC atribuídas por lei, delegadas pelas AJ competentes ou requeridas pelas respetivas autoridades administrativas, constituem algumas das principais atividades que se encontram no centro de gravidade das atribuições da Guarda (GNR, 2014e).

Os fatores distintivos previstos na Estratégia em análise, são exercidos pelas diferentes valências da GNR, sendo que no que concerne à estrutura criminal, é fundamental sublinhar a elevada capacidade de recolha de informação, nomeadamente informação criminal, face à dispersão territorial. Deste modo, face ao elevado espetro de atuação da Guarda, a Estratégia 2020 da Guarda, prevê, no período compreendido entre 2015 e 2020, um esforço institucional contínuo nos avanços respeitantes à especialização técnica e científica dos respetivos recursos, no desenvolvimento da vertente tecnológica, bem como em novos métodos ao nível da cooperação e da coordenação, quer no domínio interno, ou seja, nas relações com outras forças, quer ao nível externo/internacional (GNR, 2014e).

Nesta senda, os requisitos operacionais são estruturados por intermédio de um conjunto sólido de capacidades orientadas pelo nível de ambição desenhado com base na disponibilidade e qualidade dos recursos. Por conseguinte, a Estratégia da Guarda 2020, tendo como referência a sua pluralidade de domínios de atuação, vem privilegiar uma estrutura organizacional cimentada nas seguintes diretrizes: unidade estratégica, coordenação, utilização racional e eficiente de recursos e inteligência estratégica. A Unidade estratégica, enquanto ferramenta necessária para a agregação de todas as dimensões institucionais, permite convergi-las para os objetivos estratégicos comuns. Por sua vez, a coordenação contribui para a cooperação e colaboração com entidades diversas. Paralelamente, a utilização racional e eficiente de recursos vem garantir um alinhamento entre o objetivo estratégico definido e a natureza das ameaças e riscos em causa. Por fim, a inteligência estratégica, definido como "potencial estratégico da Guarda", assume um papel

preponderante na construção de uma visão prospetiva, bem como na capacidade de planeamento e tomada de decisão (GNR, 2014e, p. 50).

1.1. Linhas de Orientação Estratégica

Com a finalidade de garantir a prossecução do modelo estruturado na Missão e na Visão institucionais, foram delineadas na presente Estratégia, quatro Linhas de Orientação Estratégica, designadamente (GNR, 2014e):

- "Força de Segurança Presente e Próxima" ("Reforçar a Confiança dos Cidadãos na Instituição") (GNR, 2014e, p. 67). A GNR constitui uma força de segurança com elevada dispersão e presença territorial, o que conduz a uma proximidade para com o Cidadão. Esta presença é garantida mediante o reforço do patrulhamento comunitário e de proximidade, centrado na proteção dos cidadãos (GNR, 2014e).

- "Otimizar para criar Valor" ("Otimizar os recursos criando valor") (GNR, 2014e, p. 68), isto é, utilizar os recursos disponíveis com critério e de forma racional, a fim de garantir elevados padrões de operacionalidade. Para tal, é essencial criar novos caminhos de financiamento, mediante projetos de modernização de equipamentos e tecnologias e, não menos importante, de formação e especialização dos recursos humanos (GNR, 2014e).

- "Modernizar, Inovar e Simplificar" ("Modernizar, inovar e simplificar, garantindo a celeridade e eficiência dos processos") (GNR, 2014e, p. 70). Esta Linha Estratégica tem em vista não apenas uma atuação profícua em prol da segurança do cidadão, como também, o redireccionamento constante para a missão institucional. Consequentemente, a Estratégia da Guarda 2020, privilegia a inovação tecnológica e o recurso às TIC, enquanto meio ao serviço da segurança. Estas promovem a desmaterialização de processos e a simplificação de procedimentos, moldando a estrutura operacional e potenciando uma crescente articulação entre as FSS. É neste contexto que, a valorização da formação dos recursos humanos, apresenta caráter vinculativo, sendo fundamental, consequentemente, apostar numa formação técnica sólida com o intuito de tornar os recursos humanos mais qualificados. A fim de garantir a modernização, inovação e simplificação, a Estratégia 2020 define como prioritário garantir a continuidade do esforço na consolidação do Sistema Integrado de Informação Criminal e valorizar a partilha de informações operacionais entre as FSS, por intermédio da PIIC (GNR, 2014e).

Por outro lado, o SIIOP materializa o sistema pilar na prestação ao Cidadão de um serviço policial de qualidade, contribuindo para uma superior capacidade de resposta

operacional no domínio da prevenção e combate à criminalidade. Paralelamente, contribui para a interoperabilidade entre os SI dos diferentes parceiros que garantem a segurança quer nacional, quer internacional (GNR, 2014e).

Neste âmbito, afirma-se igualmente como estratégia da Guarda, a fomentação de SI como instrumento de apoio à Decisão, estabelecendo como meta a sua operacionalização no domínio da formação e desmaterialização do processamento da informação. A implementação de medidas de modernização operacional decorre do levantamento de um leque de domínios prioritários, designadamente, no que concerne à racionalização e simplificação de formalidades, desenvolvimento de instalações e equipamentos e, também, a adoção de um conjunto de sistemas e métodos modernizadores que contribuam para uma resposta célere às solicitações legítimas dos cidadãos, tendo em vista o aumento da qualidade de intervenção operacional (GNR, 2014e).

- "Qualidade – Cooperar para Melhorar" ("Incrementar a cooperação e articulação com outros organismos procurando melhorar a qualidade dos Serviços") (GNR, 2014e, p. 72). Um dos desígnios da GNR é contribuir para a cooperação institucional e garantir uma estreita articulação com os diferentes atores pertencentes aos sistemas nacionais de segurança, proteção e defesa e com os quais a Guarda interage diariamente. Enquadra-se igualmente, neste domínio, o fortalecimento de relações com as forças congéneres, uma vez que contribuem para a partilha de experiências, lições aprendidas e conhecimentos, fundamentais no desenvolvimento e capacitação dos recursos humanos (GNR, 2014e).

Mediante um quadro de proximidade de relações com as forças congéneres, são definidas na Estratégia da Guarda 2020, diferentes iniciativas com o intuito de estreitar essas relações, nomeadamente: implementar uma troca de informações policiais mais aprofundada e em número superior devido à complexidade e flexibilidade inerente à evolução dos métodos e fenómenos criminais; intensificar os contactos num grau central e local entre os Oficiais de Ligação, no âmbito das Operações, Informações, IC, entre outras e, não só mas também, ampliar o intercâmbio no domínio da formação, garantindo a uniformização de procedimentos e mecanismos de intervenção. A afirmação da GNR no âmbito da cooperação internacional compreende uma parcela com atenção estratégica do ponto de vista organizacional, particularmente no domínio da IC, no âmbito da União Europeia (GNR, 2014e).

1.2. Objetivos Estratégicos

As Linhas de Orientação Estratégica definidas constituem a diretriz de ação da Guarda, a partir das quais foram deduzidos os objetivos estratégicos de suporte esboçados para o período 2015-2020. Estes abrangem, no seu campo de visão, diversas medidas edificadas numa linha de atuação sobre os fenómenos da criminalidade, bem como no desenvolvimento e operacionalização da estrutura tecnológica institucional. Tendo em conta os objetivos estruturados nos pilares anteriormente descritos, destacam-se (GNR, 2014e):

- Desenvolver a capacidade de Comando, Coordenação e Controlo harmonizada com a gestão das estruturas de apoio operacional, aperfeiçoando os sistemas tecnológicos e de informação, de modo a orientar com superior eficácia operações, quer a nível tático (Comandos Territoriais), quer a nível tático-operacional (Comando Operacional);
- Desenvolver um maior contacto entre a Guarda e o cidadão, potenciando os Programas Especiais de Prevenção e Policiamento e o recurso às redes e TI;
- Fortalecer a supervisão das principais fontes de perigo, com o intuito de garantir a prevenção, redução e repressão da criminalidade, assim como de comportamentos e condutas que coloquem em causa a segurança e tranquilidade públicas;
- Promover a capacidade de intervenção na dimensão ciber, capacitando a Instituição para uma resposta integrada à cibercriminalidade;
- Reforçar a eficiência operacional, através da requalificação de infraestruturas e equipamentos, entre os quais, a nível tecnológico, garantindo melhores condições de trabalho dos militares;
- Priorizar a utilização das novas TIC, reforçando a formação dos recursos humanos, "(...) desmaterializando atos e simplificando procedimentos, visando requalificar o serviço operacional e de apoio (...)" (GNR, 2014e, p. 79) e contribuindo para o fortalecimento da cooperação e articulação com as restantes FSS;
- Potenciar a simplificação e racionalização de procedimentos, melhorando a interoperabilidade e articulação entre os diferentes SI operacionais e de apoio ao serviço operacional;
- Fortalecer e qualificar a capacidade de resposta operacional em diversos domínios, entre os quais, a IC.

2. Análise dos Planos de Atividades 2015-2019

Um dos instrumentos de gestão essenciais para o enquadramento da atuação de determinada instituição é Plano de Atividades Anual. Este, tal como previsto no Decreto-Lei n.º 183/96, de 27 de setembro, permite delinear a estratégia, priorizar opções, programar ações e levantar e mobilizar os recursos necessários. Segundo o n.º 2 do art.º 1.º do referido Decreto-Lei, o Plano de Atividades Anual deve detalhar os objetivos a atingir, enquanto instrumento institucional de referência, para o ano em análise. Consequentemente, todo o trabalho desenvolvido ao longo do ano, bem como os resultados obtidos, são materializados através do Relatório de Atividades Anual, igualmente previsto no Decreto-Lei n.º 183/96, de 27 de setembro. Analisando o n.º 3 do art.º 1.º do referido Decreto-Lei, o Relatório de Atividades deverá mencionar os objetivos alcançados, o grau de realização dos programas e os recursos empregues na prossecução dos objetivos delineados no Plano de Atividades.

Neste sentido, tendo como margem de análise a definida para a presente investigação, serão abordados os Planos de Atividades referentes ao período entre 2015 até à atualidade, a fim realizar um levantamento dos objetivos institucionais no âmbito das TI, enquanto instrumento promotor da eficácia operacional. Deste modo, é fundamental analisar as medidas delineadas em cada ano, bem como os resultados decorrentes, no sentido de compreender os pontos de contacto entre as mesmas e as necessidades e problemas operacionais existentes na estrutura de IC das Unidades Territoriais.

Os Planos de Atividades da GNR para o período em análise, edificam as atividades a desenvolver em dez programas centrais. Todavia, com o intuito de analisar as medidas definidas no âmbito das TI e o seu emprego no domínio operacional, serão tidos como base de análise os quatro programas seguintes: P1 (Emprego Operacional e Comando e Controlo), P2 (Formação e Gestão do Conhecimento), P4 (Projetos Cofinanciados) e P7 (Sistemas e Tecnologias de Informação) (GNR, 2014f; GNR, 2015; GNR, 2016c; GNR, 2017a; GNR, 2018d).

O Programa 1 (Emprego Operacional e Comando e Controlo) remete para a globalidade de operações e demais ações operacionais que estruturam a principal atividade desenvolvida pela GNR, no sentido da segurança e tranquilidade pública. A partir de 2016, este Programa foi subdividido em patamares distintos, tendo sido selecionados, como objeto de análise, a Prevenção e Combate ao Crime e o Comando, Coordenação e Controlo. Em 2018, foi acrescentado a este Programa o domínio das Informações. Em primeiro lugar, a Prevenção e Combate ao Crime propõe otimizar e reforçar a capacidade de IC, isto é,

prevenir, minimizar e reprimir os fenómenos criminais, controlando as principais fontes de perigo, neste âmbito. Por seu turno, o Comando, Coordenação e Controlo remete para a sistematização e estruturação das capacidades operacionais utilizando, para tal, uma conjugação eficiente entre os recursos humanos, material, equipamento, estruturas e treino, cimentadas numa perspetiva adequada e na interoperabilidade de sistemas. Por fim, no que concerne ao domínio das informações, o foco principal versa sobre a estruturação e desenvolvimento do Centro de Informações da Guarda (CIG)[109] (GNR, 2014f; GNR, 2015; GNR, 2016c; GNR, 2017a; GNR, 2018d).

Relativamente ao Programa 2 (Formação e Gestão do Conhecimento), o mesmo enquadra todas as medidas de desenvolvimento e disseminação da formação e do conhecimento a fomentar no ano em análise. Traduz-se, portanto, na atualização e formação dos recursos humanos da Instituição, com o intuito de prepará-los, a fim de exercerem a sua atividade com elevados patamares de qualidade e competência (GNR, 2014f; GNR, 2015; GNR, 2016c; GNR, 2017a; GNR, 2018d).

O Programa 4 (Projetos Cofinanciados) determina o conjunto de prioridades referentes à aquisição de recursos, através de Fundos Comunitários, sendo estes disponibilizados para o aprofundamento e reforço de capacidades institucionais (GNR, 2014f; GNR, 2015; GNR, 2016c; GNR, 2017a; GNR, 2018d).

Diretamente relacionado com o tema da presente investigação, o Programa 7 (Sistemas e Tecnologias de Informação), abrange toda a gestão dos Sistemas e Tecnologias de Informação, nomeadamente, a obtenção de equipamento informático (*hardware* e *software*), a gestão da infraestrutura tecnológica, bem como a obtenção de equipamentos de telecomunicações. Para tal, estas atividades deverão estar articuladas com a melhoria da capacidade de Comando, Controlo e Coordenação alinhada com o apoio operacional, promovendo a utilização dos sistemas tecnológicos e de informação (GNR, 2014f; GNR, 2015; GNR, 2016c; GNR, 2017a; GNR, 2018d).

Os principais objetivos dos programas em análise prendem-se com a estruturação e melhoria das capacidades operacionais e a utilização da tecnologia ao serviço da atividade operacional. Neste sentido, apresenta-se seguidamente, o Quadro n.º 3, referente às

[109] O CIG foi criado enquanto instrumento de apoio à decisão alicerçado na modernidade tecnológica e evolução procedimental, com especial ênfase na capacidade OSINT. O CIG constitui um centro de receção, partilha e difusão de informações provenientes das diferentes Direções e Unidades, um gestor e utilizador da vertente específica das informações no SIIOP e, também, um centro de alarmística que permite sinalizar a ocorrência de incidentes, eventos ou outros, permitindo, por sua vez, a identificação de ameaças e eventos em tempo real, maximizando a oportunidade de intervenção e eficiência operacional, conforme a Informação n.º I060627-201802-DI, de 22 de fevereiro de 2018, da DI/CO.

principais medidas delineadas nos Planos de Atividade entre 2015 e 2019, no que concerne à atividade operacional em fusão com a vertente de IC, assim como a utilização e desenvolvimento das TIC, neste domínio. Posteriormente, serão analisados os principais resultados decorrentes da implementação destas medidas recorrendo, para tal, aos Relatórios de Atividades subsequentes.

Quadro n.º 3 - Tecnologias de Informação e Comunicação: Principais medidas previstas nos Planos de Atividades da GNR (2015-2019)

2015	**P1: Emprego Operacional e Comando e Controlo**		- Dinamização dos Programas Especiais de Prevenção e Policiamento, bem como das parcerias locais a fim de prevenir e reduzir a criminalidade.
	P2: Formação e Gestão do Conhecimento		- Ponderação acerca da implementação de um **sistema *e-learning* alargado**: utilização de equipamentos e redes móveis.
	P4: Projetos Cofinanciados		- Desenvolvimento de projetos no âmbito da prevenção e combate da criminalidade, nomeadamente o **Programa prevenir e combater a criminalidade (ISEC)**.
	P7: Sistemas e Tecnologias de Informação		- Prossecução da estratégia parcelar definida na "Estratégia da Guarda 2020" com a finalidade de garantir a **unificação dos SI** numa plataforma única; - Desenvolvimento de esforços no sentido da conclusão do **Projeto SAMA** (Sistema de Apoio à Modernização e Capacitação da Administração Pública), mediante o incremento da **infraestrutura física** e da **ampliação do SIIOP** a todo o dispositivo; - Estruturação do novo **Centro de Comando, Coordenação e Controlo Operacional** do Comando-Geral da Guarda (CCCO); - **Desenvolvimento tecnológico das Salas de Situação** dos Comandos Territoriais de Setúbal e Santarém, com perspetiva de dilatar esta política às Salas de Situação de todo o dispositivo territorial.
2016	**P1: Emprego Operacional e Comando e Controlo**	**Prevenção e Combate ao Crime**	- **Implementação das áreas forenses** de Análise Digital e Marcas Instrumentais; - Desenvolvimento e aquisição de instrumentos para a vertente de Análise de Informação Criminal e os Núcleos Técnico-Periciais (NTP); - Extensão da valência IC – Criminalística às Regiões Autónomas; - Constituição de equipas "*First Responders*": investigação de ameaças do âmbito digital.
		Comando, Coordenação e Controlo	- **Dilatação da formação**, implementação e utilização do Sistema SIIOP às Regiões Autónomas; - Continuação da fomentação dos sistemas de apoio à decisão e gestão documental; - **Operacionalização da interoperabilidade** entre o SIIOP, SIGRI, SIG-GNR e o Sistema de Gestão Documental.
	P2: Formação e Gestão do Conhecimento		- Ponderação acerca da implementação de um sistema *e-learning* alargado; - Desenvolvimento de diversas iniciativas: 1. Programação do Sistema de Gestão de Qualidade; 2. Programação do "**Centro de Lições Aprendidas da Guarda**"; 3. Promoção da conceção de **Módulos *e-learning;*** - Estudo e incremento de um portal de formação – **plataforma de *Learning Management System* (LMS)**.
	P4: Projetos Cofinanciados		- Aquisição de tecnologia destinada a **sistemas de vigilância** e para o **projeto de interoperabilidade entre o SIGRI e o SIIOP** (*hardware*, *software* e desenvolvimento) – Fundo de Segurança Interna;

2016	**P4: Projetos Cofinanciados**		- **Projeto "Portugal 2020 (P2020)**": investimento da Administração Pública na eficiência e capacidades operacionais da Guarda, investindo na interoperabilidade dos SI operacionais e de apoio ao serviço operacional. Reforço no domínio tecnológico – *software*, *hardware* e o seu desenvolvimento.
	P7: Sistemas e Tecnologias de Informação		- **Aquisição de material e equipamentos**, *hardware* e *software*: deteção de ameaças, recolha e processamento de informação, manutenção da custódia de prova digital; - **Fortalecimento da interoperabilidade entre Sistemas** – realização de estudos para o levantamento dos requisitos operacionais e técnicos; - **Edificação de um Sistema de Informações da Guarda**, no âmbito da Estratégia da Guarda 2020 - Desenvolvimento do projeto de criação do **Centro de Informações da Guarda (CIG)**; -Utilização da Plataforma de Monitorização do Plano Estratégico: avaliar e monitorizar, em tempo útil, a concretização dos objetivos estratégico e operacionais.
2017	**P1: Emprego Operacional e Comando e Controlo**	**Prevenção e Combate ao Crime**	- Início do processo de credenciação e de certificação da vertente de **Criminalística**; - Emprego do patrulhamento orientado com base na recolha de informações, subordinado ao modelo policial ("***Intelligence Led Policing***").
		Comando, Coordenação e Controlo	- **Promoção** do recurso às **funcionalidades de registo de dados, do submódulo de dados** (subsistema do SIIOP-O), cimentando o Ciclo de Produção de Informações na Guarda; - Desenvolvimento da **capacidade analítica e preditiva** da GNR, mediante uma **estreita articulação entre a DI e a DIC**, por forma a melhorar a proatividade de atuação e o apoio à tomada de decisão; - Estabelecimento de uma **unidade OSINT**, resultante da edificação de um **Centro de Informações da Guarda (CIG)**, garantindo a permanente recolha, análise e fluxo das informações policiais e criminais (em tempo real) em apoio da atividade operacional – maximização da intervenção e eficiência operacional.
	P2: Formação e Gestão do Conhecimento		- Implementação do "**Centro de Lições Aprendidas da Guarda**"; - Formação da Estrutura Nuclear e Rede de Suporte do "Centro de Lições Aprendidas da Guarda".
	P4: Projetos Cofinanciados		- Prosseguimento dos objetivos definidos para o projeto "**Portugal 2020 (P2020)**".
	P7: Sistemas e Tecnologias de Informação		- **Migração dos Sistemas de Voz para VOIP (*Voice Over Internet Protocol*)** - conceção de um canal multisserviços nos acessos da RNSI, possibilitando a interligação de serviços de voz sobre IP, sem custos associados (sincronia com as medidas TIC 2020 do MAI). **Instalação de acessos tipo VOIP SIP-TRUNK**, anulando diversos acessos locais e assinaturas mensais, o que conduz a poupanças consideráveis no âmbito das comunicações; - **Obtenção de terminais de redes de dados periféricos** – manutenção, em tempo útil, dos parques de terminais de processamento de dados da Guarda, considerando o tempo de vida útil dos equipamentos e custos associados; - **Infraestruturas de redes locais e equipamentos ativos para conexão à RNSI** – incremento de infraestruturas de rede que cumpram os requisitos de conexão à RNSI das instalações da GNR, permitindo completar a cobertura digital da Guarda e o suporte à modernização dos SI, nomeadamente, o SIIOP; - **Sistemas Multimédia de apoio às Salas de Situação** – utilização das TIC como ferramentas de reforço da eficácia operacional mediante a atualização permanente da informação georreferenciada e classificada.

2018	**P1: Emprego Operacional e Comando e Controlo**	**Prevenção e Combate ao Crime**	- Continuação do processo de Credenciação e de Certificação da vertente de **IC – Criminalística**; - Implementação das áreas forenses de **Marcas Instrumentais** e **Áudio Digital**.
		Informações	- Desenvolvimento de uma **componente alarmística** com a unificação de todas as notícias adquiridas, a fim de sinalizar os incidentes que necessitam de um tratamento diferenciado; - **Reforço da capacidade preditiva e prospetiva da Repartição de Análise**, fomentando a articulação com outros órgãos, nomeadamente, a DO, DIC, CCCO (Centro de Comando e Controlo Operacional), GTTSI (Grupo de Trabalho para as Tecnologias de Sistemas de Informação) e CTer e com outras Forças ou entidades num prisma de cooperação policial no domínio das informações.
		Comando, Coordenação e Controlo	- Operacionalização do contato direto com o Ponto Único de Contacto para a Cooperação Policial Internacional (PUC-CPI); - **Levantamento de boas práticas e metodologias** de atuação mediante articulação e intercâmbio com outras estruturas semelhantes.
	P2: Formação e Gestão do Conhecimento	- Ponderação acerca da implementação de um sistema *e-learning* alargado.	
	P4: Projetos Cofinanciados	- Prosseguimento dos objetivos definidos para o **projeto** "**Portugal 2020 (P2020)**", com **reforço da qualidade do serviço**, por meio do Projeto de Certificação do Atendimento ao Cidadão.	
	P7: Sistemas e Tecnologias de Informação	- **Convergência e implementação dos Sistemas de Videovigilância** - Enquanto recurso comum no âmbito da segurança de instalações, contribui para efetuar o levantamento das sinergias da RNSI, bem como a convergência de locais de visualização e registo particulares, economizando, deste modo, recursos humanos. Todavia, carece de definição normativa técnica; - **Finalização do Projeto de criação do Centro de Informações da Guarda (CIG)**, com foco na estruturação da capacidade de OSINT. Este Centro irá permitir uma análise e produção profícua de informações mediante a partilha e intercâmbio de informação policial com outras entidades; - Diversificação dos acessos a fontes de informação pelas estruturas de Comando e Controlo, nomeadamente, o CCCO e as Salas de Situação.	
2019	**P1: Emprego Operacional e Comando e Controlo**	**Prevenção e Combate ao Crime**	- Consolidação dos reajustamentos no modelo vigente da estrutura de IC, procurando a sua **simplificação e o desenvolvimento de eficácia e eficiência na intervenção** dos órgãos e da estrutura operacional da Guarda; - Consolidação do processo de Credenciação e Certificação da vertente de **IC – Criminalística**; - Continuação do processo de implementação das áreas forenses de Marcas Instrumentais e Áudio Digital; - Fomentar e equipar os **Núcleos de Apoio Operativo (NAO)** e os **Núcleos Técnico-Periciais (NTP)**; - Continuação do desenvolvimento das ferramentas necessárias ao incremento do sistema de patrulhamento orientado pelas informações (segundo o modelo *Intelligence Led Policing*).
		Informações	- **Otimização e crescimento da capacidade operacional** do Centro de Informações da Guarda, com destaque para a capacidade OSINT e incremento da sua capacidade de análise;

2019	**P1: Emprego Operacional e Comando e Controlo**	**Informações**	- Utilização do **CIG** como centro único da GNR no **intercâmbio de informações** com o Ponto Único de Contacto para a Cooperação Internacional (PUC-CPI) do Sistema de Segurança Interna; - Continuação do desenvolvimento da **Repartição de Análise**, a fim de potenciar a fomentação da sua capacidade prospetiva e preditiva.
		Comando, Coordenação e Controlo	- Continuação do desenvolvimento das iniciativas delineadas em 2018.
	P2: Formação e Gestão do Conhecimento		- Ponderação acerca da implementação de um sistema *e-learning* alargado; - Promoção do Ciclo Anual de Produção de Doutrina, com primazia para a vertente Operacional, assim como também, na fomentação de baias orientadoras no que diz respeito à dimensão processual de construção de Doutrina; - Prossecução do **processo de desmaterialização do sistema de formação** por intermédio da plataforma SIGForm, bem como de outras plataformas potenciadoras do processo formativo; - Implementação do "Sistema de Lições Aprendidas da Guarda".
	P4: Projetos Cofinanciados		**Projeto "Portugal 2020 (P2020):** - Participação da GNR no **projeto POCI-020-0550-FEDER-035416 – Transformação Digital da GNR**, possibilitando à Guarda assegurar a interoperabilidade entre SI através do SIIOP v3 com *dashboard* e capacidade de *Business Intelligence*[110]. Este projeto é desenvolvido no âmbito do SAMA, com o intuito de promover a modernização do Estado e, consequentemente, da Estratégia 2020 da Guarda; - No âmbito anterior, participação da GNR no **projeto POCI-05-5762-FSE-000160 – Certificação do atendimento e do sistema de formação**, com o intuito primário de certificar o Sistema de Gestão da Qualidade da Guarda.
	P7: Sistemas e Tecnologias de Informação		- Materialização de um **Sistema de Informações da Guarda**, tendo em vista otimizar e desenvolver a capacidade operacional do CIG, com destaque para as **capacidades de OSINT** e de **Análise** (à semelhança da medida prevista no P1 – Informações); - No domínio das Infraestruturas Críticas, acompanhar e cimentar a malha digital de todas as valências da GNR, tendo em vista **integrar os sistemas informáticos numa plataforma única**, permitindo a **otimização dos ciclos de decisão**. Deste modo, será reforçada a capacidade de interoperabilidade das diversas valências da Guarda perante um incidente numa Infraestrutura Crítica, permitindo a integração funcional dos sistemas e permitindo a identificação de lacunas.

Fonte: Elaboração própria, com base em (GNR, 2014f; GNR, 2015; GNR, 2016c; GNR, 2017a; GNR, 2018d)

[110] Consultar conceito de *Dashboard* e *Business Intelligence* no Apêndice A.

3. Análise dos Relatórios de Atividades 2015-2018

Analisando o quadro de referência acima estruturado, é possível verificar as principais medidas delineadas pela Guarda em cada ano correspondente, no que concerne ao desenvolvimento e operacionalização das TI. Deste modo, é fundamental avaliar os principais resultados dos objetivos definidos, em cada ano, a fim de compreender a necessidade de desenvolvimento e de utilização das TIC ao serviço da atividade operacional e, por conseguinte, da IC.

Analisando os relatórios de atividades entre 2015 e 2018, concluímos que a incorporação e a interoperabilidade da vertente informática presente na Guarda agregam uma prioridade, uma vez que a sua concretização gera fiabilidade e qualidade de informação, celeridade dos processos de trabalho e, também, uma racionalização dos recursos, quer humanos, quer materiais. A interoperabilidade entre aplicações constitui um dos desígnios tecnológicos da Guarda, podendo utilizar tecnologias normalizadas que facilitem a partilha de instâncias de bases de dados (GNR, 2016d; GNR, 2017b; GNR, 2018e; GNR, 2019b).

Em 2015, no domínio das plataformas de apoio à decisão e de natureza estratégica previstas no Relatório de Atividades de 2015, destacam-se as seguintes: o SIIOP (Sistema Integrado de Informações Operacionais de Polícia), o SIG-SIRESP (Sistema de Informação Geográfico SIRESP) e, no âmbito tático-operacional, o SG2S (Sistema de Gestão de Salas de Situação), o GNRMobile e o STM (Sistema de Transmissão de Mensagens) (GNR, 2016d).

Por outro lado, mais concretamente no âmbito das plataformas tecnológicas, foram efetuadas reuniões do Grupo de Acompanhamento da Plataforma para o Intercâmbio de Informação Criminal (GA-PIIC), com o objetivo de assegurar a implementação da totalidade das orientações estratégicas, tendo como base a gestão transversal e a evolução da PIIC, designadamente, em relação a novas funcionalidades, acesso a bases de dados complementares e fontes de informação dos OPC (GNR, 2016d).

No âmbito dos Sistemas e TI aplicadas à parte operacional, procurou-se manter o esforço no domínio dos programas especiais de policiamento e prevenção, num patamar tecnológico, designadamente, queixa eletrónica, violência doméstica, e, não só, mas também, o desenvolvimento do Sistema AFIS (GNR, 2016d).

Procedeu-se, igualmente, à implementação e manutenção parcial do Sistema Estratégico de Gestão e Apoio da Atividade Policial e Informação Criminal (SEG2APIC),

permitindo processar e transacionar informação de múltiplos SI internos e externos, possibilitando efetuar "*Data Warehousing*", "*Business Intelligence*" e procedimentos compostos de "*Reporting*" e "*Dashboarding Policial*". Concretizou-se, ainda, a implementação, manutenção e elaboração de especificações técnicas e funcionais (em cerca de 62%) de uma Plataforma de Integração e Gestão Operacional (PIGO), a fim de tornar mais eficiente e ágil a troca e tratamento de informações, bem como combater e prevenir os efeitos das ameaças criminais. Por fim, no domínio da formação, a utilização do Portal da Formação, revela um elevado impacto na formação, assente no sistema *e-learning* e *b-learning* (GNR, 2016d).

O Relatório de Atividades referente a 2016, destaca as seguintes plataformas de apoio à decisão e de natureza estratégica: o STM e o SIIOP com os seus múltiplos submódulos: principal (P), salas de situação (2S), ocorrências (O), trânsito (T), ambiente (A), documental (D) e, também, georreferenciação (G) e o sítio da GNR na *internet* (GNR, 2017b).

Em relação ao suporte dos diversos sistemas TIC, foi finalizado em 2016 a ligação de mais de duas centenas de unidades, permitindo a extensão da cobertura digital a toda a instituição e a extensão a dez distritos dos Sistemas de Informação e Comunicação, contribuindo para o tratamento sistemático dos dados reunidos pelos serviços centrais (GNR, 2017b)

No que concerne aos serviços de voz, foi fomentada sobre o suporte da RNSI, a interligação dos cerca de nove mil terminais de voz sobre IP, contribuindo para a realização de comunicações fixas sem custos entre si. Neste processo foram, também, cancelados aproximadamente 5 centenas de acessos fixos de comunicações, analógicas e digitais, dependentes de assinaturas mensais fixas, mediante a migração para acessos SIP-Trunk, num número diminuído a, aproximadamente, 3 dezenas, o que permitiu uma redução de cerca de 290 mil euros dos encargos com comunicações no ano em análise (GNR, 2017b).

Relativamente às comunicações em videoconferência, foi possível a extensão a todas as Unidades e Comandos da GNR de um terminal de videoconferência, o que conduziu a uma poupança considerável em deslocamentos. Ao nível das Salas de Situação, algumas foram dotadas com salas técnicas com energia assistida com autonomia, a fim de reforçar o suporte dos Sistemas de Informação e Comunicação críticos no domínio do Comando e Controlo da GNR (GNR, 2017b).

No âmbito da informação criminal, foram elaborados 577 Ordens/Pedidos de pesquisa. As ordens de pesquisa em análise tinham em vista a recolha de informação criminal, a fim de garantir a resposta a solicitações de órgãos internos e outras entidades

externas (PJ, PSP, Tribunais, entre outros). Com o intuito de dar resposta a solicitações de órgãos internos, designadamente, CO/DIC/RAIC, foram elaborados 11 pedidos de pesquisa. Por outro lado, quanto às solicitações dos órgãos internos do restante dispositivo da estrutura de IC, foram elaborados 36 pedidos de pesquisa. Ainda na vertente da informação criminal, foram realizados diversos relatórios temáticos de Análise relativos à criminalidade itinerante, ao furto de veículos de mercadoria, ao furto/roubo de veículos de transporte e distribuição de Tabaco, entre outros (GNR, 2017b).

A utilização das TIC, ao nível da Criminalística, espelhou um total de 1.660 exames e perícias, o que representa um aumento de 77,5% relativamente a 2015 (GNR, 2017b).

Ao longo de 2016, a GNR prosseguiu o reforço do desenvolvimento sistémico das novas TIC, com o intuito de qualificar o seu produto operacional. Para tal, de forma a permitir que, cada vez mais, haja um fluxo de informação eficaz e dinâmico, foi procurado seguir um padrão de interoperabilidade entre sistemas, nas medidas adotadas. Para além disso, foi mantido o esforço em garantir a continuidade de programas específicos de policiamento e prevenção, na sua variante tecnológica, o alargamento do Sistema AFIS e a manutenção do sítio da GNR (GNR, 2017b).

Relativamente ao ano de 2017, o Relatório de Atividades destacou, à semelhança de 2016, as seguintes plataformas de apoio à decisão e de natureza estratégica: o STM e o SIIOP com os seus múltiplos módulos: principal (P), salas de situação (2S), ocorrências (O), trânsito (T), ambiente (A), documental (D) e, também, georreferenciação (G) e o sítio da GNR na *internet* (GNR, 2018e).

No que diz respeito ao suporte dos diversos sistemas TIC verificou-se, no ano em análise, uma continuação do esforço efetuado relativamente à extensão da cobertura digital a toda a Guarda e concomitantemente aos Sistemas de Informação e Comunicação (GNR, 2018e).

Durante o ano de 2017, foram realizadas 1722 ordens de pesquisa e pedidos de pesquisa, materializando um acréscimo de cerca de 186% em relação a 2016. Numa índole mais específica, foram elaborados 17 apoios operacionais no domínio da Análise de Informação Criminal aos inquéritos que se desenvolvem nos termos da estrutura de IC das Unidades da GNR tendo sido, para o efeito, produzidos 13 Relatórios de Análise de Informação Criminal - Operacional (RAICO) (GNR, 2018e).

Quanto aos exames e perícias realizados pela GNR, é possível concluir que, foi realizado um número considerável de diligências de criminalística. No âmbito da lofoscopia, foram recolhidas 1.591 (NIC e NAT) resenhas datiloscópicas e foram realizados 13.512

exames e perícias de criminalística, o que conduziu à elaboração de 110 relatórios de extração de fotogramas (decréscimo de 49,6% face a 2016). Relativamente às TIC, foram efetuadas 1.586 pesquisas de dados informáticos[111], em dispositivos tecnológicos, o que representa um decréscimo de 4,5% em relação a 2016 (GNR, 2018e).

A fim da construir uma realidade de modernização cada vez mais presente, foram desenvolvidas diversas medidas neste âmbito, entre as quais: a criação de uma unidade OSINT, integrada no Centro de Informações da Guarda (CIG) sendo que, para tal, efetuou-se um procedimento e aquisição do *software* OSINT, com uma taxa de conclusão desta medida de 35%; instalação de equipamentos e substituição de sistemas convencionais por terminais VOIP (implementado 50%); melhoria dos mecanismos de *Governance*, redução de custos e implementação de soluções TIC mediante a elaboração de proposta de procedimento para aquisição de terminais (conclusão de 10%); avaliação de necessidades no que diz respeito ao Sistema de Telepresença da GNR; melhoria dos mecanismos de comando e controlo operacional através da avaliação de necessidades no âmbito do CiberGNR; estruturação de especificações técnicas e funcionais no domínio do Patrulhamento Móvel Digital (PMDGNR), do SEG2APIC, da Plataforma de Integração e Gestão Operacional (PIGO) e, por fim, para a modernização do SIIOP – MODERSIIOP (com uma percentagem de 20% de conclusão) (GNR, 2018e).

Em relação ao ano de 2018, o Relatório de Atividades destacou, à semelhança de 2017, as seguintes plataformas de apoio à decisão e de natureza estratégica: o STM e o SIIOP com os seus múltiplos submódulos: principal (P), salas de situação (2S), ocorrências (O), trânsito (T), ambiente (A), documental (D) e, também, georreferenciação (G) e, ainda, o sítio da GNR na *internet* (GNR, 2019b).

Ao nível das comunicações em videoconferência, através da utilização de dispositivos profissionais de videoconferência, em todas as Unidades e Comandos da GNR, foi possível uma diminuição significativa dos encargos com comunicações (GNR, 2019b).

Quanto às ordens e/ou pedidos de pesquisa realizados no âmbito da IC, foram elaboradas 1451 ordens de pesquisa e pedidos de pesquisa, o que reflete um decréscimo de cerca de 15,7% em relação a 2017. Ainda neste domínio, mas dirigido à vertente da Análise de Informação Criminal, foram efetuados 4 apoios operacionais aos inquéritos que se

[111] De acordo com a al. b) do art.º 2.º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), dados informáticos são "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".

desenvolvem na estrutura de IC das múltiplas Unidades da Guarda, tendo para o efeito sido realizados 11 RAICO (GNR, 2019b).

Durante o ano de 2018, foram realizadas diversas diligências da vertente de Criminalística, relacionadas com exames e perícias, entre as quais: elaboração de 56 relatórios de extração de fotogramas, o que representa uma diminuição de 49,1% em relação a 2017; realização, no âmbito da lofoscopia, de 427 exames laboratoriais lofoscópicos, assinalando-se um crescimento de 13,3% face a 2017 e, não só mas também, realização de 1.909 perícias lofoscópicas (decréscimo de 3,5% em relação a 2017) (GNR, 2019b).

Por seu turno, ainda no âmbito das TIC, foram realizadas 2.089 pesquisas de dados informáticos em dispositivos tecnológicos, traduzindo um crescimento de 31,7% quando comparado com 2017. Foram ainda concretizadas 6 pesquisas de dados informáticos, em resultado da emissão de Mandados Judiciais, na sequência da realização de operações (GNR, 2019b).

As medidas preconizadas para 2018, no que respeita à modernização administrativa, permitiram a continuidade do reforço e desenvolvimento de diversos projetos estabelecidos anteriormente, nomeadamente, a materialização do procedimento para aquisição do *software* OSINT, com o intuito de permitir a monitorização, acompanhamento, análise e difusão de informações policiais e criminais, tendo sido concluído 100% desta medida; substituição de sistemas convencionais por terminais VOIP, a fim de alcançar uma redução de custos e implementação de soluções TIC (concretização de 53% desta medida); renovação de equipamentos no âmbito do Sistema de Telepresença (92% concluído); realização de especificações técnicas e funcionais no domínio do Patrulhamento Móvel Digital – PMDGNR (10% concluído), do SEG2APIC (40% concluído), da PIGO (55% concluído) e, por fim, no que concerne à modernização do SIIOP – MODERSIIOP, com o intuito de reforçar os mecanismos de comando e controlo operacional, bem como a racionalização de meios e operacionalização de soluções TIC (realização de 50% desta medida) (GNR, 2019b).

Mediante a análise dos Relatórios de Atividades da GNR referentes ao período 2015-2018, podemos concluir que, o recurso às TIC, pela estrutura de IC da GNR representa, progressivamente, uma exigência para uma intervenção operacional eficaz. A mobilidade e a evolução dos fenómenos criminais impõem, às forças de segurança, uma permanente adaptação e reorganização das suas capacidades a fim de estarem preparadas, em tempo útil, para dar resposta a estas exigências. Consequentemente, a GNR, através dos seus instrumentos de gestão, procura permanentemente adaptar os seus objetivos e medidas à

realidade criminal atual permitindo, desta forma, um alinhamento entre a capacidade de resposta e as exigências impostas pela evolução da criminalidade.

Por fim, podemos concluir que, através de um contínuo investimento e desenvolvimento das TIC, a IC da Guarda, tem vindo a ser estruturada em alicerces operacionais com capacidade de resposta mais eficaz, com custos mais reduzidos e com uma superior racionalização dos meios, através do recurso às TIC como meio ao serviço da intervenção operacional das Unidades Territoriais.

APÊNDICE H - ESTRATÉGIA TIC 2020: ESTRATÉGIA PARA A TRANSFORMAÇÃO DIGITAL NA ADMINISTRAÇÃO PÚBLICA - RESOLUÇÃO DO CONSELHO DE MINISTROS N.º 108/2017

Utilizando como ponto de partida a atual Administração Pública (AP), concluímos que o recurso às TIC representa uma constante, quer para o tratamento da informação e para a gestão documental, quer no que respeita à própria prestação de serviços à comunidade. As TIC têm vindo, cada vez mais, a tornar-se numa ferramenta crucial para a modernização administrativa, contribuindo para aumentar a eficiência, incorporar e disponibilizar serviços e, ainda, prever possíveis necessidades futuras[112] (Agência para a Modernização Administrativa [AMA], 2018).

Nesta conformidade, a primeira vez que as TI e os procedimentos administrativos se agregaram, apenas produziram efeitos ao nível da desmaterialização dos circuitos em formato papel, a automatizar certos procedimentos e, posteriormente, a simplificar a comunicação, mediante o recurso à *internet*. Em consequência da permanente evolução tecnológica, para além da produção de efeitos no tempo de resposta, tornando-a mais célere, assistimos a uma expansão do conceito TIC, nomeadamente ao nível da robótica e da inteligência artificial proporcionando, atualmente, alterações profundas, quer na forma como a AP se encontra organizada, como na estruturação dos serviços[113] (AMA, 2018).

Neste sentido, a AP, em 2011, criou o Grupo de Projeto para as Tecnologias de Informação e Comunicação, denominado por GPTIC, previsto na Resolução do Conselho de Ministros n.º 46/2011, de 14 de novembro. Consequentemente, e tal como previsto na alínea g) do art.º. 199.º da CRP, o Conselho de Ministros decidiu, entre outras medidas, aprovar as diretrizes estratégicas de racionalização e diminuição de custos com as TIC na AP, previstas no Plano Global Estratégico para a Racionalização e Redução de Custos com as TIC (PGETIC), exposto pelo GPTIC. Por sua vez, este Plano foi operacionalizado em 2012 (Resolução do Conselho de Ministros n.º 12/2012), através de 25 medidas de racionalização

[112] Cf. https://tic.gov.pt/documents/37177/108997/CTIC_TIC2020_Estrategia_TIC.pdf/e2ea3d32-82a8-ed18-0fbf-9d51dfc24acc, disponível em 22 de março de 2020, às 21h10m.
[113] Cf. https://tic.gov.pt/documents/37177/108997/CTIC_TIC2020_Estrategia_TIC.pdf/e2ea3d32-82a8-ed18-0fbf-9d51dfc24acc, disponível em 22 de março de 2020, às 21h27m.

das TIC que foram sinalizadas devido ao seu carácter transversal e ao respetivo impacto na AP[114] (Presidência do Conselho de Ministros [PCM], 2012).

Subsequentemente, em resultado da Resolução do Conselho de Ministros n.º 33/2016, de 3 de junho, foi constituído o Conselho para as Tecnologias de Informação e Comunicação na Administração Pública (CTIC). Este Conselho foi responsável pela elaboração da Estratégia TIC 2020, edificada em três eixos particulares — Integração e Interoperabilidade; Inovação e Competitividade e Partilha de Recursos. Nestes três pilares encontram-se previstas doze medidas a partir das quais são delineadas as atividades a desenvolver de forma transversal e distribuída pelos diversos setores do Governo (Presidência do Conselho de Ministros [PCM], 2017).

A Estratégia TIC 2020 apresenta como principal objetivo trabalhar no sentido da transformação digital da AP, procurando recorrer às TIC enquanto catalisador da modernização (PCM, 2017).

Nesta senda, a Estratégia TIC da AP tem como principais finalidades: simplificar os serviços digitais, tornando-os mais acessíveis e inclusivos; aumentar a utilização dos serviços digitais pelos cidadãos e pelas empresas e, ainda, garantir uma fomentação sustentável no domínio da transformação digital (PCM, 2017).

Analisando particularmente cada eixo definido, serão abordadas, no presente anexo (Quadro n.º 4), as principais medidas delineadas no âmbito da Administração Interna, mais concretamente, em relação às FSS, previstas no Anexo I da Resolução do Conselho de Ministros n.º 108/2017 (PCM, 2017).

Deste modo, por força do n.º 16 da Resolução do Conselho de Ministros n.º 33/2016, de 3 de junho, bem como da alínea g) do art.º 199.º da CRP, o Conselho de Ministros determinou, entre outras medidas, aprovar a Estratégia TIC 2020 e, também, o correspondente Plano de Ação, expostos pelo CTIC e, não só mas também, estabelecer que a Estratégia TIC 2020 apresenta como meta a sua conclusão em 31 de dezembro de 2020[115] (PCM, 2017)**.**

[114] Cf. Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro de 2012.
[115] Cf. Resolução do Conselho de Ministros n.º 108/2017, 26 de julho.

Quadro n.º 4 - Estratégia TIC 2020 da AP: Principais medidas para a modernização tecnológica da GNR

EIXO 1 **INTEGRAÇÃO E INTEROPERABILIDADE**	• **Arquitetura de referência** única com prioridade para a resiliência digital e **segurança** dos vários sistemas e dos dados; • **Interoperabilidade** entre as diversas entidades da AP;	***Medida 4:*** *Arquitetura de referência TIC* ➢ Estabelecer e concretizar **arquiteturas TIC transversais:** • Evolução e reforço do **Centro de Operações de Segurança Informática (COSI**) – (2017 a 2020); • Cimentar a coordenação no reconhecimento e resolução de ameaças e ataques informáticos: Articulação do **COSI**[116] com as FSS do Ministério da Administração Interna (MAI) - Produzir um canal que possibilite a interação e partilha de informação entre o COSI e as áreas interligadas à **segurança da informação da PSP e da GNR**, a fim de otimizar a resposta às diversas ameaças/ataques informáticos); ➢ **Rentabilizar os investimentos** em TIC; ➢ Estabelecer e concretizar uma **Estratégia Nacional de Segurança** da informação.
EIXO 2 **INOVAÇÃO E COMPETITIVIDADE**	• Reforço da acessibilidade dos serviços eletrónicos, aproximando e **reduzindo os custos**, assim como a cooperação dos cidadãos e das empresas, através de uma **superior partilha de recursos.**	***Medida 7:*** *Serviços eletrónicos* ➢ Instalar *roaming Wi-Fi* na AP—***GOVroam*:** • Efetuar o *upgrade* do modelo atual que assenta numa plataforma desatualizada. O sistema deverá ser capacitado de uma plataforma de monitorização e segurança que atualmente não abrange todas as FSS do MAI - **Sistema *WIFI* na RNSI**[117]; ➢ Converter o **arquivo físico** da AP em formato digital: • **MoniGNR** - Plataforma responsável pelo controlo, racionalização, otimização da eficiência e eficácia das competências administrativas e operacionais da GNR, permitindo a disseminação de dados ao cidadão através da Gestão da Experiência do Cidadão nos processos de atendimento – 2016 a 2020).

[116] Em 2012, foi criado o Centro de Operações de Segurança Informática (COSI), enquanto estrutura de resposta a incidentes de segurança informática efetivado pela equipa *Computer Security Incident Response Team* (CSIRT) do MAI. A partir desta estrutura é desenvolvido um esforço contínuo, com epicentro na prevenção, monitorização, controlo e reação, em matéria de segurança no ciberespaço, conforme https://www.csirt.rnsi.mai.gov.pt/, disponível em 5 de abril de 2020, às 12h36m.

[117] A Rede Nacional de Segurança Interna (RNSI) constitui uma rede de comunicações segura, alicerçada num sistema de partilha de serviços, cooperação e de gestão articulada e integrada, habilitada a suportar dados, voz e imagem, concedida às FSS e restantes entidades do MAI. Esta Rede foi concebida com a finalidade de uniformizar e otimizar as infraestruturas de comunicações de dados e fomentar, deste modo, a interoperabilidade entre todos os Organismos do MAI, com progresso na interação entre pessoas e aplicações, conforme https://www.sg.mai.gov.pt/Tecnologias/RNSI/Paginas/default.aspx, disponível em 5 de abril de 2020, às 16h19m.

EIXO 2 **INOVAÇÃO E COMPETITIVIDADE**	• Reforço da acessibilidade dos serviços eletrónicos, aproximando e **reduzindo os custos**, assim como a cooperação dos cidadãos e das empresas, através de uma **superior partilha de recursos.**	***Medida 8:*** *Inovação setorial (Projetos TIC de inovação nos Planos Setoriais TIC GNR)* ➢ Fomentar ações setoriais que garantam a **melhoria da qualidade** dos serviços concedidos e/ou **reforçar a eficiência** interna da AP mediante o **recurso às TIC**: • **Projeto de Atualização das Redes Rádio — PARR -** Projeto com o objetivo de **fomentar** as capacidades das **redes rádio** e vigilância florestal em desenvolvimento pela GNR, bem como a remodelação dos terminais e acessórios e, paralelamente, decrescer os custos associados ao suporte das infraestruturas das redes analógicas vigentes; • **Projeto de Atualização dos Terminais de Dados – PATR** (2016 a 2020) - Projeto que visa a manutenção permanente dos parques de terminais de processamento de dados da GNR, atendendo ao tempo de vida dos equipamentos, as respetivas exigências e os custos associados; • A fomentação das TIC, em conformidade com a sua normalização e convergência a nível tecnológico, disponibiliza aos **CTer da Guarda** e **Salas de Situação**, promotores da eficácia e melhoria da implementação de meios nas respetivas zonas de ação. As Estações de Trabalho controlam e mantêm atualizada a informação georreferenciada e classificada, a fim de disponibilizar nos sistemas de multimédia, uma imagem operacional aproximada à realidade e encurtar o Ciclo de Tomada de Decisão. A finalidade é **instalar 8 C3T (*Command, Control and Communications – Tactical*) até 2020** (projetos TIC de inovação setoriais nos Planos setoriais TIC GNR- **Sistema de Comando Controlo e Coordenação Operacional da Guarda - SC3OG -** de 2017 a 2020**)**; • Fornecer aos patrulheiros da GNR a capacidade de inserção e consulta de dados nos SI internos e externos, em qualquer local, **reduzindo o Ciclo de Produção de Informação** da GNR; (**Patrulhamento Móvel Digital —PMDGNR**: 2016 a 2020); • Modernização a nível tecnológico de processos e capacidades do **SIIOP**, reforçando a sua fomentação e interoperabilidade com sistemas, quer internos, como externos das FSS, como por exemplo a PIIC e o SIS II e outros no domínio policial e criminal, capacitando o processamento e transação da informação de múltiplos SI internos e externos à Guarda, com capacidade para "***Data Warehousing***", "***Business Intelligence***" e procedimentos compostos de "***Reporting***" e "***Dashboarding***" Policial (**Modernização do SIIOP— Moder-SIIOP -** 2016 a 2020);

EIXO 2 **INOVAÇÃO E COMPETITIVIDADE**	• Reforço da acessibilidade dos serviços eletrónicos, aproximando e **reduzindo os custos**, assim como a cooperação dos cidadãos e das empresas, através de uma **superior partilha de recursos.**	• Fomentação de capacidades em **Cibersegurança** para prevenção e repressão de condutas criminais provenientes do ciberespaço ou que colocam em risco a segurança da Informação das infraestruturas críticas nacionais, realizando alerta e disseminação ao MAI e ao cidadão (**CiberGNR -** 2016 a 2020).
EIXO 3 **PARTILHA DE RECURSOS**	• Otimização das capacidades TIC da AP, mediante **ações de formação;** • Fomentação de uma rede de comunicações multisserviços segura que permita **eliminar redundâncias desnecessárias**;	***Medida 10:*** *Centros de dados na nuvem* ➢ Otimizar e centralizar a capacidade de computação nos centros de **processamento de dados**; ➢ Conceber uma **nuvem interoperável**: • Clonagem dos Sistemas Core das FSS no *Disaster Recovey* (DC)/*Business Continuity* do MAI, em Contumil. Deste modo, as FSS, nomeadamente a **GNR (SIIOP)** deverá ter o seu *core* replicado no DC da RNSI ***Medida 11:*** *Comunicações na Administração Pública* ➢ Racionalizar **comunicações de voz e dados**; ➢ Desenvolver uma **Rede comum de comunicações** multisserviços: • Materialização de infraestruturas de rede que preencham as necessidades de ligação à RNSI das Unidades da GNR, a fim de preencher a cobertura digital da GNR e o apoio, em termos tecnológicos, à modernização administrativa estabelecida pelo MAI, enfatizando o suporte ao SIIOP/GNR - Incorporar e cablar os PTer da GNR sem ligação à RNSI e outras remodelações de redes locais — **RCPNLR3L -** 2016 a 2020; • Estruturação de um canal multisserviços nas ligações à RNSI a, aproximadamente, seis centenas de *sites* da GNR, permitindo a conexão sem custos de serviços de voz e videoconferência sobre IP, continuando a incorporação da GNR no Plano de Numeração do MAI e a interoperabilidade entre as diversas entidades sob tutela do MAI. A instalação de acessos tipo **VOIP SIPTRUNK**, possibilita a anulação das diversas assinaturas mensais, convergindo-as – Centralização dos acessos das comunicações de voz às redes públicas - 2016 a 2020;

EIXO 3 **PARTILHA DE RECURSOS**	• Otimização das capacidades TIC da AP, mediante **ações de formação;** • Fomentação de uma rede de comunicações multisserviços segura que permita **eliminar redundâncias desnecessárias**;	• Uma vez que a estrutura da GNR integra uma dispersão elevada, alicerçada numa orgânica hierárquica que assenta, territorialmente, em vinte CTer ligados às divisões administrativas dos dezoito distritos do país e dois arquipélagos, isto é, os Açores e a Madeira, comprovando a necessidade de recurso a tecnologias de comunicação audiovisual que estimulem uma poupança acrescida nas ações de Comando, Coordenação, Instrução, Formação e outras, atualmente providas de terminais HD (*High Definition*) de videoconferência - **Sistema de Telepresença da GNR -** 2016 a 2020. ➢ Delinear e implementar estratégias de comunicações unificadas. ***Medida 12:*** *Aplicações comuns e em código aberto* ➢ Desenvolver e difundir o ***software* de código aberto (OSS)**: • Estação de trabalho padrão operativa da GNR — Através deste projeto, a GNR procura criar uma Estação de Trabalho normalizada, utilizando exclusivamente soluções alicerçadas em normas abertas (*Open-Source*) - **Projeto ETPOG -** 2016 a 2020.

Fonte: Elaboração própria, com base em (PCM, 2017)

APÊNDICE I – DESENHO DE INVESTIGAÇÃO

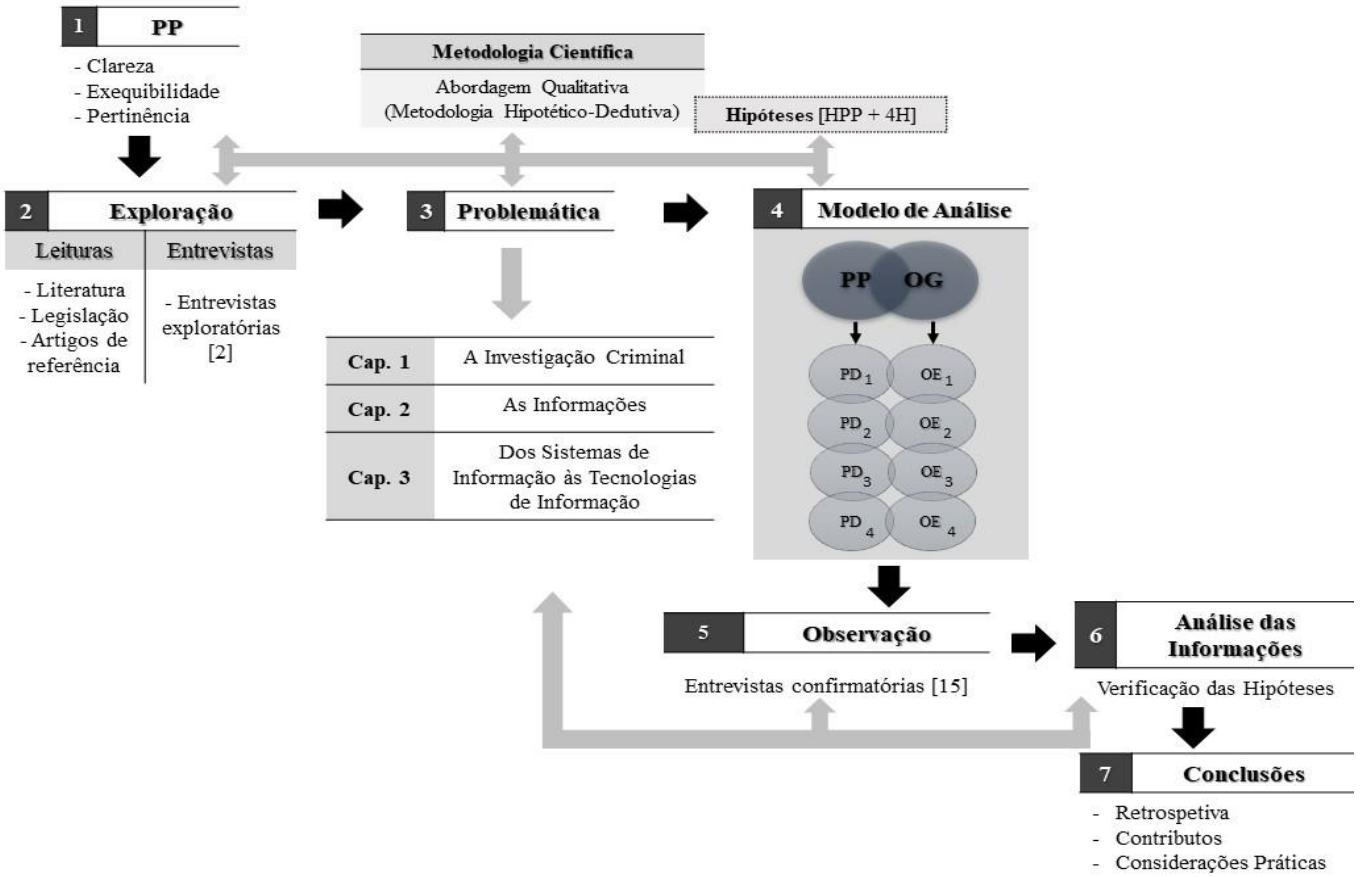


Figura n.º 5 - Desenho de investigação

Fonte: Elaboração própria, com base em (Quivy & Campenhoudt, 2017)

APÊNDICE J – MODELO DE ANÁLISE

Quadro n.º 5 - Modelo de análise da investigação

<table>
<tr><td>TEMA</td><td colspan="6">“As Tecnologias de Informação na estrutura de Investigação Criminal das Unidades Territoriais da Guarda Nacional Republicana Territorial”</td></tr>
<tr><td>Objetivo Geral</td><td colspan="6">“Analisar os principais contributos da utilização das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da GNR.”</td></tr>
<tr><td>Pergunta de Partida</td><td colspan="6">“Quais os principais contributos das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da GNR?”</td></tr>
<tr><td>Perguntas Derivadas</td><td>HPP</td><td>Objetivos Específicos</td><td colspan="2">Tratamento e Análise dos Dados
Categorias</td><td>Revisão da Literatura</td><td>Técnicas de Recolha de dados</td></tr>
<tr><td>PD1: Qual a função das Informações Criminais na resposta aos fenómenos criminais?</td><td>H1</td><td>OE1: Descrever a função das Informações Criminais na resposta aos fenómenos criminais.</td><td colspan="2">Contributos das Informações na IC
Utilização das Informações Criminais</td><td rowspan="4">Capítulo 1
A Investigação Criminal

Capítulo 2
As Informações

Capítulo 3
Dos Sistemas de Informação às Tecnologias de Informação</td><td rowspan="4">- Pesquisa Documental
e
Pesquisa Bibliográfica

- Entrevistas Exploratórias
e
Entrevistas Confirmatórias</td></tr>
<tr><td>PD2: Quais as principais Tecnologias e Sistemas de Informação utilizados pelas Unidades Territoriais da GNR na vertente de Investigação Criminal?</td><td>H2</td><td>OE2: Caracterizar as principais Tecnologias e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades Territoriais da GNR.</td><td>TI na estrutura de IC da GNR</td><td>SI na estrutura de IC da GNR</td></tr>
<tr><td>PD3: Quais as vantagens e desvantagens decorrentes do funcionamento e utilização dos Sistemas e Tecnologias de Informação pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?</td><td>H3</td><td>OE3: Identificar os pontos fortes e as debilidades subjacentes à estrutura e funcionamento dos Sistemas e Tecnologias de Informação na estrutura de Investigação Criminal das Unidades Territoriais da GNR.</td><td colspan="2">Potencialidades da utilização dos Sistemas e TI na IC
Aptidão das TI, utilizadas pelas SIIC, na resposta às exigências criminais
Debilidades da utilização e funcionamento dos Sistemas e TI</td></tr>
<tr><td>PD4: Quais as melhorias a implementar nos Sistemas e Tecnologias de Informação, por forma a reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?</td><td>H4</td><td>OE4: Identificar as melhorias a implementar nos Sistemas e Tecnologias de Informação para reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR.</td><td colspan="2">Debilidades da estrutura de IC das Unidades Territoriais da GNR
Adequabilidade dos objetivos e medidas da Estratégia e Planos de Atividades da GNR
Melhorias a implementar nos Sistemas e TI</td></tr>
</table>

Fonte: Elaboração própria, com base em (Quivy & Campenhoudt, 2017)

APÊNDICE K – RELAÇÃO ENTRE PERGUNTAS DE INVESTIGAÇÃO E QUESTÕES DAS ENTREVISTAS CONFIRMATÓRIAS

Quadro n.º 6 - Relação entre perguntas de investigação e questões das entrevistas confirmatórias

PERGUNTA DE PARTIDA		
	"Quais os principais contributos das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da GNR?"	
	Perguntas Derivadas	**Questões das Entrevistas Confirmatórias**
	PD1: Qual a função das Informações Criminais na resposta aos fenómenos criminais?	**2.** Nesta senda, considera importante o contributo das informações policiais e das informações criminais para este objetivo? Por que razão? **3.** De que modo são utilizadas as informações criminais pelas estruturas de Investigação Criminal das Unidades Territoriais, na resposta aos fenómenos criminais?
	PD2: Quais as principais Tecnologias e Sistemas de Informação utilizados pelas Unidades Territoriais da GNR na vertente de Investigação Criminal?	**4.** Face ao exposto, quais as Tecnologias de Informação e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades Territoriais da GNR? Utilize como referência as vertentes funcionais da Investigação Criminal (IC - Operativa; IC - Criminalística e IC - Análise de Informação Criminal).
	PD3: Quais as vantagens e desvantagens decorrentes do funcionamento e utilização dos Sistemas e Tecnologias de Informação pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?	**5.** Atendendo às Tecnologias e Sistemas de Informação anteriormente enumerados, quais são as potencialidades decorrentes da sua utilização pela estrutura de Investigação Criminal das Unidades Territoriais da GNR? **6.** Considera estas suficientes para um desempenho eficaz na análise, prevenção e combate dos fenómenos criminais? Por que razão? **7.** Analisando as principais Tecnologias e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades da GNR, mencione as principais debilidades decorrentes do funcionamento e utilização dos mesmos.
	PD4: Quais as melhorias a implementar nos Sistemas e Tecnologias de Informação, por forma a reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?	**1.** Considera que a Investigação Criminal das Unidades Territoriais da GNR apresenta debilidades na sua capacidade de resposta às exigências criminais atuais? Em caso de resposta afirmativa, quais os principais problemas/limitações a destacar, quer ao nível da estrutura, caso existam, quer ao nível da sua intervenção operacional? **8.** Atendendo à Estratégia da Guarda 2020, referente ao período entre 2015 e 2020, bem como os Planos de Atividades elaborados desde 2015 até à atualidade, considera que os objetivos e medidas definidos no domínio das Tecnologias de Informação dão resposta às necessidades operacionais da estrutura de Investigação Criminal das Unidades Territoriais? Por que razão? **9.** Quais são, na sua opinião, as melhorias a implementar no domínio dos Sistemas e Tecnologias de Informação, de modo a reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?

Fonte: Elaboração própria, com base em (Quivy & Campenhoudt, 2017)

APÊNDICE L – PROCEDIMENTO CIENTÍFICO: DA PERGUNTA DE PARTIDA ÀS HIPÓTESES DE INVESTIGAÇÃO

Quadro n.º 7 – Da pergunta de partida às hipóteses de investigação

PERGUNTA DE PARTIDA

"Quais os principais contributos das Tecnologias de Informação para o incremento da eficácia operacional dos órgãos da estrutura de Investigação Criminal das Unidades Territoriais da GNR?"

Questões de Entrevistas Exploratórias	Revisão da Literatura	Perguntas Derivadas	Hipóteses de Investigação
2. Como são utilizadas as Informações pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?	**Capítulo 1** A Investigação Criminal	**PD1:** Qual a função das Informações Criminais na resposta aos fenómenos criminais?	**H1**
3. Quais as Tecnologias e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?		**PD2:** Quais as principais Tecnologias e Sistemas de Informação utilizados pelas Unidades Territoriais da GNR na vertente de Investigação Criminal?	**H2**
4. Enumere as principais vantagens e desvantagens resultantes da utilização dos Sistemas e Tecnologias de Informação pela estrutura de Investigação Criminal das Unidades Territoriais da GNR.	**Capítulo 2** As Informações	**PD3:** Quais as vantagens e desvantagens decorrentes do funcionamento e utilização dos Sistemas e Tecnologias de Informação pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?	**H3**
1. Quais as limitações da estrutura de Investigação Criminal das Unidades Territoriais da GNR? **5.** Quais as melhorias que consideraria necessárias implementar no âmbito dos Sistemas e Tecnologias de Informação, a fim de reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?	**Capítulo 3** Dos Sistemas de Informação às Tecnologias de Informação	**PD4:** Quais as melhorias a implementar nos Sistemas e Tecnologias de Informação, por forma a reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?	**H4**
EXPLORAÇÃO	**PROBLEMÁTICA**	**MODELO DE ANÁLISE**	

Hipótese da Pergunta de Partida

Fonte: Elaboração própria, com base em (Quivy & Campenhoudt, 2017)

APÊNDICE M – CARTA DE APRESENTAÇÃO

ACADEMIA MILITAR

AS TECNOLOGIAS DE INFORMAÇÃO NA ESTRUTURA DE INVESTIGAÇÃO CRIMINAL DAS UNIDADES TERRITORIAIS DA GUARDA NACIONAL REPUBLICANA

Autor: Aspirante de Infantaria da GNR Amílcar da Cunha Pereira

Orientador: Tenente-Coronel de Infantaria da GNR António Duarte Rodrigues Lobo de Carvalho

Coorientador: Capitão de Administração da GNR Luís Carlos Rodrigues Malheiro

Mestrado Integrado em Ciências Militares, na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, março de 2020

CARTA DE APRESENTAÇÃO

O presente estudo, subordinado ao tema "As Tecnologias de Informação na estrutura de Investigação Criminal das Unidades Territoriais da Guarda Nacional Republicana", emerge no domínio da elaboração do Relatório Científico Final do Trabalho de Investigação Aplicada, da Academia Militar, tendo como finalidade a obtenção do grau académico de Mestre em Ciências Militares, na especialidade de Segurança.

Neste sentido, a presente investigação tem como objetivo analisar os contributos operacionais decorrentes da utilização das Tecnologias de Informação (TI) pela estrutura de Investigação Criminal (IC) das Unidades Territoriais da Guarda Nacional Republicana (GNR). Perante a crescente complexidade e evolução dos fenómenos criminais, torna-se vinculativo privilegiar o incentivo para a utilização das TI, não só enquanto ferramenta imprescindível para a capacidade de resposta e tomada de decisão, como também, enquanto princípio ativo da eficácia operacional. Por conseguinte, pretende-se identificar e caracterizar as diferentes TI utilizadas no domínio da IC da GNR, bem como as vantagens e respetivas debilidades, decorrentes do recurso às mesmas.

Por consequência, identifica-se a necessidade de concretizar diversas entrevistas, com a finalidade de recolher informações neste âmbito. Neste sentido, as entrevistas devem ser dirigidas a entidades que, em consequência da sua experiência profissional e/ou do atual desempenho de funções neste campo, possuam conhecimentos específicos, quer no domínio da IC como, também, no desenvolvimento e utilização das TI ao nível das Unidades Territoriais da GNR.

Pelo que antecede, venho por este meio solicitar a Vossa Excelência que me conceda uma entrevista referente ao tema em análise, na medida em que o seu contributo é fundamental para a concretização dos objetivos delineados na presente investigação.

Grato pela sua disponibilidade e colaboração.

Atenciosamente,

Amílcar da Cunha Pereira

Aspirante de Infantaria da GNR

APÊNDICE N – GUIÃO DAS ENTREVISTAS EXPLORATÓRIAS

1. Identificação do Entrevistado

Nome	
Posto	
Idade	
Habilitações Literárias	
Função	
Local	
Distrito	
Data	
Hora de Início/Fim	

2. Entrevista

As suas respostas às questões apresentadas na seguinte entrevista são essenciais para a concretização dos objetivos delineados na presente investigação. Deste modo, é fundamental que a resposta a cada questão seja o mais completa e pormenorizada possível, tendo em conta a sua experiência e conhecimento profissional. Uma vez que a totalidade das respostas apenas serão utilizadas como objeto de estudo desta investigação, é-lhe solicitada autorização para realizar a sua gravação, a fim de proceder à sua posterior transcrição.

Caso pretenda, previamente à integração e análise das respostas na presente investigação, as mesmas ser-lhe-ão expostas, de modo a garantir a possibilidade de retificar algum aspeto que seja do seu interesse.

1. Quais as limitações da estrutura de Investigação Criminal das Unidades Territoriais da GNR?
2. Como são utilizadas as Informações pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?
3. Quais as Tecnologias e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?
4. Enumere as principais vantagens e desvantagens resultantes da utilização dos Sistemas e Tecnologias de Informação pela estrutura de Investigação Criminal das Unidades Territoriais da GNR.

5. Quais as melhorias que consideraria necessárias implementar no âmbito dos Sistemas e Tecnologias de Informação, a fim de reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?

APÊNDICE O – GUIÃO DAS ENTREVISTAS CONFIRMATÓRIAS

1. Identificação do Entrevistado

Nome	
Posto	
Idade	
Habilitações Literárias	
Função	
Local	
Distrito	
Data	
Hora de Início/Fim	

2. Enquadramento

A evolução da ciência e da tecnologia tem vindo a gerar, ao longo dos últimos dois séculos, uma "sociedade intensiva de conhecimento" (Castells, 2004, p. 14). Mediante um quadro social que, cada vez mais, prioriza o acesso e a utilização da informação, verificamos que o desenvolvimento de infraestruturas capacitadas para a sua recolha, armazenamento e processamento tornam-se, progressivamente, uma parcela significativa do esforço de uma organização na prossecução da sua atividade (Gouveia & Ranito, 2004).

Neste sentido, partindo da premissa de que, a utilização das Tecnologias de Informação não representam um fim em si mesmo, mas um meio, importa sublinhar que estas desempenham um papel vinculativo na fomentação da eficácia, eficiência e sustentabilidade das atividades organizacionais (Carvalho, 2010).

Por conseguinte, analisando a atual conjuntura, qualquer organização moderna privilegia o recurso às Tecnologias de Informação e Comunicação (TIC) como meio de reforço da função dos Sistemas de Informação enquanto pilar ao fluxo de informação (Gouveia & Ranito, 2004). A informação, uma vez sujeita ao seu tratamento sistemático mediante o recurso a sistemas centralizados que potenciem todo o processo desde a compilação à sua difusão, converte-se em conhecimento da criminalidade (Braz, 2020). Deste modo, o desenvolvimento das tecnologias assume um papel imprescindível no apoio à investigação criminal (Braz, 2016).

A utilização das novas TI pelas estruturas de investigação criminal das Forças e Serviços de Segurança, nomeadamente da GNR, permite a simplificação, celeridade e desburocratização

da atividade operacional, garantindo um vasto leque de soluções, quer a nível tático, como a nível estratégico (Guarda Nacional Republicana [GNR], 2014e). Partindo da coordenação, cruzamento e partilha de informação entre diferentes Sistemas de Informação até ao aumento da capacidade de tratamento e análise da informação, apoio ao planeamento e referenciação das tendências e padrões criminais emergentes, as Tecnologias de Informação e, consequentemente, os Sistemas de Informação, representam importantes instrumentos de coordenação e eficácia operacional no âmbito da prevenção e combate à criminalidade (Braz, 2020).

Desta forma, o presente estudo tem como objetivo analisar os contributos operacionais da utilização das Tecnologias de Informação pela estrutura de Investigação Criminal das Unidades Territoriais da GNR, a fim de compreender as vantagens e debilidades resultantes da sua utilização, bem como as melhorias a implementar neste domínio. Por consequência, é fundamental o contributo, na presente investigação, de entidades com experiência e competência, quer ao nível das Tecnologias de Informação, como ao nível da Investigação Criminal, nomeadamente, entidades das Secções de Informações e de Investigação Criminal dos Comandos Territoriais e, também, da Direção de Informações, Direção de Investigação Criminal e Direção de Comunicações e Sistemas de Informação, do Comando Operacional.

O guião da entrevista seguidamente apresentado, engloba diversas matérias, entre as quais, o papel das informações; as informações policiais e as informações criminais; a utilização das informações no combate e prevenção criminais; a estrutura de Investigação Criminal ao nível das Unidades Territoriais da GNR; o recurso às Tecnologias de Informação para a produção, tratamento e análise de informações e, não só mas também, as melhorias a implementar no âmbito das Tecnologias de Informação, por forma a garantir uma superior eficácia operacional ao nível da estrutura de Investigação Criminal.

3. Bibliografia

Braz, J. (2016). *Ciência, Tecnologia e Investigação Criminal: Interdependências e Limites num Estado de Direito Democrático*. Coimbra: Almedina.

Braz, J. (2020). *Investigação Criminal: A Organização, O Método e A Prova: Os Desafios da Nova Criminalidade* (5ª edição). Coimbra: Almedina.

Carvalho, J. Á. (2010). Tecnologias e Sistemas de Informação: uma área científica orientada às necessidades de conhecimento dos profissionais envolvidos na contínua transformação das organizações através das tecnologias da informação. *Encontros Bibli: Revista*

Eletrónica de Biblioteconomia e Ciência Da Informação, 1–25. doi:10.5007/1518-2924.2010v15nesp2p1.

Castells, M. (2004). *The network society: a cross-cultural perspective.* Massachusetts: Edward Elgar Publishing.

Gouveia, L. & Ranito, J. (2004). *Sistemas de Informação de Apoio à Gestão.* Porto: Principia, Publicações Universitárias e Científicas.

Guarda Nacional Republicana [GNR] (2014e). Estratégia da Guarda 2020: Uma Estratégia de Futuro. In *Sítio da Guarda Nacional Republicana.* Acedido a 6 de fevereiro de 2020 em *https://www.gnr.pt/estrategia.aspx*

4. Entrevista

As suas respostas às questões apresentadas na seguinte entrevista são essenciais para a concretização dos objetivos delineados na presente investigação. Deste modo, é fundamental que a resposta a cada questão seja o mais completa e pormenorizada possível, tendo em conta a sua experiência e conhecimento profissional. Uma vez que a totalidade das respostas apenas serão utilizadas como objeto de estudo desta investigação, é-lhe solicitada autorização para realizar a respetiva gravação, com o intuito de proceder à sua posterior transcrição.

Caso pretenda, previamente à integração e análise das respostas na presente investigação, as mesmas ser-lhe-ão expostas, de modo a garantir a possibilidade de retificar algum aspeto que seja do seu interesse.

1. A Investigação Criminal, tal como definido no artigo 1.º da Lei de Organização da Investigação Criminal (LOIC), constitui "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, p. 6038). Porém, a evolução da realidade criminal exige um acompanhamento da mesma por parte das Forças e Serviços de Segurança.

   Considera que a Investigação Criminal das Unidades Territoriais da GNR apresenta debilidades na sua capacidade de resposta às exigências criminais atuais? Em caso de resposta afirmativa, quais os principais problemas/limitações a destacar, quer ao nível da estrutura, caso existam, quer ao nível da sua intervenção operacional?

2. A informação materializa um dos bens mais valiosos de uma organização, sendo que a sua fiabilidade, qualidade e segurança são essenciais para o apoio à capacidade de tomada de decisão. Neste sentido, as informações desempenham um papel preponderante no combate e/ou prevenção da prática de crimes, o que nos conduz à distinção entre, pelo menos, dois tipos de informações.

   Nesta senda, considera importante o contributo das informações policiais e das informações criminais para este objetivo? Por que razão?
3. De que modo são utilizadas as informações criminais pelas estruturas de Investigação Criminal das Unidades Territoriais, na resposta aos fenómenos criminais?
4. A evolução dos fenómenos criminais, bem como dos diferentes *modus operandi* emergentes exigem, cada vez mais, uma resposta mais célere e eficaz por parte dos órgãos de investigação criminal. Por este motivo, tem se vindo a privilegiar o recurso às novas tecnologias no apoio progressivo à atividade operacional, bem como nas ações de controlo e supervisão.

   Face ao exposto, quais as Tecnologias de Informação e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades Territoriais da GNR? Utilize como referência as vertentes funcionais da Investigação Criminal (IC - Operativa; IC - Criminalística e IC - Análise de Informação Criminal).
5. Atendendo aos Sistemas e Tecnologias de Informação anteriormente enumerados, quais são as potencialidades decorrentes da sua utilização pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?
6. Considera estas suficientes para um desempenho eficaz na análise, prevenção e combate dos fenómenos criminais? Por que razão?
7. Analisando as principais Tecnologias e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades da GNR, mencione as principais debilidades decorrentes do funcionamento e utilização dos mesmos. Complete a sua resposta com exemplos práticos subjacentes à realidade operacional de cada vertente funcional da Investigação Criminal.
8. Atendendo à Estratégia da Guarda 2020, referente ao período entre 2015 e 2020, bem como os Planos de Atividades elaborados desde 2015 até à atualidade, considera que os objetivos e medidas definidos no domínio das Tecnologias de Informação dão resposta às necessidades operacionais da estrutura de Investigação Criminal das Unidades Territoriais? Por que razão?

9. Quais são, na sua opinião, as melhorias a implementar no domínio dos Sistemas e Tecnologias de Informação, de modo a reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?

APÊNDICE P – CARACTERIZAÇÃO DOS ENTREVISTADOS

Quadro n.º 8 - Caracterização dos entrevistados

	N.º	Nome	Posto	Idade	Função	Localidade	Habilitações	Data
Entrevistas Exploratórias	**EA**	Tiago Lourenço Lopes	Major	41 anos	Ex-Chefe da Repartição de Análise Digital Forense	Lisboa	Mestrado	4/03/2020
	EB	Hugo Miguel Grave Carneiro	Major	37 anos	Chefe da Repartição de Sistemas Operacionais	Lisboa	Licenciatura	6/03/2020
Entrevistas Confirmatórias	**E1**	Adriano Ferreira da Rocha	Major	43 anos	Chefe de SIIC	Porto	Mestrado	21/03/2020
	E2	João Firmino Nortadas	Tenente-Coronel	53 anos	Diretor da Direção de Investigação Criminal	Lisboa	Licenciatura	23/03/2020
	E3	Joni Helder Gouveia Seabra Ferreira	Capitão	36 anos	Chefe de SIIC	Vila Real	Licenciatura	24/03/2020
	E4	Fernando Miguel Magano Martins	Major	40 anos	Chefe de SIIC	Braga	Doutoramento	25/03/2020
	E5	Carlos Manuel Gonçalves Fernandes	Major	36 anos	Chefe de SIIC	Viana do Castelo	Mestrado	26/03/2020
	E6	Diogo Almeida e Brito Moreira Dores	Tenente-Coronel	43 anos	Chefe da Divisão de Criminalística	Lisboa	Mestrado	30/03/2020
	E7	João Carlos do Nascimento Nunes	Tenente-Coronel	53 anos	Chefe da Divisão de Sistemas de Informação	Lisboa	Mestrado	31/03/2020
	E8	José Manuel Cascalho Moisés	Coronel	48 anos	Diretor da Direção de Informações	Lisboa	Mestrado	2/04/2020
	E9	Nuno Alexandre Cortez Gonçalves Santos	Major	41 anos	Chefe de SIIC	Beja	Licenciatura	21/04/2020

	N.º	Nome	Posto	Idade	Função	Localidade	Habilitações	Data
Entrevistas Confirmatórias	**E10**	Nuno Tiago Pinto Taveira	Capitão	31 anos	Adjunto do Chefe de SIIC	Setúbal	Mestrado	24/04/2020
	E11	José Carlos da Costa Guilherme	Coronel	54 anos	Diretor da Direção de Comunicações e Sistemas de Informação	Lisboa	Licenciatura	24/04/2020
	E12	Carlos Manuel Neves Bengala	Major	41 anos	Chefe de SIIC	Faro	Licenciatura	26/04/2020
	E13	Jorge António de Jesus Soares da Cunha dos Santos Cardoso	Major	43 anos	Chefe da Repartição de Análise de Informação Criminal	Lisboa	Licenciatura	27/04/2020
	E14	João Paulo Gonçalves dos Santos	Major	44 anos	Chefe de SIIC	Leiria	Mestrado	28/04/2020
	E15	Filipe André Correia Paulino	Capitão	32 anos	Chefe de SIIC	Lisboa	Mestrado	04/05/2020

Fonte: Elaboração própria, com base nas entrevistas exploratórias e confirmatórias

APÊNDICE Q – ANÁLISE DE CONTEÚDO DAS ENTREVISTAS EXPLORATÓRIAS

Quadro n.º 9 - Análise de conteúdo das entrevistas exploratórias – Entrevistado A

N.º	Argumentação
EA	**1. Quais as limitações da estrutura de Investigação Criminal das Unidades Territoriais da GNR?**
	- "As debilidades da Investigação Criminal existentes nas Unidades Territoriais da GNR têm origem nas opções estratégicas da própria organização, (…). Considero que o atual conceito das vertentes funcionais da Investigação Criminal (modelo clássico que não evoluiu) estão desajustadas à realidade funcional e quantidade de prova, que é necessária manusear para os dias de hoje, na medida em que a GNR não tem capacidade total instalada em algumas das áreas, pois faz apenas "meio trabalho de policia", ficando assim dependente de terceiras entidades (quer públicas quer do setor privado) para obtenção ou análise de prova para os seus processos crime."
	2. Como são utilizadas as Informações pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?
	- "(…) fora da atividade processual penal, destinada a antecipar operações, predição de fenómenos específicos, planear operações para emprego dos meios operacionais e decidir opções estratégicas dentro de determinada organização. Esta é a dimensão mais relevante para prevenir alguns dos tipos penais, apesar de reduzido número, cujo a proatividade policial é a mais determinante." - "Por regra, inserida dentro da atividade processual penal, destinam-se a cumprir as finalidades do inquérito penal. As informações criminais, ou melhor a prova penal, destina-se investigar um crime depois de já ter acontecido. É uma atividade que tem a supervisão de um representante público que defende os interesse do Estado: um procurador/a do Ministério Público. Esta dimensão está focada para a descoberta da verdade e para "combater" os crimes nas mais diversas tipologias." - "(…) tenha um processo crime confiado está constantemente a "manusear" informação criminal, que pode ter várias origens, como por exemplo, fontes humanas (inquirições e interrogatórios), prova documental, acesso a base de dados, normalmente de acordo com a gestão feita no inquérito (…) cujas diligências poderão ser autorizadas por um Procurador ou um Juiz (…)."
	3. Quais as Tecnologias e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?
	- "Estão perfeitamente massificadas, pois os NAIIC das Seções de Investigação criminal dos Comandos Territoriais possuem a capacidade tecnológica (*IBM Security i2 Analyst's Notebook*) adequada para conferir resposta à tipologia de crimes, (…)" - "(…), utilizam várias ferramentas, da *Cellebrite's Digital* (…) *UFED Ultimate*."
	4. Enumere as principais vantagens e desvantagens resultantes da utilização dos Sistemas e Tecnologias de Informação pela estrutura de Investigação Criminal das Unidades Territoriais da GNR.
	- "Assim, a GNR dispõe de um conjunto diversificado de ferramentas forenses, dedicadas e para manusear informação criminal. Para análise de informação criminal, a ferramenta mais eficaz é o *IBM Security i2 Analyst's Notebook*. Para a extração e análise de prova em suporte eletrónico apreendido ou em redes, utilizam várias ferramentas (…)." - "Têm várias desvantagens relativas à sua dependência do sector privado porque atualmente o Estado não tem ferramentas próprias desenvolvidas para o efeito."
	5. Quais as melhorias que consideraria necessárias implementar no âmbito dos Sistemas e Tecnologias de Informação, a fim de reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?
	- "(…) fazer a diferença e ter relevância distintiva, quer na formação de militares da estrutura de Investigação Criminal, sob a coordenação da DIC, quer no apoio incondicional ás propostas que possam ser apresentadas pelos órgãos técnicos (…)."

Fonte: Elaboração própria, com base nas entrevistas exploratórias

Quadro n.º 10 - Análise de conteúdo das entrevistas exploratórias – Entrevistado B

N.º	Argumentação
EB	**1. Quais as limitações da estrutura de Investigação Criminal das Unidades Territoriais da GNR?**
	- "Como em qualquer atividade, os resultados da Investigação Criminal não poderão ser dissociados dos Recursos Humanos, logísticos e acima de tudo de TIC. Evidentemente que a capacidade de resposta será tanto melhor, quanto maior o grau de satisfação destas necessidades." - "Por outro lado, a LOIC acaba por, com frequência, acarretar constrangimentos, na medida em que para um determinado catálogo de crimes conduz a que o OPC que efetua as primeiras diligências, como medidas cautelares e de polícia, não seja o mesmo que depois o investiga. Esta organização que a LOIC estabelece leva a que, por exemplo para os crimes de competência reservada da PJ, seja criado um lapso temporal que, se não existisse, para muitas ocasiões beneficiaria os resultados da investigação pela redução do tempo de resposta."
	2. Como são utilizadas as Informações pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?
	- "As Unidades Territoriais têm na sua base o que, na minha perspetiva, é essencial para as informações criminais, que é a capacidade de recolha de informações para posterior tratamento. As Unidades, através dos NAIC´s, com apoio dos NIC e restantes estruturas de Investigação Criminal, acabam por trabalhar as informações, canalizando-as em sentido descendente e ascendente." - "Considero que as informações são, sem dúvida, essenciais para o combate e prevenção da criminalidade." - "No que concerne ao combate da criminalidade é fundamental ter capacidade de aglutinar em tempo todas as informações de índole criminal, de forma a poder identificar e combater o fenómeno criminal." - "Já no que respeita à prevenção da criminalidade, assume também extrema importância, permitindo estudar o fenómeno criminal, prevendo a sua evolução. Dessa forma torna-se possível orientar o policiamento nas suas diferentes vertentes."
	3. Quais as Tecnologias e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?
	- "Atualmente o SIIOP-P é a ferramenta que permite a recolha e registo de informação. Numa fase posterior serão desenvolvidas outras ferramentas nomeadamente na vertente da criminalística e Informação criminal."
	4. Enumere as principais vantagens e desvantagens resultantes da utilização dos Sistemas e Tecnologias de Informação pela estrutura de Investigação Criminal das Unidades Territoriais da GNR.
	- "O SIIOP-P permitiu centralizar toda a informação da criminalidade da GNR. Por outro lado, o sistema de supervisão e verificação, tem aumentado a qualidade da informação. O registo em tempo real que esta ferramenta veio permitir, veio na prática traduzir-se em capacidade de reação também em tempo real." - "A Guarda encontra-se atualmente a integrar os diferentes módulos de registo de informação, de forma a estabelecer um repositório único onde seja efetuado registo de toda a informação. Esse é sem dúvida um ponto essencial, uma vez que permite uniformizar, padronizar e sistematizar a recolha de informação para uma melhor utilização."
	5. Quais as melhorias que consideraria necessárias implementar no âmbito dos Sistemas e Tecnologias de Informação, a fim de reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?
	- "A Guarda ambiciona desenvolver uma ferramenta de *Bussiness Intelligence* de forma a poder "trabalhar" todo a informação que seja recolhida. Desta forma serão automatizados processos que permitirão apoio relevante e essencial à atividade da investigação criminal."

Fonte: Elaboração própria, com base nas entrevistas exploratórias

APÊNDICE R – CODIFICAÇÃO DAS RESPOSTAS ÀS ENTREVISTAS CONFIRMATÓRIAS

Quadro n.º 11 - Codificação numérica e cromática das entrevistas confirmatórias

N.º	Questão	Categoria	Subcategoria	Unidade de Registo
1	Considera que a Investigação Criminal das Unidades Territoriais da GNR apresenta debilidades na sua capacidade de resposta às exigências criminais atuais?	Debilidades da estrutura de IC das Unidades Territoriais da GNR	Normativa	1.1
			Partilha de Informação	1.2
			Formação	1.3
			Investimento Tecnológico	1.4
			Recursos Humanos	1.5
			Organização/Gestão Estrutural	1.6
2	Considera importante o contributo das informações policiais e das informações criminais para este objetivo? Por que razão?	Contributos das Informações na IC	Repressão	2.1
			Prevenção	2.2
3	De que modo são utilizadas as informações criminais pelas estruturas de Investigação Criminal das Unidades Territoriais, na resposta aos fenómenos criminais?	Utilização das Informações Criminais	Finalidades do Inquérito	3.1
			Tomada de Decisão	3.2
			Planeamento e Intervenção	3.3
			Análise	3.4
			Natureza do Crime	3.5
			Coordenação/Articulação	3.6
4	Quais as Tecnologias de Informação e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?	TI na estrutura de IC da GNR	*i2 Analyst´s Notebook*	4.1.1
			QGIS	4.1.2
			PowerBI	4.1.3
			FTK	4.1.4
			Cellebrite UFED Ultimate	4.1.5
			AFIS	4.1.6
			ArcGIS	4.1.7
			4IQ	4.1.8
			Paragon	4.1.9
			NUIX	4.1.10
			PC-Crash	4.1.11
		SI na estrutura de IC da GNR	SIIOP	4.2.1
			Serviços Partilhados	4.2.2
			PIIC	4.2.3

N.º	Questão	Categoria	Subcategoria	Unidade de Registo
5	Atendendo aos Sistemas e Tecnologias de Informação anteriormente enumerados, quais são as potencialidades decorrentes da sua utilização pela estrutura de Investigação Criminal das Unidades Territoriais da GNR?	Potencialidades da utilização dos Sistemas e TI na IC	Análise/Sintetização da Informação	5.1
			Identificação de Necessidades Processuais	5.2
			Pesquisa/Recolha de Informação	5.3
			Rentabilização dos Meios	5.4
			Preservação da Prova/Valor Probatório	5.5
			Identificação de Vestígios	5.6
			Partilha de Informação	5.7
			Armazenamento/Centralização da Informação	5.8
			Desmaterialização de Procedimentos	5.9
			Segurança da Informação	5.10
6	Considera estas suficientes para um desempenho eficaz na análise, prevenção e combate dos fenómenos criminais? Por que razão?	Aptidão das TI, utilizadas pelas SIIC, na resposta às exigências criminais	Insuficientes	6.1
			Suficientes	6.2
7	Analisando as principais Tecnologias e Sistemas de Informação utilizados pela estrutura de Investigação Criminal das Unidades da GNR, mencione as principais debilidades decorrentes do funcionamento e utilização dos mesmos.	Debilidades da utilização e funcionamento dos Sistemas e TI	Diversidade Tecnológica	7.1
			Recursos Humanos	7.2
			Formação	7.3
			Grau de Utilização	7.4
			Interoperabilidade entre Sistemas	7.5
			Registo e Acesso à Informação	7.6
			Partilha de Informação	7.7
			Gastos Logísticos	7.8
			Custo dos Equipamentos	7.9

N.º	Questão	Categoria	Subcategoria	Unidade de Registo
8	Considera que os objetivos e medidas definidos no domínio das Tecnologias de Informação dão resposta às necessidades operacionais da estrutura de Investigação Criminal das Unidades Territoriais? Por que razão?	Adequabilidade dos objetivos e medidas da Estratégia e Planos de Atividades da GNR	Parcialmente Adequados	**8.1**
			Desadequados	**8.2**
			Adequados	**8.3**
9	Quais são, na sua opinião, as melhorias a implementar no domínio dos Sistemas e Tecnologias de Informação, de modo a reforçar a eficácia operacional da estrutura de Investigação Criminal das Unidades Territoriais da GNR?	Melhorias a implementar nos Sistemas e TI	Interoperabilidade	**9.1**
			Novas Ferramentas Tecnológicas	**9.2**
			Base de Dados IC	**9.3**
			Confidencialidade da Informação	**9.4**
			Formação	**9.5**
			Recursos Humanos	**9.6**

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

APÊNDICE S – ANÁLISE DE CONTEÚDO DAS ENTREVISTAS CONFIRMATÓRIAS

Quadro n.º 12 - Análise de conteúdo da Questão n.º 1

N.º	Unidade de Contexto	UR
E1	- "No meu ponto de vista, o Despacho 18/14 que regula toda a estrutura da investigação criminal carece de uma revisão."	1.1
	- "Mas isso já tinha que entrar quase na reformulação de todo o Despacho 18/14."	
	- "(…) defendo que deveria haver uma centralização da investigação criminal. (…) Tudo isto teria como finalidade estar tudo no mesmo edifício, toda a gente troca experiência, toda a gente partilha informação. A partilha de informação é má e por vezes surgem quezílias entre os efetivos. Pessoalmente, defendo a centralização, em que deveria estar tudo junto num só edifício, numa só cascata."	1.2
	- "Existem imensas debilidades. A partilha da informação, é a maior delas todas."	
	- "Debilidades ao nível da formação e ao nível da integração de recursos humanos na estrutura da SIIC está a ser um problema atual, gravíssimo. Não se consegue introduzir militares na estrutura da SIIC, não há cursos de investigação criminal operativa quase há dois anos para Guardas. Falta de capacidade formativa e formação técnica."	1.3
	- "Os crimes cada vez têm evoluído mais e cada vez recorrem mais a tecnologias informáticas e nós estamos a ficar para trás no acompanhamento desses fenómenos, e em acompanhar este tipo de investigações. Longe vai o tempo em que as interceções telefónicas eram a solução para tudo. Temos que rever um pouco toda a nossa forma de estar, pois estamos a ficar para trás em relação à evolução que o crime tem vindo a ter."	1.4
E2	- "Quanto à vertente operativa, efetivamente, com o Despacho 18/14, houve uma redução significativa dos seus efetivos, acabaram as EII (Equipas de Investigação e Inquérito) dos Postos Territoriais, mas também trouxe alguns problemas, ao nível dos NAO. Também nestes núcleos houve uma redução de efetivos, o que muitas vezes compromete a recolha de prova fundamental para os Inquéritos, uma vez que são quem tem as missões de efetuar seguimentos e vigilâncias, a pedido das investigações mais complexas."	1.5
	- "Quanto a recursos humanos, a Guarda tem os mesmos efetivos que tinha há 10 anos atrás. O problema é que a sociedade evoluiu e passaram a existir novas exigências que resultaram no aparecimento de novas valências. (…) E aquilo que está a ser exigido às forças de segurança, é que em todas as situações que sejam consideradas de risco elevado, o inquérito seja elaborado e entregue à Autoridade Judiciária em setenta e duas horas. Isto é uma responsabilidade e uma carga enorme para todos os militares dos NIAVE."	
	- "Claro que se tivéssemos mais efetivo na estrutura de investigação criminal, principalmente na parte operativa, (…)."	
E3	- "(…), julgo que seria fundamental dotar as estruturas de Investigação Criminal dos Comandos Territoriais de equipamento digital e informático que nos permitisse extrair e processar dados, que no fundo são a prova essencial em muitos dos inquéritos em curso."	1.4
	- "As principais debilidades prendem-se com a falta pontual de recursos humanos, viaturas (…)."	1.5
E4	- "(…) e depois devia ao nível da estrutura superior, haver uma capacidade de ligação entre todos os Comandos. Neste momento, nós obviamente ligamo-nos, mas ligamo-nos por conhecimentos próprios, por via informal. Não existe, efetivamente, uma centralização do que é a Investigação Criminal. Nós se estivermos a investigar um indivíduo ou um grupo de indivíduos da prática de um determinado crime, não sabemos se existe mais algum Comando a investigar a mesma pessoa."	1.2
	- "Para além disso, há uma outra questão, mas que é transversal a todos, que é a falta de investimento na formação. Nós neste momento, pela falta de formação nos últimos 5 ou 6 anos, nunca mais houve um curso de formação inicial para Guardas, principalmente de Investigação Criminal. O resultado é termos as estruturas altamente debilitadas em termos de efetivo formado (…)."	1.3

N.º	Unidade de Contexto	UR
E4	- "(…) também, em termos de recursos tecnológicos. Tem os seus custos, mas se não houver investimento não acompanhamos a evolução da criminalidade."	1.4
	- "(…) havendo um reforço em termos do efetivo dos NIC, um reforço adequado de acordo com a realidade criminal do Destacamento onde se inserem (…), contudo há Destacamentos que o seu NIC necessitaria de mais face à sua realidade criminal."	1.5
	- "A Investigação Criminal devia ser repensada totalmente (…). O Chefe da SIIC devia ter a capacidade de investir mais num determinado Destacamento porque tem uma vaga de criminalidade. Devia ter a capacidade de, efetivamente, retirar militares de um lado e colocar no outro. Isto verifica-se essencialmente nos Comandos que não têm um NIC de Comando que permitam ao Chefe da SIIC poder gerir isso."	
	- "(…) os Postos trabalham 24 horas para responder às necessidades do cidadão em termos de lançamento de patrulhas, em termos preventivos, realização de operação, etc., mas a estrutura de Investigação Criminal não está ajustada para um trabalho de 24 horas. Poderia haver, inclusive, estratégias de rentabilização dos militares em apoio à Investigação Criminal, como por exemplo, utilizar os militares que estão em situações mais condicionadas como uma lesão ou outro motivo, para fazer parte, por exemplo, das equipas de transcrição, o que já seria uma mais-valia e iria poupar horas e horas de trabalho aos militares dos NIC."	1.6
E5	- "A falta de mentalidade de partilha de informação é uma das coisas que temos vindo a combater ao longo dos tempos, mas com principal incidência nestes últimos anos, em que o SIIOP-notícias está em vigor."	1.2
	- "(…) e a formação dos recursos humanos, (…) e não tem existido formação."	1.3
	- "Damos a formação inicial, mas depois não damos formação de atualização."	
	- "Os meios materiais também são parcos, as viaturas apresentam algum desgaste e idade, os meios tecnológicos não são abundantes."	1.4
	- "Em termos de estrutura o principal problema é o número, (…) os recursos são poucos."	1.5
	- "(…) existem diferentes realidades em termos de Comandos Territoriais e cada comando é diferente do outro em termos de realidade. Esse para mim é logo o principal problema. Não se pode olhar para as Unidades todas da mesma forma, existem Unidades que pelo volume de trabalho e de ocorrências criminais precisam de estruturas com mais efetivo e uma coordenação diferente das Unidades com menor índice de criminalidade e menos volume de trabalho. A Estrutura não deveria ser igual em todas as Unidades, onde praticamente só difere o número de militares afetos à estrutura."	1.6
	- "A estrutura em termos de recursos humanos também é muito estanque, isto é, tens um núcleo com oito militares, mas em determinados momentos oito podem ser poucos, era necessário agilizar o reforço pontual de recursos humanos."	
E6	- "O principal problema da Investigação Criminal prende-se com a falta de recursos humanos. A Investigação Criminal, neste momento, terá um efetivo global de cerca de 1400 militares quando, na minha opinião, deveria ter no mínimo 2000, para um serviço de excelência."	1.5
E7		
E8		
E9	- "Outro dos constrangimentos traduz-se na inclusão das "Informações" no âmbito das SIIC."	1.2
	- "Existem algumas debilidades na Investigação Criminal das Unidades Territoriais da GNR, começando desde logo pela falta de exclusividade de funções do Chefe da SIIC."	1.6
E10	- "Sim. Atualmente o crime não conhece fronteiras, os tribunais e as forças policiais apresentam divisões administrativas, que dificulta uma rápida perceção e combate dos fenómenos criminais. A título de exemplo, os crimes de furto de residências, o furto de interior de veículos, carteiristas, entre outros crimes, que quando observados de forma isolada apresentam pouca preocupação, mas analisados a nível nacional, mostram-nos estarmos na presença de criminalidade organizada que geram lucros avultados."	1.2
E11	- "(…) sendo fundamental a utilização de tecnologias, e constantemente renovadas/atualizadas, como ferramentas de apoio à atividade e às operações."	1.4
E12	- "(…) por falta da realização de cursos de ingresso (…) nos últimos anos."	1.3
	- "O primeiro tem a ver com a gestão de recursos humanos na Guarda e que por exemplo nas últimas transferências de SAJ ocorridas conduziu a que do total de 12 Núcleos (6 NIC, 2 NIAVE, 2 NAT, 1 NICAV e 1 NAO) 5 tivessem perdido o respetivo chefe (…)."	1.5
	- "(…) são os QOR deficitários pois o seu restabelecimento não tem sido efetuado (…)."	
E13	- "(…), a falta de formação especializada, (…)."	1.3

N.º	Unidade de Contexto	UR
E13	- "(…) e acesso a Sistemas de Informação, plataformas relevantes e *softwares* de pesquisa em fontes abertas, a necessidade de recursos informáticos acima dos padrões existentes na instituição, fruto da quantidade de informação a analisar e a tratar." - "Verifica-se o incremento da dificuldade de investigação dos crimes de catálogo, quando praticados com recurso à *internet* ou aos meios informáticos. A meu ver existe a necessidade de evoluirmos neste tipo de investigação e análise." - "Neste caso em concreto, os principais problemas / limitações são a falta de recursos humanos dedicados à análise de informação criminal, (…)."	1.4 1.5
E14	- "(…), falta de formação base e especifica." - "Sim, devido à carência de meios humanos e materiais, (…)."	1.3 1.5
E15	- "E curso de Investigação Criminal para Guardas, já não se verifica, o que limita, em muito, a entrada de militares nos Núcleos." - "E podíamos ter mais meios materiais, (…)." - "A estrutura de Investigação Criminal apresenta um grande problema, há algum tempo, que se prende com a falta de efetivo. Apesar de transversal a todas as valências da Guarda, a Investigação Criminal tem sofrido um pouco mais que as restantes."	1.3 1.4 1.5

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

Quadro n.º 13 - Análise de conteúdo da Questão n.º 2

N.º	Unidade de Contexto	UR
E1	- "As informações criminais apenas participam, genericamente, na componente do combate." - "Por isso, a informação criminal tem que ser vertida e é importante na componente da repressão. Se é importante na componente da repressão, estamos a falar no combate."	2.1
	- "Na componente da prevenção, estamos a falar já noutro tipo de informações, já estamos a falar na informação de ordem pública. As informações de ordem pública remetem para o como é que atuam, saber o *modus operandi*, ou seja, já não se está focado no indivíduo, no grupo, mas sim, no *modus operandi* e em função desse tipo de *modus operandi*, serão agilizadas medidas de segurança que permitam inviabilizar os seus intentos." - "(…) visam claramente a prevenção e tem a ver com estudar fenómenos criminais, a componente estatística, fazer a georreferenciação desses crimes, em função dessa georreferenciação, (…) visam a adoção depois de medidas e de empenhamento operativo, preventivamente."	2.2
E2	- "Quando essa informação policial conduz a uma informação criminal, é transmitida à Direção de Investigação Criminal, ou então no próprio plano territorial que, normalmente, procede logo em conformidade, é elaborado o auto de notícia quando se verifica que se está perante uma situação criminal." - "Nós, na Direção de Investigação Criminal, normalmente trabalhamos mais especificamente os casos concretos, os Inquéritos que o Ministério Público delegou na GNR para investigação."	2.1
	- "A informação policial é toda aquela notícia que depois de ser trabalhada torna-se informação, para a qual ainda não foi feito um auto de notícia e atribuído um NUIPC. Quando existe a elaboração do auto de notícia, passa a ser uma situação de investigação criminal."	2.2
	- "Portanto, estas são as razões em que tanto uma como outra, se complementam. Só é possível ter bons resultados quando, efetivamente, existe aqui uma complementaridade entre aquilo que é as informações policiais e aquilo que é a informação criminal, (…)."	2.1 2.2
E3	- "Por outro lado, as informações criminais dispõem de elementos de informação fundamentais para inquéritos em curso, pelo que o seu tratamento e partilha poderá dar um contributo significativo nas investigações que se encontram à responsabilidade das policias."	2.1
	- "Neste sentido, as informações policias são determinantes no domínio da prevenção criminal, na medida em que fornecem um conjunto de elementos de informação que se constituem como fundamentais ao planeamento operacional, levando o decisor a efetuar um balanceamento de recursos materiais e humanos, a empenhar em determinado lugar, espaço temporal e modo, com base nas informações, com o objetivo de dissuadir práticas criminosas."	2.2

N.º	Unidade de Contexto	UR
E4	- "(…), quer para a parte repressiva, em termos de combate de crimes." - "(…) e a DIC trata das informações criminais." - "(…) como das informações criminais, no âmbito da repressão (…)." - "(…), quer ao nível das informações criminais, mais vocacionado para a parte operativa que não faz prevenção, faz sim repressão da criminalidade." - "As informações, efetivamente, desempenham um papel imensamente importante, quer para a parte preventiva, (…)." - "Atendendo à estrutura superior da Guarda, a Direção de Informações trata das informações policiais, incluindo a parte da estatística, (…)." - "Porém, apesar das SIIC desempenharem um papel preponderante tanto as informações policiais, no âmbito da prevenção, (…)" - "Ao nível dos Comandos Territoriais, tudo se articula. As SIIC acabam por agrupar, quer as informações policiais, quer as informações criminais."	**2.1** **2.2** **2.1** **2.2**
E5	- "A informação criminal está diretamente relacionada com a atividade da investigação criminal." - "As informações policiais são destinadas à prossecução direta das missões legalmente atribuídas a serviços de natureza policial, sejam de nível estratégico ou operativo, isto é toda a informação que consegues recolher e tratar e que cada um ao seu nível a utiliza para as diversas missões que lhes estão atribuídas, são mais abrangentes que a informação criminal." - "As informações policiais mais relacionadas com a parte preventiva." - "Mas ao nível dos Comandos Territoriais, na parte operacional, estes dois tipos de informação complementam-se."	**2.1** **2.2** **2.1** **2.2**
E6	- "Na Investigação Criminal costumamos utilizar uma expressão muito simplista para, de alguma forma, diferenciar os dois conceitos: se tem NUIPC é Informação Criminal." - "As Informações Policiais atuam numa perspetiva mais preventiva, assente em modelos preditivos, em que se pretende, de uma forma genérica, antecipar e/ou acompanhar ações ou eventos relevantes para a missão geral da Guarda."	**2.1** **2.2**
E7	- "Tal como disse acima, as informações assumem hoje, mais que nunca, um papel crucial no combate ao crime (…)." - "Através da recolha de dados em massa, com qualidade, é possível realizar vários estudos, utilizando modelos matemáticos otimizados, mediante o histórico de dados, podendo correlacionar eventos e melhor determinar as suas causas, bem como poder prever a sua ocorrência."	**2.1** **2.2**
E8	- "Por sua vez, no âmbito da investigação criminal, o conjunto de elementos recolhidos no domínio da investigação em concreto e, por consequência, enquadrados num determinado processo crime, poderão adotar a designação de informações constantes no processo crime." - "A investigação criminal integra duas dimensões. Por um lado, a prevenção criminal, isto é, a primeira das suas dimensões, a qual está prevista em diversos documentos da Direção de Investigação Criminal, estruturantes relativamente à atividade da investigação criminal, e também no PCCCOFSS e, por outro lado, a investigação criminal, propriamente dita." - "(…) são fundamentais para a estrutura de investigação criminal, quer no âmbito da prevenção, através do desenvolvimento de ações operacionais concretas que permitam evitar o cometimento de crimes, (…)."	**2.1** **2.2** **2.2**
E9	- "O contributo das informações, sejam elas criminais ou policiais é de extrema e vital importância, pois permite-nos conhecer o nosso adversário, quer em termos estruturais/organizacionais (…)." - "O contributo das informações (…) é de extrema e vital importância para as instituições policiais, pois permite-nos conhecer (…) padrões de atuação, quer sejam eles de lugar ou de modo."	**2.1** **2.2**
E10	- "Sim, as informações policiais e as informações criminais, encontram-se separadas por uma linha ténue, (…)." - "(…) importantes para uma atuação sustentada na prevenção e na proatividade (…), torna-se fundamental a previsão e antecipação do risco, considerando-se, por essa razão as informações um fator de extrema importância para o sucesso da missão policial."	**2.1** **2.2** **2.2**

N.º	Unidade de Contexto	UR
E11	- "(…) em matéria de investigação criminal, nas vertentes operativa, criminalística e de análise de informação criminal."	2.1
	- "(…) elaborar estudos referentes às atividades de informações policiais e de segurança (…)."	2.2
E12	- "(…) no segundo, é a eficiência da própria investigação criminal que está em causa."	2.1
	- "(…) permite antecipar um potencial problema / acontecimento, permitindo proteger a forma e/ou ser mais eficaz na gestão/aplicação dos recursos. Se no primeiro caso (informações policiais) o maior benificiário dos produtos das informações é a área das operações (…)."	2.2
E13	- "O contributo das informações, independentemente destas se incluírem na componente policial ou criminal, é importantíssimo para o combate e/ou prevenção da prática de crimes. São estas componentes que permitem apoiar os decisores, no geral, nos seus diversos níveis, sejam eles estratégico, operacional e tático, (…) e da investigação criminal, (…)."	2.1 2.2
	- "(…) nos âmbitos da prevenção (…), mas também apoiar os investigadores e os patrulheiros no direcionamento da sua investigação e patrulhamento, respetivamente."	2.2
E14	- "Sim, pois a informação é a base da investigação, (…) para saber de onde partimos e para onde pretendemos ir na investigação de determinado fenómeno criminal."	2.1
	- "(…) e da preparação para a boa execução de uma operação, sem conhecimento dos dados essenciais e das várias condicionantes do fenómeno policial ou criminal, (…)."	2.2
E15	- "As informações criminais são aquelas que são trabalhadas dentro de um determinado processo crime."	2.1
	- "As informações policiais são fundamentais para orientar a ação policial e, portanto, a prevenção. Permitem orientar o patrulhamento, em certa áreas, com determinados objetivos."	2.2
	- "A estrutura de Investigação Criminal não se baseia apenas num tipo de informação. As informações criminais e as informações policiais são trabalhadas pelos NAIIC."	2.1 2.2

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

Quadro n.º 14 - Análise de conteúdo da Questão n.º 3

N.º	Unidade de Contexto	UR
E1	- "(…) na área do combate, na área repressiva, que hão-de ter sempre por base o inquérito e é nessa base do inquérito em que depois toda essa informação, a partir da qual saímos daquela componente da informação de ordem pública e entramos na informação criminal."	
	- "Passamos a ter um grupo, passamos a ter um suspeito e vamo-nos focar naquele grupo, naquele indivíduo."	3.1
	- "As informações criminais estão assentes no grupo, no indivíduo, no meliante, nos suspeitos, não está assente na análise de fenómenos criminais."	
	- "(…) a informação criminal é extremamente importante para a tomada de decisão (…)."	3.2
	- "(…) para o planeamento, e para a execução no âmbito repressivo."	3.3
	- "(…) processo fazendo o respetivo diagrama, a respetiva informação, criam o diagrama de conexões que é agregado ao processo e é feita a análise."	
	- "Através do NAIIC, é feito um acompanhamento dos fenómenos criminais, é feita uma avaliação e estudo de determinados fenómenos."	3.4
	- "A dinâmica consiste em, por exemplo, a operativa pede, vem para a análise, vai para o NTP. A operativa tem um acesso, quer que seja feita a análise do processo, vem para a análise e os analistas analisam o processo (…). É feita na análise, têm de solicitar."	3.6
E2	- "No entanto, temos outro tipo de criminalidade, como os roubos em residências, e mesmo às vezes os furtos em residência, já não falando no tráfico de estupefacientes, etc., que muitas vezes, ultrapassam a Zona de Ação de um Comando Territorial. Portanto, só trabalhando depois a nível dos NAIIC e na DIC, ao nível da RAIC (Repartição de Análise de Informação Criminal), é que é possível perceber se se trata de fenómenos que ultrapassam um Comando Territorial. Desta forma permite fazer uma análise das informações criminais que será difundido e trabalhado não só na própria investigação, mas também ao nível da prevenção."	3.5

N.º	Unidade de Contexto	UR
E2	- "(…) desta forma, permite fazer uma análise das informações criminais que será difundido e trabalhado não só na própria investigação, mas também ao nível da prevenção."	**3.6**
E3	- "(…) que compreende um conjunto de diligências processuais que visam provar a existência de crime, identificar os seus autores e correspondente responsabilidade, recolher os meios de prova existentes e identificar as circunstâncias de tempo, lugar e modo em que os factos ocorreram."	**3.1**
	- "(…) para que elaborem o respetivo planeamento operacional, com base na informação cedida, com vista a neutralizar o fenómeno criminal em análise, alocando os meios que acharem necessários."	**3.3**
	- "Com base nisso elaboram relatórios de informação que são enviados aos NIC, por forma a ceder elementos relevantes para a investigação e aconselhamento técnico, por forma a orientar o planeamento operacional."	
	- "(…), também são elaborados relatórios de informação criminal, com elementos recolhidos a nível distrital e nacional, recorrendo a sistemas e modos de análise de informação (…)."	**3.4**
	- "(…) procurando identificar fenómenos criminais e a forma como se comportam, nomeadamente o número de ocorrências, alvos, área geográfica, horário, *modus operandi*, entre outros."	**3.5**
	- "(…) para que os NIC do Comando Territorial tenham acesso a todos os elementos de informação criminal, servindo muitas vezes para apurar elementos em falta que se revelam essenciais para as investigações em curso."	**3.6**
E4	- "(…) onde é compilada toda a informação, sendo posteriormente disseminada, para que todos tenham a necessidade de conhecer e de se ajustar, pois são identificadas viaturas, são identificados indivíduos."	**3.3**
	- "(…) que estão focados, essencialmente, na georreferenciação dos crimes, no acompanhamento dos *hotspots* (…)."	**3.4**
E5	- "(…) as informações criminais ligadas à repressão, pois o fim da investigação criminal é descobrir quem cometeu o ilícito e leva-lo à justiça."	**3.1**
	- "(…) recolhemos a informação interna, a das redes sociais e fornecemos as informações tratadas às operações, para o planeamento da operação."	**3.3**
	- "A Parte Operativa, recebe os relatórios de informação, direciona o patrulhamento, efetua pesquisa de informação HUMINT."	
	- "(…) através da análise e inter-correlação das informações disponíveis nos Sistemas de Informação ou de fenómenos de estudos criminais. Na prática o NAIIC analisa a informação dos autos de notícia (…) e efetua estudos das tipologias criminais (…)."	**3.4**
	- "(…) é analisada a informação, efetuados estudos comparativos de caso (…)."	
	- "A partir das informações criminais recolhidas deteta-se um determinado fenómeno criminal, furto de máquinas de tabaco por exemplo (…)."	**3.5**
	- "(…) e é coordenada a IC para a questão da Investigação criminal e o dispositivo territorial para o patrulhamento. Os analistas por iniciativa procuram fenómenos ou pode ser também a pedido dos NIC (…)."	**3.6**
	- "Aos NAIIC compete apoiar os investigadores operativos, (…) remete ao dispositivo para os Comandantes de Destacamento e Postos Territoriais direcionarem o patrulhamento, para determinados locais, a determinadas horas."	
E6	- "A informação criminal assenta numa perspetiva repressiva, dando corpo ao objetivo da Investigação Criminal, de descobrir o crime, os seus agentes e o modo como terá ocorrido. Pretende, assim, encontrar prova de qualidade que auxilie o investigador na sua busca pela verdade dos factos."	**3.1**
	- "Neste sentido, procura também abrir eventuais novas linhas de investigação."	
	- "(…) e colaboram na difusão ao dispositivo de procedimentos claros de atuação, de recolha de informação e de investigação criminal."	**3.3**
	- "A Análise de Informação Criminal, nas Unidades Territoriais, está a cargo dos NAIIC (Núcleo de Análise de Informações e Informação Criminal)."	
	- "Numa outra fase, esta vertente procura estabelecer associações, ou seja, criar relações entre diversas entidades (pessoas, documentos, veículos, locais, processos, etc.), nomeadamente, as com maior probabilidade de se encontrarem associadas ao fenómeno criminal em análise."	**3.4**
	- "Numa perspetiva de estudo, os analistas de informação criminal procuram conhecer novos modos de atuação dos suspeitos por tipologia criminal."	**3.5**
	- "Existe ainda uma componente importante de partilha de informação com outras Forças e Serviços de Segurança ou entidades, diretamente relacionadas com informação criminal."	**3.6**

N.º	Unidade de Contexto	UR
E7		
E8	- "(…) das informações decorrentes da nossa atividade, serão fundamentais para o sucesso do desenvolvimento do processo crime, tendo em vista apurar a identidade dos suspeitos da prática de um crime e, tendo por base essa prova, serem responsabilizados pela prática desse mesmo crime."	**3.1**
E9	- "As informações criminais são utilizadas pelas estruturas de investigação criminal das Unidades Territoriais, na resposta aos fenómenos criminais, para nos permitir estabelecer padrões de atuação do nosso adversário, em termos territoriais, temporais ou de grupo de autores (…)."	**3.4**
	- "(…) e ainda dar conhecimento (…) sobre novos tipos de criminalidade."	**3.5**
E10	- "(…) com estudos quantitativo e qualitativo do crime, os seus intervenientes (suspeitos, arguidos e vítimas) e outros assuntos de segurança pública (ex. sociodemográficos, espaciais, temporais), auxiliam na redução, prevenção e avaliação da criminalidade."	**3.3**
	- "Nas Unidades Territoriais, estas informações são trabalhadas pelos Núcleos de Analise de Informação e Informações Criminais. Esta missão corresponde a um conjunto de processos analíticos e sistemáticos (...)."	
	- "O aspeto analítico deste processo implica a decomposição de um problema-chave complexo nos seus múltiplos constituintes. A quantificação de variáveis de um crime, do espaço e do tempo em que ocorre, permite a identificação de tendências (aumento, estabilização ou diminuição) de um fenómeno criminal, assim como o estabelecimento de correlações entre fatores ou conjuntos de crimes."	**3.4**
	- "(…) que visam facultar (…) as informações criminais de forma a dotar os vários Núcleos de Investigação com estudos quantitativo e qualitativo do crime (…)."	**3.6**
E11	- "(…) e na obtenção de prova no âmbito da investigação criminal."	**3.1**
	- "Obtenção de informações de diversas fontes (…), para apoiar a tomada de decisão, no sentido de tendências da atividade criminal (…)."	**3.2**
	- "O apoio ao processo de tomada de decisão/ação, baseado em informação (…)."	
	- "(…) tratamento da informação criminal em coordenação com a Direção de Informações."	**3.6**
E12	- "Permitem compreender o fenómeno e, se houver uma logica de atuação por parte dos adversários criminosos, atuar preditivamente e, eventualmente, permitir até antecipar movimentos, locais e datas e, no limite, efetuar detenções em flagrante."	**3.3**
	- "O estudo e análise das informações criminais permite, antecipadamente, perceber padrões e fenómenos criminais que possam estar em curso, melhorando a capacidade de reação e de investigação."	**3.4**
E13	- "Permite que o analista de informação criminal possa providenciar a informação necessária para suportar o processo de decisão (…)."	**3.2**
	- "(…) permitindo direcionar a prevenção dos ilícitos criminais, respetivamente. Permite alocar recursos humanos."	**3.3**
	- "(…) e assim desenvolver estratégias para a prevenção do crime, para resolver um processo crime em investigação, para efetuar a detenção de criminosos."	
	- "As informações criminais recolhidas e analisadas pelos Núcleos de Análise de Informações e Informação Criminal das Unidades Territoriais (…)."	**3.4**
	- "(…) são difundidas, consoante a finalidade, aos investigadores e aos patrulheiros, permitindo investigar em determinado sentido, (…)."	**3.6**
E14	- "Por outro lado, no decorrer dos processos, os investigadores procuram obter as suas informações criminais e pesquisam junto das outras Subunidades ou Unidades por informações de fenómenos idênticos."	**3.6**
E15	- "As informações criminais destinam-se a cumprir as finalidades do inquérito. Fornecem-nos linhas para a carreação de prova para um processo crime e identificação dos suspeitos."	**3.1**
	- "As informações criminais são utilizadas dentro de um determinado processo, orientando o trabalho dos investigadores e propondo linhas orientadoras de investigação (…)."	**3.3**

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

Quadro n.º 15 - Análise de conteúdo da Questão n.º 4

N.º	Unidade de Contexto	UR
E1	- "Na Guarda por inerência, o *software* que é utilizado é o *i2 Analyst´s Notebook* da IBM." - "O único que está generalizado em toda a Guarda é o i2."	4.1.1
	- "(…) e estou a utilizar o QGIS."	4.1.2
	- "Sei que, por exemplo, Santarém, para efeitos de georreferenciação utiliza o *PowerBI*."	4.1.3
	- "No caso aqui do Porto, temos um laboratório de digital forense, e utiliza também duas ferramentas. Estão a utilizar o FTK (…) para fazer a análise de equipamentos informáticos."	4.1.4
	- "No caso aqui do Porto, temos um laboratório de digital forense, e utiliza também duas ferramentas. (…) e estão a utilizar o *Cellebrite UFED Ultimate*, para fazer a análise de equipamentos informáticos."	4.1.5
	- "Em termos depois de *softwares*, aí não, já está bloqueado. (…) quando falo no ArcGIS, (…) estou a falar no âmbito dos NAIIC."	4.1.7
	- "Por toda a gente, independentemente das áreas é utilizado o SIIOP-P (…)." - "Por exemplo, o SIIOP-G apenas está aberto a alguns militares de análise."	4.2.1
	- "(…) as plataformas que estão partilhadas na *intranet*, TMenu, o SISII, o I24-7. As várias plataformas que estão partilhadas e em que há um conjunto de militares que têm acesso a elas, quer seja pela área operativa, quer seja pela área de análise, quer seja pela área da Criminalística."	4.2.2
E2	- "Na parte de análise criminal, o *i2 Analyst´s Notebook* continua a ser uma ferramenta fundamental para correlação e sintetização dos dados."	4.1.1
	- "(…) temos o caso da digital forense, que permitem a recolha e análise forense e dispõe de todos aqueles *softwares* que permitem retirar dos telemóveis e computadores, como o *Cellebrite UFED Ultimate*."	4.1.5
	- "A nível de criminalística são utilizados na lofoscópica *softwares* específicos, como é o caso do sistema AFIS."	4.1.6
	- "Existem também outras ferramentas de pesquisa e recolha de informação que permitem também chegar a outros dados importantes para a investigação, pesquisando em fontes abertas (OSINT) como é o caso do 4IQ, que o Centro de Informações da Guarda já tem uma licença para este *software*."	4.1.8
	- "(…) e o nosso SIIOP."	4.2.1
E3	- "Os Principais Sistemas utilizados são: SIIOP-P, (…)."	4.2.1
	- "Os Principais Sistemas utilizados são: (…), SIS II, SEGURNET, TMENU, SCoT, (…)."	4.2.2
	- "Os Principais Sistemas utilizados são: (…), e a PIIC."	4.2.3
E4	- "Temos o *i2 Analyst´s Notebook*, (…)."	4.1.1
	- "A criminalística utiliza o AFIS, que é um sistema fechado, e utilizado na pesquisa, no qual são introduzidas as resenhas no sistema e fazem as comparações."	4.1.6
	- "(…) o ArcGIS utilizados pela análise de informação criminal (…)."	4.1.7
	- "(…) o nosso SIIOP, incluindo o SIIOP-P (…)." - "(…) e o SIIOP-G (…)."	4.2.1
	- "(…) e depois as nossas plataformas internas onde temos o nosso SIIOP e neste os serviços partilhados, que são comuns a todas as vertentes. Porém o acesso nos serviços partilhados não é igual para todos, por exemplo o TMENU é mais fácil de pedir ao trânsito que conseguem aceder mais facilmente e principalmente ao nível das contraordenações."	4.2.2
	- "(…), a PIIC, (…)."	4.2.3
E5	- "Análise de Informação criminal trabalha com (…) o *i2 Analyst´s Notebook* (…)."	4.1.1
	- "Na parte da Criminalística, foram recentemente implementados os NDF que efetuam o trabalho de pesquisa nos telemóveis, *tablets*, PC, GPS…etc., e que trabalham com imensos *softwares*, como o *UFED Ultimate da Cellebrite*."	4.1.5
	- "A Criminalística utiliza também (…) o AFIS (*Automated Fingerprint Identification*), possuem também uma base em *Access*."	4.1.6
	- "A Análise de Informação criminal trabalha com o (…) ArcGIS (…)."	4.1.7
	- "Trabalha também com o *Paragon* da PJ, por causa das escutas telefónicas. Depois tratam a informação à base dos processadores de texto e dados."	4.1.9

N.º	Unidade de Contexto	UR
E5	- "A Parte Operativa utiliza essencialmente o SIIOP-P, para efetuar as suas pesquisas, recorrendo à análise quando necessitam de utilizar outro tipo de Sistemas de Informação."	**4.2.1**
	- "E posso acrescentar ainda, a PIIC no âmbito da partilha de informação entre os OPC."	**4.2.3**
E6	- "Na recolha, tratamento e análise de informação criminal (…), o *i2 Analyst´s Notebook*, entre outros."	**4.1.1**
	- "Na recolha, tratamento e análise de informação criminal (…) *UFED Ultimate* (…)."	**4.1.5**
	- "(…) o sistema AFIS na criminalística (…)."	**4.1.6**
	- "Na recolha, tratamento e análise de informação criminal, o NUIX (…)."	**4.1.10**
	- "(…) e o *PC-Crash*."	**4.1.11**
	- "(…) e o SIIOP."	**4.2.1**
E7	- "(…) deve ser tido em conta o Sistema Integrado de Informações Operacionais de Polícia (SIIOP) para registar a atividade operacional e, também, analisar tendências e efetuar análises espaciais."	**4.2.1**
E8	- "Por seu turno, no que concerne à análise de informação criminal, é utilizada a aplicação *i2 Analyst´s Notebook*."	**4.1.1**
	- "Em primeiro lugar, importa destacar o SIIOP-P, enquanto ferramenta central, (…)."	**4.2.1**
	- "(…), assim como o acesso a um conjunto de bases de dados que a GNR tem disponibilidade para aceder, nomeadamente, a base de dados *Schengen*, automaticamente pesquisada através de consulta no SIIOP-Principal, a base de dados da *Interpol*, viaturas furtadas, entre outras."	**4.2.2**
E9	- "São ainda, ao nível do tratamento dos dados recolhidos, usadas as ferramentas como o *i2 Analyst´s Notebook* (…)."	**4.1.1**
	- "(…) ou ainda da *Cellebrite UFED Ultimate*."	**4.1.5**
	- "(…), assim como o SIIOP."	**4.2.1**
	- "São utilizadas na pesquisa várias ferramentas, quer internas, quer em serviços partilhados com outras entidades, quer nacionais, quer estrangeiras, como a *Interpol* ou as partilhadas no espaço *Schengen*."	**4.2.2**
E10	- "A nível de Sistemas de Informação todos utilizam o Sistema Integrado de Informações Operacionais de Polícia (SIIOP/GNR), (…)."	**4.2.1**
	- "(…) relativamente a sistemas de informação é possível efetuar consultas em diversas bases de dados em uso nesta Guarda."	**4.2.2**
E11	- "(…) *UFED Ultimate* (…)."	**4.1.5**
	- "(…) do Sistema Integrado de Informações Operacionais de Polícia" (vulgo SIIOP)."	**4.2.1**
E12	- "(…) destaco neste particular, a última versão do SIIOP, que se mostra funcional a diversos níveis (embora a GNR a esteja cada vez mais a sobrecarregar com módulos)."	**4.2.1**
	- "A existência e acesso às diferentes Bases de Dados (condutores/veiculo, Registos de Propriedade/ SEI/ SISII, etc.), também é uma importante ferramenta tecnológica, que facilitam o dia a dia dos OPC, particularmente aqueles que realizam Investigação Criminal."	**4.2.2**
E13	- "As de conhecimento comum são: SIIOP (…)."	**4.2.1**
	- "(…), SIS II, 24/7 INSYST, SEGURNET, SCoT, (…) (a maioria destas referidas são utilizadas quer pela vertente operativa, criminalística e de análise de informação criminal)."	**4.2.2**
	- "(…), PIIC, (…)."	**4.2.3**
E14	- "SIIOP-P, SIIOP-2S, SIIOP-G, (…)."	**4.2.1**
	- "(…) SEI, EuVID, SCHENGEN II, GUR-tráfico de pessoas, *Interpol-INSYST*, TMENU, SEGURNET, Condutores & Veículos, SCoT, entre outros."	**4.2.2**
E15	- "A Análise de Informação Criminal trabalha muito com o *i2 Analyst´s Notebook*."	**4.1.1**
	- "A Criminalística também usa sistemas como o AFIS."	**4.1.6**
	- "O *Paragon*, permite-nos fazer a transcrição das escutas, a localização dos suspeitos e ouvir as comunicações, mas está sob a alçada da PJ."	**4.1.9**
	- "(…) e ainda o SIIOP, usado praticamente na recolha de informações."	**4.2.1**
	- "(…) e os Serviços Partilhados."	**4.2.2**

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

Quadro n.º 16 - Análise de conteúdo da Questão n.º 5

N.º	Unidade de Contexto	UR
E1	- "O i2 para efeitos de análise, construção de gráficos, correlações e diagramas de conexões e utilizo o QGIS para efeitos de georreferenciação de fenómenos criminais. Há um determinado fenómeno criminal, quero analisar, estou a fazê-lo com o QGIS. Tudo isto permite a sintetização da informação. Essa é a principal, sintetização de informação. (…) Permite-nos, também, verificar quando temos a informação toda sintetizada, verificar focos, *hotspots* de criminalidade."	5.1
	- "Permite-nos verificar no âmbito, por exemplo, de uma investigação, limitações ou elementos que ainda temos de carregar para o processo, em termos de prova porque quando temos toda a informação sintetizada, sabemos a informação que ainda nos falta ter, os elementos probatórios que ainda nos faltam."	5.2
	- "Melhor recolha, visualização e interpretação da informação."	
	- "Permite-nos, através da informação recolhida, identificar *hotspots* e permite-nos identificar locais onde requerem a adoção de medidas de segurança, medidas preventivas."	5.3
E2	- "Na vertente de análise de informações, temos o exemplo do i2, já referido que permitem a análise criminal e correlação dos dados (…)."	5.1
	- "(…) a utilização de *softwares* que permitem o acompanhamento das viaturas dos suspeitos sob investigação. Hoje em dia, mesmo que façamos um seguimento, o seguimento nunca pode ser em linha de vista, para não nos denunciarmos. Se nós temos uma sala de controlo e os nossos militares que estão na viatura, através de um *tablet* conseguem verificar a que velocidade vai o carro a deslocar-se, para onde se está a deslocar, onde parou, etc., o nosso carro à distância também permite fazer isso."	
	- "Estes *softwares* de pesquisa permitem fazer uma pesquisa profunda, constituindo uma mais-valia nas pesquisas dos indivíduos suspeitos, uma vez que um suspeito que já está referenciado, está autorizado pela Autoridade Judiciária, para que se investigue aquele crime (…)."	5.3
	- "(…) existem *softwares* fundamentais na pesquisa e recolha de informação OSINT, permitindo até verificar se determinados indivíduos suspeitos estão a fazer pagamentos em *bitcoins.* Portanto, isto é muito bom (…)."	
	- "Na criminalística, temos a digital forense, que são aqueles *softwares* que permitem retirar dados dos telemóveis e computadores, digamos assim, e aprofundar o seu conteúdo (…)."	
	- "(…) antes tínhamos de despender de 5 ou 6 viaturas, para conseguir fazer um trabalho de um dia, para saber o que estes suspeitos andavam a fazer, na prática de crimes ou na sua preparação."	5.4
	- "(…) em que o indivíduo é suspeito, dando legitimidade de aprofundar as situações, situações essas que depois são fundamentais para constituírem prova, após a sua validação pela Autoridade Judiciaria competente."	5.5
	- "Adicionalmente, temos o sistema AFIS, da parte lofoscópica, que continua a ser uma parte fundamental (…)."	
	- "Mas a verdade é que por vezes a parte lofoscópica tem resultados muito positivos em que coloca determinados indivíduos no local do crime, e isso é fundamental. É claro que não se faz só recolha lofoscópica, essa recolha de vestígios também pode ser biológica e até química. Na parte biológica, um indivíduo que deixa uma beata, que cuspiu no local do crime, pode-se muitas vezes chegar a saber quem é o indivíduo que cometeu o crime ou que pelo menos esteve naquele local."	5.6
E3	- "(…) e elaboram matrizes de comparação de casos, diagramas de conexão, entre outros que visam, essencialmente, perceber o *modus operandi* e se existe algum tipo de padrão. Com base nisso, elaboram relatórios de informação que são enviados aos NIC, por forma a ceder elementos relevantes para a investigação e aconselhamento técnico, por forma a orientar o planeamento operacional. Por outro lado, são elaborados relatórios de informação que são remetidos às subunidades operacionais, por forma a que o planeamento operacional tenha em conta as informações veiculadas, por forma a que as subunidades atuem de forma preventiva."	5.1
	- "Os NAIIC recolhem os elementos de informação achados pertinentes através destas tecnologias (…)."	5.3
	- "(…), entre outros organismos, e em que todas elas, na maioria dos casos, têm acesso através da partilha de informação."	5.7
	- "(…), que são alimentados pelas próprias policias (…)."	5.8

N.º	Unidade de Contexto	UR
E4	- "Estes programas permitem-nos, por exemplo, ao nível da análise de informações, estabelecer correlações, conexões e diagramas sobre toda a informação recolhida."	
	- "Na parte da análise de informação criminal, o *i2 Analyst´s Notebook* é uma ferramenta de análise extremamente poderosa. É uma ferramenta que é essencial principalmente nos processos de maior complexidade."	**5.1**
	- "(…) para passarmos a fazer os processos através de uma aplicação que poupa muito tempo, em termos da elaboração do relatório final."	
	- "Por exemplo, durante algum tempo houve determinados campos que não eram obrigatórios, como por exemplo, a localização geográfica do crime e é uma coisa essencial. Existe, efetivamente, alguns programas que permitem potenciar as coisas."	**5.2**
	- "As tecnologias dão-nos aquilo que nós quisermos. Existe, portanto, uma vastidão de locais onde conseguimos ir buscar a informação."	**5.3**
	- "Ao nível da criminalística, o AFIS é um programa excecional, operado por peritos e que atualmente é muito acessível. É o único método para o qual não existe contra-argumentação (…)."	
	- "O facto de a maior parte dos criminosos ter telemóvel, utilizar telemóvel como meio de conversação, quer seja telefonicamente, mas principalmente através das redes sociais é um obstáculo para a investigação. E neste momento, os Núcleos da Digitais Forenses, desempenham um papel fundamental na aquisição de prova para os processos."	**5.5**
	- "(…) se existe um vestígio biológico em como o indivíduo esteve naquele local do crime, o indivíduo não pode dizer que não esteve, (…) estabelece logo uma relação com o crime que não pode ser negada."	**5.6**
	- "Nós utilizamos as Tecnologias de Informação e as plataformas da Guarda porque é onde se encontram os dados que são a base do nosso trabalho."	**5.8**
	- "Por exemplo, dantes encontrava-se tudo escrito, eram feitos relatórios de informações e havia muita coisa escrita, não havendo a aposta que existe hoje nas informações policias, sendo fundamental, neste âmbito, o separador notícias."	**5.9**
E5	- "(…) produção de relatórios de análise operacional, em apoio a investigações em curso, produção de relatórios de OSINT, produção de relatórios de análise da criminalidade, análise de Listagens de *traceback*, Levantamentos GSM/WCDMA, georreferenciação através registos GPS, (…) que depois são traduzidos em relatórios, utilizados, por exemplo, para direcionamento de patrulhamento ou alertar o Comando Superior para determinado fenómeno. O *i2 Analyst´s Notebook* é utilizado quando temos muita quantidade de informação."	**5.1**
	- "Em termos de criminalística, os Núcleos Digitais Forenses (NDF) trabalham com diversos programas e faz a análise da informação que está nos computadores, nos *tablets*, nos GPS."	
	- "No caso de outros tipos de crimes, permite-nos recolher informação, preencher algumas lacunas que ficam na investigação."	**5.2**
	- "(…) análise das redes sociais e análise/avaliação a equipamentos informáticos/celulares a fim de recolher informações, extração de vídeos de sistemas de videovigilâncias (…)."	
	- "Na investigação criminal trabalhamos também com o *Paragon*, sob a alçada da PJ, nas escutas e isso permite-nos também através da análise das células, recolher informação sobre onde está o nosso alvo através do nosso sistema de triangulação, que serve para as vigilâncias, se tivermos as escutas telefónicas."	**5.3**
	- "Através da análise do telemóvel, conseguimos recolher toda essa informação. Através da análise dos telemóveis, conseguimos recuperar as mensagens que ela apagou, ou que ele apagou, ele ou ela vai apresentar queixa, mas só mostra a parte que lhe interessa. Com este *software* vamos recuperar a conversa toda, aquilo é parte a parte depois, e isso também é extremamente útil."	
	- "(…) e apoio em buscas para a correta preservação de dados digitais através dos Núcleos Digitais Forenses (NDF), (…)."	
	- "Em termos dos NDF, enquanto vantagens, temos o acesso à informação presente, por exemplo no *Whatsapp* do telemóvel do indivíduo, mas apesar de não termos acesso a essa informação em tempo real, conseguimos depois apensar para o processo."	**5.5**
	- "Mas estão também a ser muito eficazes para a questão da violência doméstica, em termos de prova na violência doméstica."	
	- "A criminalística também usa o AFIS, que é o sistema que permite depois a comparação das impressões digitais. Depois de estar inserido no sistema, pode ser realizada uma pesquisa e verificar se aquele indivíduo já tinha sido identificado, noutro crime e se aquela impressão digital pertence àquele indivíduo."	**5.6**

N.º	Unidade de Contexto	UR
E5	- "(…) consegues recolher a informação do que se passou a nível nacional, (…). Por outro lado, o pessoal do NAIIC tem acesso ao Comando todo, e mais dois ou três homens por cada NAIIC, tem acesso a tudo o que se passa a nível da Guarda. Nisso, a ferramenta também é boa e é muito útil porque o crime não tem fronteiras."	5.7
	- "(…) temos concentrados todos os autos de notícia da Unidade e conseguimos tratar de maior quantidade de informação, o que é útil para a parte da investigação criminal." - "Em termos de criminalística, o SIIOP é mais como um repositório." - "(…) e insere-se isso tudo no sistema, que é o AFIS." - "As vantagens da Análise de Informação Criminal, em termos de SIIOP, são idênticas, ou seja, está lá a informação concentrada (…)."	5.8
	- "O SIIOP tem um campo para inserir essa informação, que antigamente usava-se a guia de patrulha. Os militares iam registar a guia de patrulha, os contactos que fizeram com a população, a informação que reuniram e agora temos o SIIOP-notícias. Isso já é uma evolução em relação a Sistemas de Informação. (…) e que antigamente só eram registadas no relatório de atendimento, ficando arquivado em formato papel no Posto. Hoje em dia, registam no SIIOP-notícias. O pessoal da Investigação criminal tem acesso a essa informação." - "Antigamente, os autos de notícia eram remetidos em papel para o Destacamento. Tinham os autos de notícia todos, mas estavam em papel. Para tratar era muito mais complexo (…)."	5.9
E6	- "(…) tratamento e análise de informação criminal (NUIX, *UFED Ultimate*, *i2 Analyst´s Notebook*, entre outros) (…)." - "O *PC-Crash* é uma ferramenta de simulação de colisão e trajetória do *Windows* que permite a análise precisa de uma ampla variedade de colisões de veículos a motor e outros incidentes. É uma ferramenta imprescindível (…) no que respeita à investigação de acidentes de viação com sinistralidade grave (mortos e/ou feridos graves), com um elevado número de vítimas ou de elevada complexidade."	5.1
	- "Grande parte do trabalho de análise encontra-se suportado nas Tecnologias de Informação, sem sistemas informáticos e programas facilitadores da recolha, (…)." - "Na área digital forense, existe uma panóplia de ferramentas e soluções que são utilizadas para recolha (…)."	5.3
	- "Acresce referir que, a impressão digital é ainda hoje o único tipo de vestígio que coloca, inequivocamente, um indivíduo num certo local ou a manusear um certo objeto." - "(…) e preservação de prova em suporte tecnológico."	5.5
	- "(…) e permite associar uma identificação a um vestígio lofoscópico (impressão digital) encontrada em cena de crime." - "(…) exercer todas as competências técnicas que temos no tratamento e comparação de impressões digitais."	5.6
	- "(…) e a partilha indireta de informação." - "Queremos, no futuro, além de promover a partilha de estações com os outros OPC, conforme determina a Lei de Identificação Judiciária e Lofoscópica, (…)."	5.7
	- "Os Sistemas de Informação comportam parte da informação necessária para ampliar os antecedentes dos suspeitos, as associações que possam existir com outras entidades (…)." - "O AFIS que nos permite alimentar e ter acesso ao Ficheiro Central de Dados Lofoscópicos, responde às necessidades da investigação criminal, (…)."	5.8
	- "Assim, para além das bases de dados de registo de expediente, exames e perícias, (…)."	5.9
E7	- "(…) permite análise de tendências, análises espaciais, etc." - "(…), mas tem outras ferramentas de análise e de reconstrução de eventos."	5.1
	- "(…), que tem como suporte a base de dados de analítica do SIIOP e outras bases de dados internas e externas à Guarda."	5.7
	- "(…) deve ser tido em conta que o SIIOP ao registar toda a atividade operacional, (…)." - "(…), que tem por referência a base de dados (…) do SIIOP, (…)."	5.8
E8	- "(…), bem como a produção de relatórios de análise de informação criminal, isto é, a análise de processos crime em curso, permitindo fazer face à evolução dos fenómenos." - "(…) e que nos permitam concretizar uma análise de toda a dinâmica criminal e, deste modo, conseguir interpretar tendências e atuar preventivamente, relativamente à evolução destes mesmos fenómenos criminais."	5.1

N.º	Unidade de Contexto	UR
E8	- "(…), sobre os mandados de detenção pendentes, que deverão ser registados no SIIOP-P, assim como outras áreas concretas da nossa atividade."	5.2
	- "(…) é possível o registo, a recolha, o tratamento e a produção de Informações, em termos globais, (…)."	5.3
	- "(…) para que possamos ter prova e dados fiáveis, relativamente aos crimes registados na zona de ação da GNR. Importa sublinhar que, não se trata apenas de registar os respetivos crimes, trata-se de registar um conjunto de dados associados a esses mesmos crimes, testemunhados por nós ou por terceiros (…)."	5.5
	- "(…) e, por outro lado, exportar, automaticamente, para outros Sistemas, um conjunto de informações (…)."	5.7
	- "Consequentemente, toda essa informação tramita, de forma automática, entre o SIIOP-P e o sistema informático de estatística da justiça, da Direção Geral Política de Justiça."	
	- "Com o elevado volume de informação e o emergir de situações que se desenvolvem, cada vez mais, com uma dinâmica mais célere (…). A partir destes, é possível o registo (…)."	5.8
	- "O SIIOP tem a capacidade de nos disponibilizar informação detalhada sobre todos os crimes e notícias registados na Guarda, (…)."	
	- "(…) diversos procedimentos tendentes à desmaterialização de procedimentos para que, efetivamente, o SIIOP, seja um Sistema de Informação destinado ao registo de toda a atividade da Guarda, e, neste caso em particular, o registo criminal da Guarda."	5.9
E9	- "(…), bem como no tratamento de grandes volumes de dados."	5.1
	- "(…), pois atendendo ao grande volume de dados a pesquisar ou tratar, permite-nos rapidez, fiabilidade (…)."	5.3
	- "(…) são essencialmente utilizadas pelo NAIIC, na recolha e pesquisa de informações em fontes abertas ou reservadas (…)."	
	- "(…) e ainda integridade dos dados recolhidos e/ou tratados."	5.5
E10	- "(…), que evitaria a duplicação de investigações a fenómenos idênticos e muitas vezes aos mesmos suspeitos."	5.4
	- "Usado na sua plenitude pela investigação criminal, estamos a falar de um repositório único de informação, (…)."	5.8
E11	- "Permitir o cruzamento de informação (disponibiliza uma imagem contextual da situação)."	
	- "Garantir a unicidade da informação, uma vez que o sistema está disponível em todo o dispositivo, (…)."	5.1
	- "A forma de agregar a informação registada e tratada assenta numa lógica de processos, em que o sistema disponibiliza a criação de normas específicas para cada tipologia de registos."	
	- "(…) realização de pesquisas de dados informáticos simples a equipamentos apreendidos à ordem de processos crime."	
	- "O registo de informação é um dos fatores críticos de sucesso. A recolha da informação na origem e a qualidade dos dados recolhidos é um dos fatores que influencia diretamente todo o desempenho do sistema."	5.3
	- "(…) e a rentabilização da capacidade instalada, potenciando o facto da GNR se encontrar implementada em todo o Território Nacional."	5.4
	- "No âmbito da atividade digital forense é fundamental em sede de arquivo digital corrente, ter capacidade para armazenar as imagens dos equipamentos digitais apreendidos em processo crime."	5.5
	- "Garantir a interoperabilidade dos sistemas, através de importação/exportação de dados para outros sistemas."	5.7
	- "(…) a partir de um repositório único e centralizado, é possível garantir que a informação assim que é registada, possa ser reutilizada ou completada por qualquer militar, desde que devidamente credenciado para o efeito."	5.8
	- "A investigação criminal clássica, de uma forma genérica, assentava essencialmente na vigilância e nos seguimentos, nos depoimentos e interrogatórios, nos registos de interceções e comunicações, na consulta de base de dados (abertas, públicas, mandado judicial), nos estudos de documentos, nos exames e perícias diversas. Na última década, foram adicionados novos ingredientes que devem ser considerados (…)."	5.9
	- "Preservar a necessidade de saber, fornecendo a informação a quem dela necessita e garantindo o acesso à informação apenas a quem de direito."	5.10

N.º	Unidade de Contexto	UR
E12	- "(…) a maior facilidade que há na interpretação de dados sistematizados aproveitando, neste particular, a Análise de Informação Criminal." - "(…), principalmente, no trabalho de análise, (…) na sistematização da informação e, particularmente, na sua correlação, para permitir chegar a resultados."	5.1
	- "(…) o tratamento informático que hoje é dado aos processo e que facilita a extração de dados e, também nesta área, aproveitam todas as vertentes funcionais da Investigação Criminal (…)."	5.3
	- "(…) na rentabilização dos recursos disponíveis, (…)."	5.4
	- "Hoje em dia, grande parte dos criminosos e da criminalidade recorre às tecnologias informáticas, sejam em comunicações (Telemóveis/T*ablet*/PC's), sejam através do recurso a sistemas informáticos. A aposta nestas áreas tem apresentado resultados excecionais reconhecidos pelos nossos investigadores, na melhoria dos resultados operacionais alcançados e pelos próprios tribunais (magistrados Judiciais e do MP)."	5.5
	- "Desde logo, no arquivo e consulta dos processos e este vetor abrange todas as vertentes funcionais da Investigação Criminal, (…)."	5.9
E13	- "(…), integramos a mesma na produção de diversos produtos de análise (matrizes, diagramas de associação, diagramas de conexões, cronogramas, fluxogramas, etc.) e efetuamos a sua análise (…)." - "(…) efetuam a integração e tratamento de informação, reduzem o tempo de resposta."	5.1
	- "(…), realizamos uma recolha de informação sobre as mais diversas entidades (pessoas, locais, contactos, viaturas, etc.), circunscrita no âmbito de vários ou de um Número Único de Identificação de Processo Crime (NUIPC), (…)." - "(…) ajudam a recolher informação, (…)."	5.3
E14	- "Obtenção de informação diversificada e proveniente de várias Entidades, disponível *online* e acessível de forma remota."	5.3
E15	- "O i2 é das maiores potencialidades que a Investigação Criminal tem. Tem potencialidades de análise de informação criminal, que pode ser usado nas informações policiais também." Tem possibilidades enormes de relação dos suspeitos."	5.1
	- "Em termos de potencialidades, é principalmente aquilo que os NAO dispõem, em termos de vigilância e fotografia remota, importante na recolha de informação."	5.3
	- "As provas recolhidas no AFIS permitem-nos, mais tarde, identificar um suspeito de um crime cometido agora, pois esse vestígio fica em sistema."	5.5
	- "O sistema AFIS tem essa possibilidade de nos permitir identificar os vestígios, desde que tenham a mínima qualidade."	5.6

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

Quadro n.º 17 - Análise de conteúdo da Questão n.º 6

N.º	Unidade de Contexto	UR
E1	- "Não, existem diversos constrangimentos, nomeadamente, ao nível da fiabilidade e da qualidade dos dados que se encontram inseridos nos Sistemas de Informação, isso por um lado. Por outro lado, não chega só termos um Sistema de Informação, não chega só a informação estar carregada no sistema se não a conseguirmos de lá extrair e depois ter meios humanos e meios tecnológicos, *softwares* para, de uma forma centralizada e agregada, conseguirmos fazer a sua análise. Se não o tivermos, não conseguimos." - "Temos carências ao nível de um conjunto de tecnologias, que muitas vezes nos deveriam facilitar os trabalhos ao nível da análise. Há ferramentas que podiam logo estar interligadas e, neste momento, não estão. (…) hoje, quase todos os crimes acabam por envolver Tecnologias e Sistemas de Informação que depois nós temos dificuldade em reunir prova, em conseguir reunir elementos, ter informação em tempo útil para conseguir acompanhar o crime, (…)."	6.1

N.º	Unidade de Contexto	UR
E2	- "Não. (…), isto implica, também, em todas as investigações, um trabalho de HUMINT, trabalho esse feito pela pessoa, de preferência qualificada para tal. As tecnologias não substituem muitas vezes o trabalho necessário que tem que se fazer no terreno." - "O próprio Ministério Público exige também, o seu complemento com situações presenciais, porque enquanto na fase de inquérito ou de investigação, isto pode ser considerado como prova, em fase de julgamento só há uma coisa que é válida, que é a prova testemunhal. Em Tribunal, é fundamental haver esta prova testemunhal." - "A partir do momento em que damos a conhecer aos criminosos todas as tecnologias que utilizamos, estes começam a tomar providências de contramedidas para a utilização destas tecnologias. A grande dificuldade é que os criminosos tomam, cada vez mais, um cuidado acrescido com as interceções telefónicas."	**6.1**
E3	- "Não. Os sistemas de informação enumerados anteriormente dispõem de um universo vastíssimo de informação que, por si só, não se revela eficaz na prevenção e combate à criminalidade. Para que isso seja possível, há a necessidade de tratar essa informação e subordinar as operações às informações para que a prevenção seja eficiente."	**6.1**
E4	- "Não são. Não são porque há uma ferramenta, que para mim é essencial, que é o mapeamento do crime que é, efetivamente, o ponto chave de tudo, em termos de Investigação Criminal. Este programa permite fazer análise estatística, permite fazer a questão dos *hotspots*, permite fazer uma leitura extensiva do terreno, permite compreender, efetivamente, a evolução do crime, em determinados contextos territoriais, ao longo do tempo e, o mais importante, permite fazê-lo ao momento. São ferramentas plenas que atualmente é totalmente necessário."	**6.1**
E5	- "Sim, considero que temos ferramentas suficientes, em qualidade para efetuar o nosso trabalho, em quantidade deveríamos ter mais. Claro que não é o que desejamos, e apesar de querermos sempre mais, temos o necessário para conseguir analisar a informação, efetuar seguimentos e vigilâncias, entre outras missões."	**6.2**
E6	- "É uma área com tendência para crescer, na qual temos prestado um serviço de enorme qualidade aos investigadores, embora tenhamos algumas pendências, pois o volume de trabalho tem aumentado exponencialmente, com pedidos não só da Investigação Criminal da Guarda, como também, dos Tribunais, do Ministério Público e de outros OPC."	**6.2**
E7		
E8	- "Não poderão ser considerados suficientes, (…) visto que ambicionamos ter sistemas que nos possam dar e, por sua vez, responder, a tudo aquilo que são as nossas necessidades. Deste modo, existe, ainda, um caminho a percorrer no sentido da melhoria dos nossos sistemas. (…) devemos continuar a progredir, no sentido do aperfeiçoamento de todos estes sistemas disponíveis, quer no âmbito do registo, quer no domínio da análise de informação."	**6.1**
E9	- "A rápida capacidade de reorganização e de rearticulação dos diversos fenómenos de criminalidade, tornada possível pelos avanços tecnológicos, dinamizaram as atividades criminosas tradicionais e viabilizaram a prática de novos crimes. Assim as ferramentas atualmente ao dispor são manifestamente insuficientes tornando-se rapidamente obsoletas."	**6.1**
E10	- "Não, em virtude de o sistema ainda não estar dotado de um sistema de *Data Mining* ou Prospeção de dados, que constitui um conjunto de ferramentas que permitem agregar e organizar grandes quantidades de dados e identificar padrões, regras de associação, mudanças e anomalias relevantes."	**6.1**
E11	- "(…) pretende-se colmatar, em parte, soluções para o novo paradigma da investigação criminal, por força das disrupções tecnológicas positivas, adquirindo equipamentos com vista a otimizar os recursos humanos da estrutura Investigação Criminal e elevar a qualidade dos procedimentos, (…) sendo fundamental no âmbito da atividade digital forense (…)."	**6.1**
E12	- "A nível de potenciar uma maior eficácia no combate aos fenómenos criminais, hoje em dia, temos alguns recursos a este nível. No entanto, estão obsoletos e a sua utilização não está devidamente regulada internamente."	**6.1**
E13	- "Não. Existem plataformas com informação relevante que, atualmente, a vertente de análise de informação criminal, ou mesmo a vertente operativa, apenas acede por triangulação, ou seja, através de pedidos de informação externos, não sendo a melhor forma de recolher informação, por questões de celeridade."	**6.1**
E14	- "Não, porque apenas constituem uma base de trabalho. Para o bom andamento da investigação é fundamental realizar tarefas de investigação, seguimento e vigilância e obter outros meios de prova."	**6.1**

N.º	Unidade de Contexto	UR
E15	- "Não é suficiente, porque os Núcleos estão deficitários em termos de vários materiais, principalmente, nesta áreas dos Sistemas e Tecnologias de Informação. Em termos de prevenção e combate, não tem o suficiente. Existe muito a necessidade de os militares utilizarem os seus próprios meios, ou seja, têm de dispor dos seus bens pessoais e que apresentam melhores capacidades, do que aquilo que é disponibilizado institucionalmente para um trabalho eficaz."	6.1

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

Quadro n.º 18 - Análise de conteúdo da Questão n.º 7

N.º	Unidade de Contexto	UR
E1	- "Hoje em dia há um conjunto de ferramentas disponíveis pelo mercado, mas que tirando, praticamente o *i2 Analyst´s Notebook*, praticamente em termos de Guarda, nada mais se utiliza. Há mais ferramentas de análise que podem ser utilizadas e informação, que muita vezes está disponível, e não somos capazes de a analisar. Temos que melhorar nesse campo. Poder-se-ia rentabilizar muito mais."	7.1
	- "(…), faltam-nos depois ferramentas."	
	- "(…), temos carências ao nível de recursos humanos, em quantidade (…)."	7.2
	- "Normalmente essas ferramentas, muitas delas, requerem conhecimentos técnicos para operar com as mesmas, o que implica formação, implica tempo."	7.3
	- "(…) mas não tenho ArcGIS, não há licença de ArcGIS. O sistema que temos não pode ser ligado à rede, senão não funciona, porque as licenças estão caducadas (…)."	7.4
	- "(…) e depois não temos capacidade de resposta. As Unidades têm que ter, e trabalham com essas ferramentas caducadas. Quem diz essas, diz outras ferramentas."	
	- "Deveríamos ter o nosso SIIOP-P agregado diretamente ao i2, já que utilizamos o *Analyst Notebook* através do *IBridge* ligado. Deste modo, poderíamos utilizar, automaticamente, o próprio I2 e fazer-nos a análise de toda da informação que lá se encontra. Mas, também, temos de, na base, fazer as coisas em condições."	7.5
	- "Deveria ter um outro *software* anexado diretamente ao SIIOP-P e em função dos pedidos, recolhia logo essa informação (…)."	
	- "Na base, também não se pode estar a criar um documento por peças, ou seja, quando se inserem os dados. Por exemplo, há um furto e são furtadas 20 peças ou 20 bens. Temos de criar bem a bem no *software* e, muitas vezes, o que acontece é: quem está a inserir não os criam. Faz o descritivo só no auto de notícia, sendo que depois no sistema, surgem constrangimentos ao nível da pesquisa. Elas estão lá, mas nem sempre devolve resultados. Há muita informação que nós temos, que está carregada, mas depois, não está acessível, (…)."	7.6
	- "Outro constrangimento que existe é, muita vezes, a fiabilidade e qualidade dos dados e a forma como são carregados. A informação existe, mas não é possível extraí-la dos Sistemas de Informação. Ela está lá, sabemos que está lá, mas não a conseguimos extrair. Esse é outro constrangimento."	
	- "O que assistimos atualmente é, por exemplo, o NIC de um Destacamento tem informação, mas não a faz passar ao camarada de outro NIC. A partilha de informação é má (…)."	7.7
E2	- "Quando são colocadas todas as diligências de Investigação Criminal no SIIOP-P, tem que haver mais uma série de perfis que têm que ser criados (…). Portanto, nesta altura tem de se desenvolver o SIIOP para garantir esta confidencialidade necessária no que diz respeito à Investigação Criminal."	7.6
	"Ou seja, poderia existir mais agilização e celeridade através de um investimento no SIIOP, algum desenvolvimento para a área de Investigação Criminal. Portanto, isto ainda está a ser feito, através dos NAIIC e pela estrutura de Investigação Criminal, em circuito fechado com a DIC."	7.7
E3	- "(…) contudo, deveria caminhar-se no sentido da integração, existindo uma só plataforma policial, onde estivesse disponível toda a informação que atualmente se encontra distribuída por diversos sistemas, que fosse comum a todas as Forças e Serviços de Segurança, respeitando o princípio da necessidade de saber."	7.5

N.º	Unidade de Contexto	UR
E3	- "Para além disto, todos os organismos deveriam concorrer, obrigatoriamente, para alimentar o respetivo sistema com os dados pretendidos."	**7.7**
E4	- "Nós não temos uma plena utilização de *Crime Mapping*. Nós não temos programas com o apoio imediato ao ArcGIS, como existem em múltiplas polícias a nível mundial."	
	- "Ao nível do Núcleo Digital Forense, esses sim, necessitariam de ter acesso a todas as ferramentas que necessitam para trabalhar, porque eles são, efetivamente, o futuro da Investigação Criminal. Eles necessitam dos meios todos que existem (…)."	**7.1**
	- "Este sim, é um Núcleo que tem de se investir em termos de mais efetivo (…)."	
	- "Neste momento, a falta de efetivo é muito grande."	**7.2**
	- "Quanto ao *i2 Analyst´s Notebook*, é uma ferramenta essencial, mas nós precisávamos de a ter formalmente plena, ou seja, nós não temos a licença. Nós trabalhamos com versões antigas. Deveria haver licenças para todos e licenças atuais."	
	- "(…) e que nem tem acesso às licenças todas. Tem acesso a determinadas licenças, mas a licença não é uma licença completa, só lhe permite fazer determinado tipo de extrações e, por vezes, quando necessita de fazer determinado tipo de extrações, tem de estar à espera que disponibilizem uma outra licença a nível nacional para ele poder trabalhar."	**7.4**
	- "Não conseguimos analisar o corpo do auto de notícia, a não ser que seja lido auto a auto. Não dá para fazer a pesquisa e, o que efetivamente dá para fazer pesquisa, é um campo muito limitado em termos de carateres."	
	- "Para se extrair dados do SIIOP-P, eu extraio os dados para uma folha *Excel* e depois, na folha *Excel*, é que posso fazer o tratamento para gráficos. A informação tem de ser trabalhada à parte e só funciona se a informação for relativamente pequena."	**7.6**
	- "Depois, também temos a questão da PIIC em que ninguém insere lá quase nada, devendo ser obrigatório os dados serem lá inseridos, e tudo isto por uma questão simples, não existe mentalidade de partilha de informação."	**7.7**
	- "Outro aspeto negativo é, no âmbito da criminalística, por exemplo, a nossa Subsecção de Criminalística acaba por fazer o tratamento dos vestígios biológicos de outros Comandos e temos de ir à estação AFIS de Aveiro, porque não temos uma estação nossa."	**7.8**
E5	- "Relativamente a qual *software* é utilizado, varia também de Unidade para Unidade (…). Por vezes em vários Comandos, a Guarda não tem assim tantos sistemas (…)."	**7.1**
	- "O Núcleo Digital Forense é extremamente útil, mas precisa de mais efetivo (…)."	**7.2**
	- "Isto vai entroncar noutro aspeto, que é a falta de formação."	
	- "Em termos dos NAIIC, também é uma aposta que tem vindo a ser feita, é preciso também investir mais na formação deles."	
	- "A principal desvantagem do *Analyst* é que nem toda a gente sabe trabalhar com ele. O NAIIC não investe em toda a gente para trabalhar no *Analyst Notebook*, (…)."	**7.3**
	- "E é preciso apostar no recurso humano. Nós damos a formação inicial apenas, e é uma das limitações na estrutura da Investigação Criminal. Damos a formação inicial, mas depois não damos formações de atualização."	
	- "(…) devia ter mais licenças, mas não tem e estamos um pouco limitados em termos de material de *hardware* e *software*."	**7.4**
	- "(…) o SIIOP ainda não está a dar as respostas corretas. Também devia ter ligações, por exemplo, à base de dados de identificação ou outras bases, o que vai permitir ter muita mais informação."	**7.5**
	- "Não existe interesse em termos muita informação e os sistemas carregados se estás numa ocorrência e não consegues saber o que diz respeito a determinado indivíduo suspeito, por exemplo, isto ao nível do patrulheiro, nível do Comando Territorial."	
	- "O SIIOP permite que consigas extrair todo o teor do auto de notícia, mas ainda não se consegue fazer isso diretamente, não é através de uma pesquisa simples, porque ainda há coisas que estão em desenvolvimento no SIIOP, ainda não estão a funcionar. E as pesquisas é um dos campos que ainda não está bem acabado. No atual SIIOP, temos de criar mesmo os passos todos outra vez. Por vezes, os militares fazem isso, inserem lá o nome e o descritivo, mas não criam bem a pessoa."	**7.6**
	- "Aqui vamos ao encontro do tal problema das mentalidades, porque nem toda a gente insere a informação que tem conhecimento, e a informação é poder."	**7.7**
	- "Outra dificuldade do *Paragon* é que temos de ir às instalações da Polícia Judiciária, no Porto. Só temos acesso a esse programa indo lá. O processo, quase diariamente, exige um militar só para ir buscar e ouvir escutas, devíamos ter acesso a isso no nosso gabinete."	**7.8**

N.º	Unidade de Contexto	UR
E5	- "A principal desvantagem quanto aos Núcleos Digitais Forenses é que, para já, os *softwares* são caríssimos, a licença do *Cellebrite* pode custar 5 000€ facilmente." - "E os custos, (…)."	7.9
E6	- "A única restrição/constrangimento existente, tem a ver com a pesquisa de informação criminal nos Sistemas de Informação, dado que esta tem de, obrigatoriamente, estar dependente da existência de uma investigação em curso ou de um NUIPC."	7.6
E7		
E8		
E9	- "(…), quer ao nível de equipamentos em uso, nomeadamente computadores, servidores, velocidades de rede ou largura de banda, que se potenciam negativamente ao nível da mobilidade de utilização em ambiente operacional exterior." - "As principais debilidades ao nível do funcionamento das TIC são, essencialmente, em termos de utilização prática das mesmas, quer ao nível de formação dos investigadores (…)."	7.1 7.3
E10	- "(…) e, ainda, a falta de meios técnicos para a sua sustentação." - "O SIIOP, base de dados que tem por finalidade organizar e manter atualizada a informação necessária ao exercício da atividade da GNR, não é alimentado pela vertente da criminalística."	7.1 7.6
E11	- "(…) e necessitam de ser constantemente renovados/atualizados (…)."	7.9
E12	- "(…) existem tecnologias que nos permitiriam melhorar a eficácia operacional em termos de investigação (por exemplo, uso de localizadores)." - "Na área da Análise de Informação Criminal, existem importantes ferramentas de *software* que facilitavam o trabalho e nos ajudariam a antever os fenómenos." - "Nesse aspeto, a melhor das tecnologias é a existência de recursos humanos em número suficiente e essa é, sem dúvida, uma das maiores debilidades da Investigação Criminal (…)." - "(…) a nível das Unidades não existem licenças de *software* nesta vertente."	7.1 7.2 7.4
E13	- "As principais desvantagens, para qualquer das vertentes de IC e no âmbito das Tecnologias de Informação, prende-se com a necessidade de manutenção de licenças."	7.4
E14	- "Existem demasiadas bases de dados, sem ligação entre si, obrigando o investigador e o analista, a um sem número de pesquisas pelo mesmo assunto em diversas plataformas (…)." - "(…) e com diferentes credenciações."	7.5 7.6
E15	- "As tecnologias que temos disponíveis não têm capacidade para dar, neste momento, uma resposta adequada às nossas necessidades operativas." - "À exceção de alguns *softwares* pontuais, existem licenças que não têm sido adquiridas. As que são disponibilizadas não apresentam a totalidade das capacidades que o *software* fornece, o que constitui uma grande debilidade."	7.1 7.4

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

Quadro n.º 19 - Análise de conteúdo da Questão n.º 8

N.º	Unidade de Contexto	UR
E1	- "Não nos dão resposta a todas as necessidades operacionais que nós temos, não. O investimento do orçamento da Guarda todo que existe, apenas uma pequena percentagem vai para investimento. (…) eu tenho um SIIOP-G que, de facto faz a georreferenciação de todos os crimes, mas está com um *delay* de 1 mês, quando eu precisava daquilo ao momento. Assim que era carregado o crime, assim que era feito o primeiro registo no SIIOP-P, automaticamente haver uma migração para o SIIOP-G, e aparecer logo."	8.2
E2	- "Não. Para haver uma uniformização e para os sistemas serem compatíveis, é fundamental que as Unidades nos reportem aquilo que estão a utilizar, aquilo que pensam evoluir, que é para nós compilarmos tudo e monitorizarmos tudo o que são equipamentos que devem ser atribuídos à estrutura da Investigação Criminal. Isso é um trabalho que já se começou a fazer, inclusive com a aplicação LPIEFSS, já pensando de 2022 a 2026."	8.2

N.º	Unidade de Contexto	UR
E3	- "Dão. Contudo deveria existir maior investimento nesta área, apostando em equipamento digital e programas de análise de informação criminal, bem como dotar os Núcleos Digitais Forenses de equipamentos necessários para a extração e tratamento da prova digital."	**8.1**
E4	- "Não. Nós estamos com um atraso imenso relativamente às outras polícias. Então se formos para a questão do *Crime Mapping*, é décadas de atraso. Não existe uma metodologia, não há uma estratégia como se vê noutros países. Se formos ver o caso de Inglaterra, vê-se todas as polícias inglesas que utilizam *Intelligence Led Policing*, que tem uma determinada estrutura de atuação, de controlo, de monitorização. Nós devíamos ter a capacidade de analisar e de começar, efetivamente, a prever."	**8.2**
E5	- "Considero que sim, em termos de Tecnologias da Informação evoluímos imenso nos últimos anos. Basta comparar as potencialidades do SIIOP antigo com o este SIIOP-P. Claro que ainda não é o ideal, mas está a melhorar e temos que continuar a investir na formação."	**8.3**
E6	- "De uma forma genérica, penso que sim. Havendo sempre espaço para melhorar, considero que foi dado um importante passo ao definir os objetivos e as medidas constantes na Estratégia da Guarda 2020, e que agora estão a ser revisitados e reformulados para a Estratégia da Guarda 2025, bem como as intenções materializadas em sede de Plano de Atividades."	**8.3**
E7		
E8		
E9	- "Existe um esforço materializado na aquisição e desenvolvimento de ferramentas e processos tecnológicos direcionados à estrutura da Investigação Criminal que deve continuar a ser desenvolvido em consonância com a Estratégia Institucional."	**8.3**
E10	- "Não. Em termos de linhas mestras de atuação, o *Intelligence-Led Policing* parte do princípio que a dinâmica e a mutualidade do meio criminal pode constituir-se como uma vantagem para as entidades policiais, uma vez que as ações conduzidas com base nas informações trabalhadas podem conseguir mudar e influenciar o meio ambiente; é suposto que a informação trabalhada seja capaz de influenciar aqueles que decidem e exige que as chefias tenham a capacidade e o empenho para usar aquela informação na escolha da ação de combate à criminalidade, visando um impacto positivo no ambiente criminal."	**8.2**
E11	- "Tendo como fundação a estratégia das TIC espelhada no documento "Estratégia TIC 2020 - Estratégia para a Transformação Digital na Administração Pública", bem como o Plano Sectorial TIC do MAI, e no sentido de prosseguir uma política de rentabilização de recursos TIC de uma forma sinérgica e alicerçada em soluções integradas que prestam serviço a todas as entidades, no âmbito das Tecnologias de Informação e de Comunicação que servem de suporte a toda a atividade, têm sido pensadas diversas medidas de inovação técnica e de processos com suporte TIC. Vêm permitir a melhoria da interoperabilidade e integração dos módulos do SIIOP e a criação de uma capacidade de geração de indicadores preditivos, (…)."	**8.3**
E12	- "Não, porque algumas estão obsoletas e outras são inexistentes ou não foram ainda adquiridas."	**8.2**
E13	- "Parcialmente sim. Foram disponibilizadas licenças para as Tecnologias de Informação, foram adquiridos alguns recursos de parque informático e os Sistemas de Informação têm vindo a ser atualizados. Por outro lado, efetuaram a desmaterialização de atos e procedimentos administrativos."	**8.1**
E14	- "Não, na medida em que não se prevê que sejam concretizáveis, face aos constantes cortes na despesa e desinvestimento na Investigação Criminal."	**8.2**
E15	- "São parcialmente adequados. A Investigação Criminal não tem sido esquecida. Apesar de haver uma preocupação das medidas adotadas neste âmbito, deveria haver muito mais investimento e não tem vindo a ser o necessário. Há previsão por parte, quer dos NAIIC, quer dos NAO, e temos vindo a assistir a algum desenvolvimento e, portanto, são adequados, em certa medida."	**8.1**

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

Quadro n.º 20 - Análise de conteúdo da Questão n.º 9

N.º	Unidade de Contexto	UR
E1	- "Os diferentes Sistemas de Informação estarem interligados, isso é a questão. Neste sentido, para obter uma informação não ter que recorrer a uma multiplicidade de Sistemas de Informação. O que acontece é que eu neste momento tenho o SIIOP-P, por exemplo, já ligado ao *Schengen*, já obtenho análise de informação, mas não está ligada a outros sistemas. O que acontece é o seguinte: eu para aceder à informação tenho de ir a um sistema e depois vou ver ao SIIOP-P, de seguida tenho de ir ver ao TMENU, depois vou ter que ir ver ao I24-7, depois tenho que ir ver ao SEGURNET, e por aí fora. É uma perda de tempo imensa."	**9.1**
	- "Termos mais tecnologias, mais *softwares*, em função daquilo, dedicados a determinado tipo de análise."	
	- "Adicionalmente, dentro das Tecnologias de Informação, a própria Instituição ter a capacidade para adquirir um conjunto de ferramentas atuais, que nos permitissem analisar grandes quantidades de dados, em simultâneo, ao nível das necessidades das diversas Unidades."	**9.2**
	- "(…) e é preciso investir na formação. Os recursos humanos ainda não têm os conhecimentos técnicos para ser um perito, digamos assim, em QGIS. Quem diz no QGIS, diz no i2, diz nas várias ferramentas que existem."	**9.5**
	- "(…) temos carências ao nível de recursos humanos, em quantidade e qualidade. É preciso investir (…)."	**9.6**
E2	- "(…), é havendo uma centralização de informação (…)."	
	- "Praticamente aquilo que está a ser partilhado na PIIC são as situações que já terminaram. Só quando o inquérito já terminou é que se tem colocado tudo na PIIC, (…). Deveria existir uma plataforma que permitisse fazer logo este *hit* interno da Guarda, ou então, até em conjugação com tudo aquilo que depois estava nesta plataforma do Ministério da Justiça ou da Procuradoria Geral da República, fizesse estes *hits*."	**9.1**
	- "(…) mas não existe, digamos assim, um SIIOP-IC, dedicado à Investigação Criminal. É claro que no SIIOP são inseridos todos os autos de notícia. Porém, as outras diligências criminais, e as outras fases que estão para ser desenvolvidas, não estão a ser inseridas no SIIOP-P, mas esta solução para a Investigação Criminal está em fase de estudo e proposta."	**9.3**
	- "Portanto, é necessário, efetivamente, ao mesmo tempo que a Guarda desenvolvesse a capacidade e a confidencialidade de ter todas as peças processuais numa plataforma, esta estar ligada aos magistrados."	**9.4**
E3	- "Estabelecer Sistemas de Informação comuns a todas as policias, onde todos teriam o dever de alimentar, mas também de aceder, obviamente respeitando o princípio da necessidade do saber."	**9.1**
	- "Para além disto deveriam ser introduzidas melhorias na rede e aquisição de equipamentos digitais e programas de análise de informação criminal, (…)."	**9.2**
	- "(…) a par de uma aposta na formação contínua dos recursos humanos."	**9.5**
E4	- "Era importante que todas as polícias tivessem uma plataforma comum e que houvesse comunicação direta. Mas não, o que acontece é que toda a gente tem a sua plataforma. Deveria toda a informação que é inserida no Sistema de Informações de cada entidade, transitar diretamente numa plataforma centralizada."	**9.1**
	- "(…), a grande questão era termos, efetivamente, um programa de *Crime Mapping* com o potencial deste século. Permitir-nos-ia olhar o que é a prevenção, através de novas modalidades de patrulhamento e ao nível da Investigação Criminal Operativa."	
	- "Temos de ter em atenção que os criminosos utilizam as tecnologias num apoio perfeito à sua atividade criminosa. Há programas que nos permitem ter determinadas soluções tecnológicas, por exemplo, de extração de dados. Custam dinheiro, custam, mas tem de se investir."	**9.2**
	- "(…) nos últimos anos para a Investigação Criminal, tem sido muito pobre em termos da formação, em termos de investimento de militares."	**9.5**
	- "(…) estamos com dificuldades em acompanhar porque não temos militares, (…)."	**9.6**
E5	- "A principal melhoria a implementar ao nível interno, era a interoperabilidade do SIIOP antigo com este SIIOP novo."	**9.1**
	- "(…) se não for um computador com capacidade, não conseguem fazer o seu trabalho porque é uma tecnologia que já está ultrapassada. Investiram inicialmente, mas é preciso mais equipamento. No nosso caso, o militar devia ter dois computadores e só tem um (…)."	**9.2**

N.º	Unidade de Contexto	UR
E5	- "(…) procurar não só na descrição sumária, mas em todas as peças processuais que se encontram no sistema, (…). Por exemplo, inquirições de testemunha que tenha dado num processo (…)."	9.3
	- "Outra coisa importante é a formação. É extremamente importante continuar a formar, dar formação aos militares, investir nessa área porque as Tecnologias de Informação estão sempre a evoluir."	9.5
	- "(…) investimento em meios humanos, precisamos de mais pessoas a tratar da informação."	9.6
E6	- "A Investigação Criminal tem a necessidade de operar uma plataforma informática, integrada ou não no SIIOP-P, de acesso muito restrito, onde seja possível não só carregar e elaborar as peças dos inquéritos, mas também registar todas as diligências, relatórios, exames, perícias e demais meios de obtenção de prova. Deverá ter a capacidade de elaborar o registo da Criminalística e a Cadeia de Custódia da Prova e, também, deverá incluir todos os produtos da análise de informação criminal. A esta plataforma ou solução (ainda em fase embrionária de estudo) temos dado a designação de SIIOP-IC."	9.3
E7	- "Continuar a trabalhar para centralizar o registo da atividade operacional no SIIOP. Desta forma a informação produzida numa região do país é automaticamente visível por outros elementos da GNR, noutra região do país permitindo, mais facilmente, combater a criminalidade itinerante. Melhorar, portanto, a interoperabilidade entre o SIIOP e outros sistemas internos e externos à Guarda."	9.1
	- "Dar mais capacidade tecnológica centralizada às Unidades, especialmente aos Comandos Territoriais."	
	- "Implementar mecanismos de *Business Intelligence* policial, para conseguir correlacionar muitos dados e permitir encontrar padrões criminais, que até agora possam estar despercebidos."	9.2
	- "Assim é necessário um continuado esforço, em todos os escalões, para que os dados sejam bem tipificados e corretamente introduzidos no SIIOP."	9.6
E8	- "(…) a integração dos submódulos do SIIOP, em funcionamento, ou seja, a centralização no SIIOP-P, dos diversos submódulos, como por exemplo, das áreas ambiental, fiscal e do domínio da gestão das ocorrências."	9.1
	- "Depois, também, está em curso o desenvolvimento do chamado SIIOP 3.0. Portanto, implicará a integração de todos estes submódulos e será uma aplicação que ganhará capacidade em termos de registo, análise e de tratamento da informação."	
	- "Paralelamente, considero essencial desenvolver e aprofundar o conjunto de ferramentas de análise e de pesquisa (…)."	9.2
E9	- "Face às novas práticas criminais, seria de extrema utilidade a renovação do material informático, (…)."	9.2
	- "Aliado a isto, deveria também ser realizado um esforço na aquisição de novas ferramentas informáticas em termos de *software*."	
	- "(…) bem como uma aposta forte na formação dos militares da estrutura da Investigação Criminal na Guarda."	9.5
E10	- "(…) possibilitar a integração de informação dos sistemas já existentes na GNR, mas também informação proveniente de fontes externas que se revelassem relevantes à atividade da GNR. Relativamente à consulta de Sistemas de Informação era importante a criação de uma ferramenta de consulta única as diferentes bases de dados."	9.1
	- "Ao nível das Tecnologias de Informação na Investigação Criminal, a introdução de uma plataforma de gestão e tratamento da informação, com base nos exemplos de soluções de *Big Data* constitui-se como um potencial aliado à prossecução das missões atribuídas à GNR, desde que estas sejam implementadas segundo modelos planeados e adaptados à instituição."	9.2
E11	- "Melhoria da interoperabilidade e integração dos submódulos do SIIOP."	9.1
	- "Criação de uma capacidade de geração de indicadores preditivos, baseados nos dados do SIIOP e outras fontes externas, capaz de indicar padrões para apoiar o planeamento operacional, bem como disponibilizar o ponto de situação num formato tipo *dashboard*, suportado numa *Datawarehouse* e em mecanismos de *Business Intelligence*."	9.2
E12	- "A criação recente dos Núcleos Forenses Digitais nas Unidades e as ferramentas que estas equipas possuem, são um bom exemplo de uma melhoria implementada e a reforçar no domínio da Investigação Criminal."	9.2
E13	- "(…) interoperabilidade entre Sistemas de Informação (redução do número de pesquisas e do tempo "perdido") e desburocratizar as trocas de informação a nível internacional."	9.1

N.º	Unidade de Contexto	UR
E13	- "(…) acessos a ferramentas OSINT relevantes, (…)."	9.2
	- "(…) qualificação dos recursos humanos e formação especializada nas Tecnologias de Informação disponibilizadas, (…)."	9.5
E14	- "Deve ser criada a interligação entre as várias aplicações, como a integração dos vários SIIOP, por exemplo, garantindo que, com menos pesquisas, se obtém informação mais célere e fiável."	9.1
	- "Os meios tecnológicos não são adequados à exigência da função."	9.2
	- "A formação complementar e de atualização não existe, ou é muito esporádica."	9.5
E15	- "É necessário mais investimento em Tecnologias de Informação, quer *hardwares*, quer *softwares*. Não tem existido, nos últimos anos, aquisição de meios que são necessários."	9.2
	- "Estando em fase de desenvolvimento uma plataforma de Investigação Criminal, é importante existir uma plataforma que possa agregar todo o trabalho desenvolvido pela Investigação Criminal, tendo em atenção o respetivo acesso à informação. E essa plataforma deveria ser pensada em conjunto com a Autoridade Judiciária, tendo apenas acesso à informação, quem dela necessita."	9.3
	- "(…) e formação dos militares."	9.5
	- "E não há efetivo suficiente para reforçar os Núcleos. De nada serve ter muitas tecnologias, se não tivermos militares para retirar as suas potencialidades."	9.6

Fonte: Elaboração própria, com base nas entrevistas confirmatórias

ANEXOS

ANEXO A - ORGANOGRAMA DA GUARDA NACIONAL REPUBLICANA

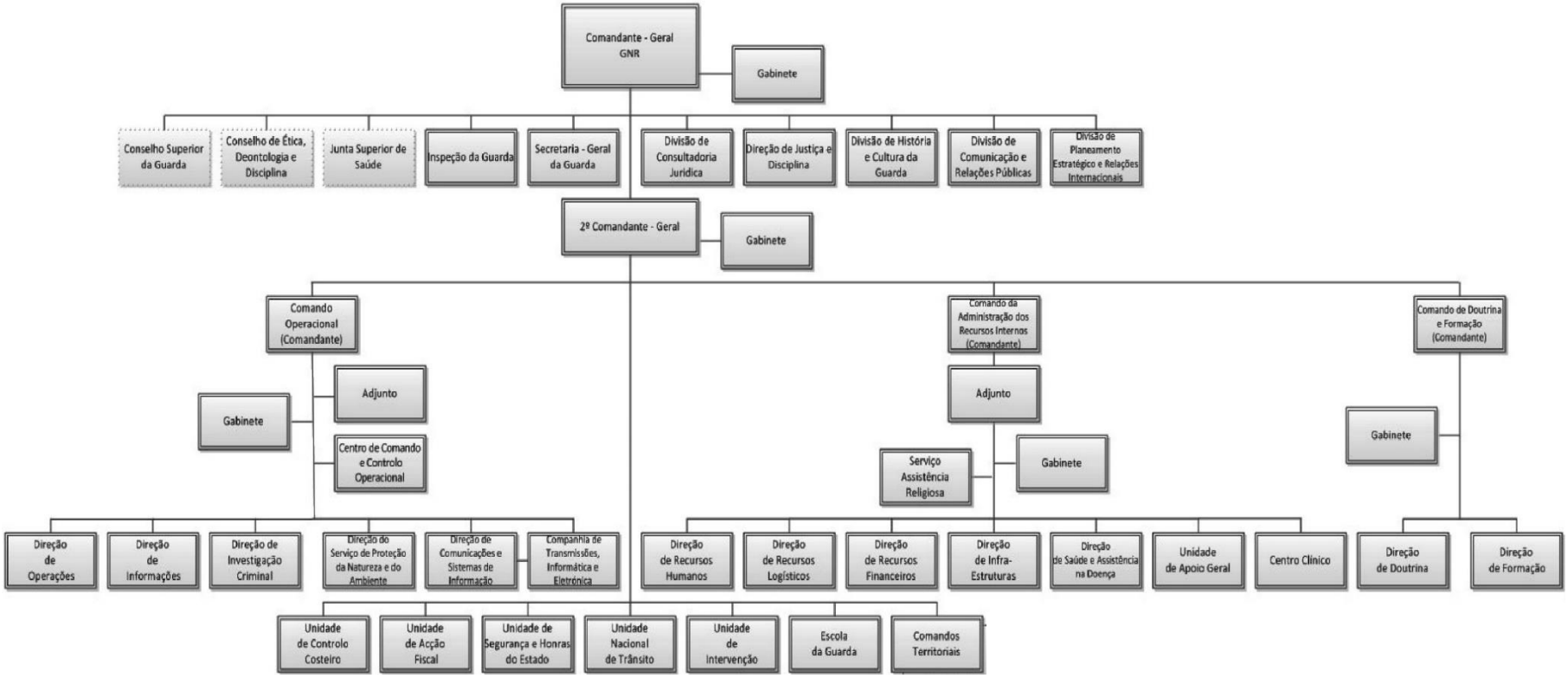
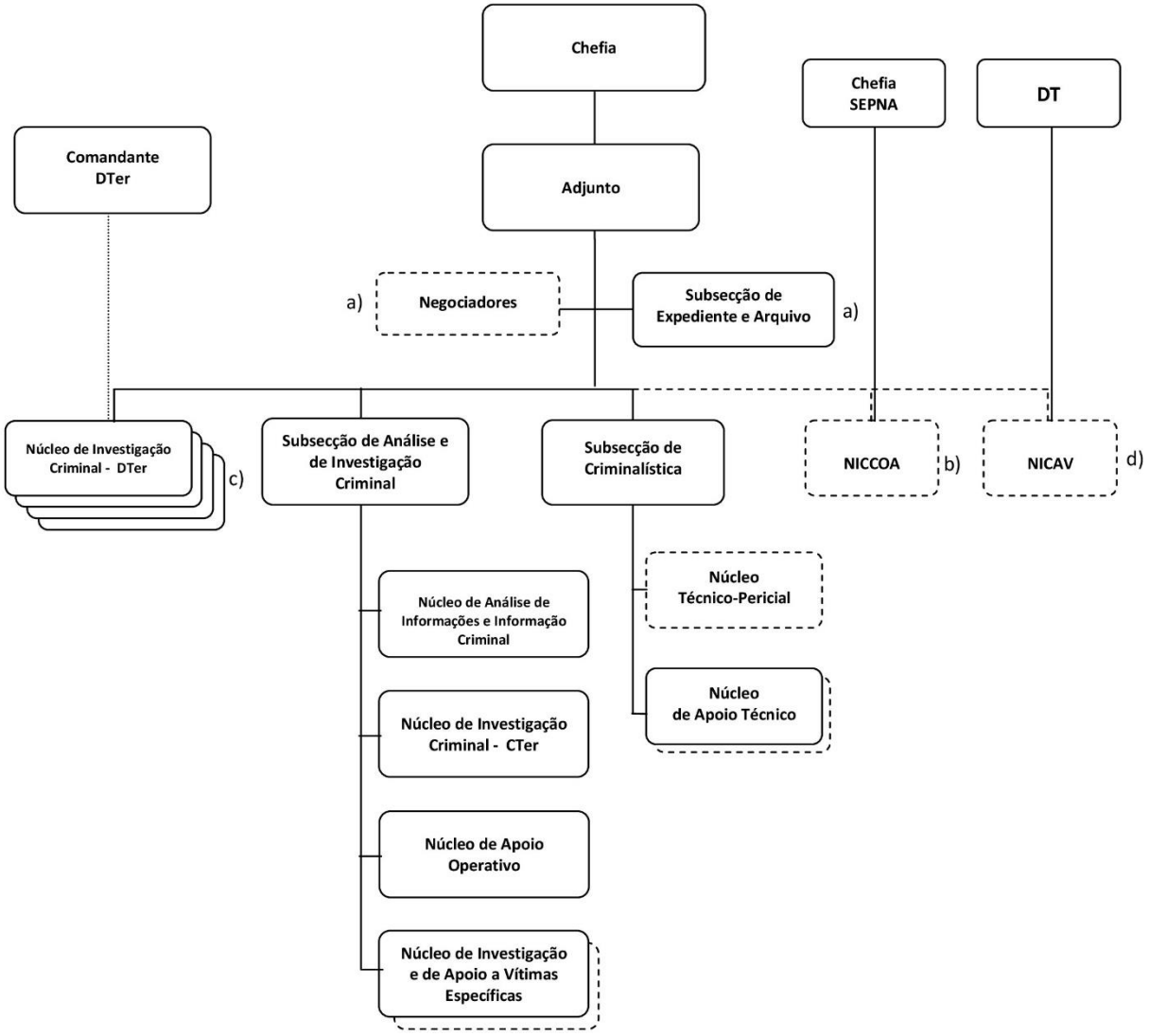


Figura n.º 6 - Organograma da GNR

Fonte: (GNR, 2019c)[118]

[118] Cf. https://www.gnr.pt/imagens/Organigrama_GNR.pdf disponível em 17 de março de 2020, às 15h41m.

ANEXO B – ORGANOGRAMA DA SECÇÃO DE INFORMAÇÕES E INVESTIGAÇÃO CRIMINAL DO CTER TIPO I

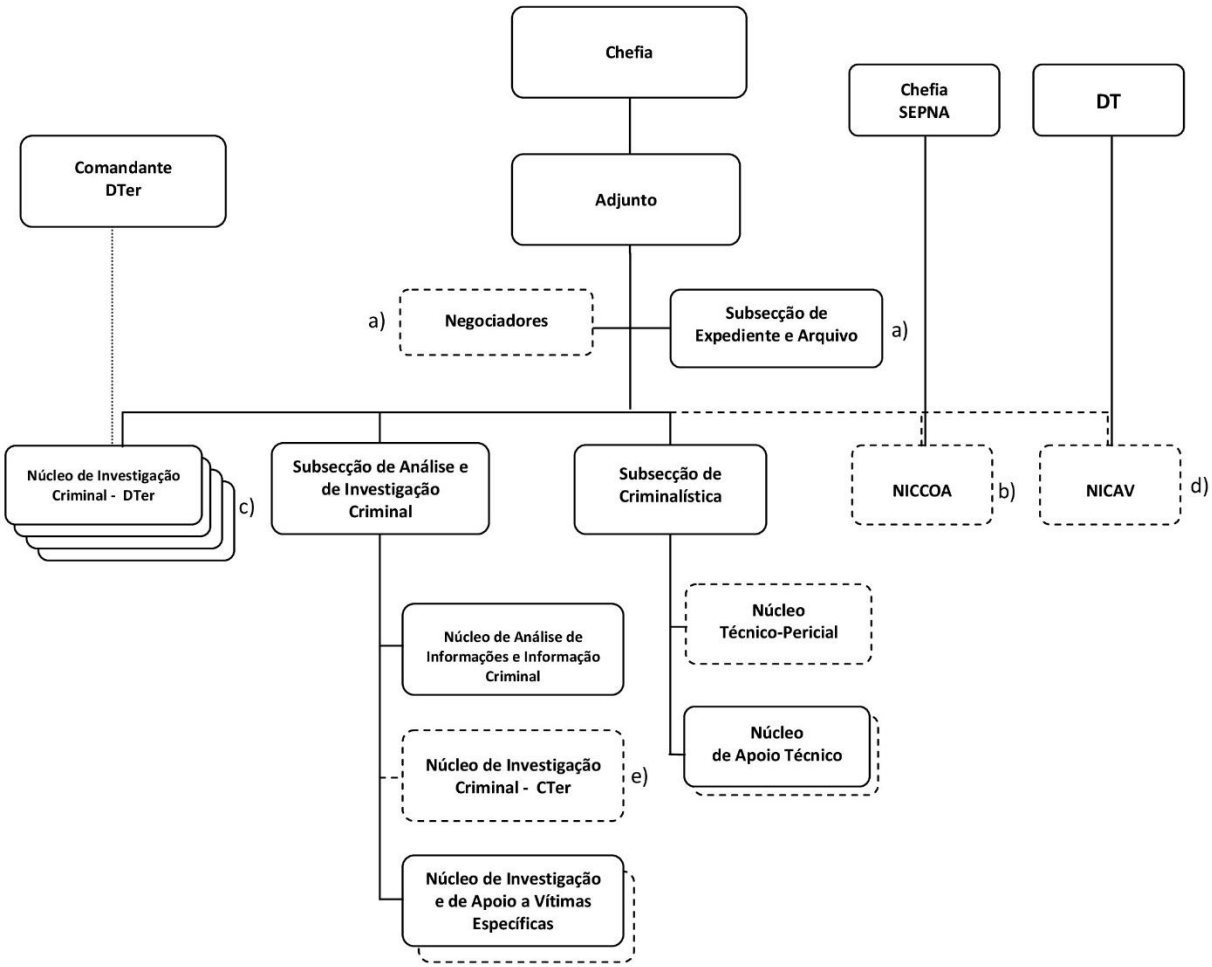


a) Em regime de acumulação funcional
b) Dependência técnica do Chefe da SIIC e funcional do Oficial SEPNA
c) Sob comando administrativo-logístico do Cmdt DTer
d) Dependência transitória até implementação da nova estrutura orgânica

Figura n.º 7 - Organograma da SIIC - CTer Tipo I

Fonte: (GNR, 2014, p. 26)

ANEXO C – ORGANOGRAMA DA SECÇÃO DE INFORMAÇÕES E INVESTIGAÇÃO CRIMINAL DO CTER TIPO II/III



a) Em regime de acumulação funcional
b) Dependência técnica do Chefe da SIIC e funcional do Oficial SEPNA
c) Sob comando administrativo-logístico do Cmdt DTer
d) Dependência transitória até implementação da nova estrutura orgânica
e) NIC eventual, a constituir para crimes de maior gravidade, complexidade ou dispersão que ocorram dentro da ZA da CTer, ou que justifiquem a gestão concentrada da investigação

Figura n.º 8 - Organograma da SIIC - CTer Tipo II/III

Fonte: (GNR, 2014, p. 35)

ANEXO D – SEGURANÇA DA INFORMAÇÃO: TRANSCRIÇÃO PARCIAL DA FICHA DE PROCEDIMENTOS N.º 1/2020 – GNR (CO/DI)

1. FINALIDADE

No âmbito da segurança da informação, considerando a transmissão da mesma através do Sistema de Gestão Documental (SIIOP-D), correio eletrónico e redes sociais, identificar os procedimentos, assim como recomendações ao Dispositivo quanto à utilização das diversas plataformas, com especial relevância para os documentos classificados.

2. ANÁLISE

a. Informação Classificada

(1) A Informação Classificada, designa qualquer informação, material ou documento, independentemente da sua forma, natureza e meios de transmissão, à qual tenha sido atribuída uma marca e um grau de classificação de segurança e que requeira proteção, cuja divulgação ponha "em perigo interesses fundamentais do Estado Português", como tal definido no n.º 6 do artigo 316.º do Código Penal;

(2) Para garantir a proteção da Informação Classificada são identificados os graus "MUITO SECRETO", "SECRETO", "CONFIDENCIAL" e "RESERVADO", obrigando à credenciação das pessoas para o seu manuseamento;

(3) O Sistema de Segurança Eletrónica da Informação (SEIF) é o Sistema de gestão documental atualmente implementado e utilizado na GNR para Gestão da Informação Classificada, o qual está acreditado pela Autoridade Nacional de Segurança (ANS), para a transmissão de informação classificada até:

(a) Grau "SECRETO" na marca "NACIONAL"; e

(b) Grau "CONFIDENCIAL" nas marcas "NATO" e "EU".

(4) O "Truecrypt" é um "Sistema" de encriptação, o qual não está acreditado pelo Gabinete Nacional de Segurança (GNS). Logo, não poderá ser utilizado para encriptar informação "suscetível de causar dano aos interesses fundamentais do Estado", cujo grau seja "CONFIDENCIAL" ou superior. Porém, poderá ser utilizado para encriptar informação "RESERVADA", para difusão a órgãos que se encontram fisicamente distantes, sendo difícil serem servidos em tempo por mensageiro.

b. Informação "Sensível"

(1) Informação não classificada, "que não seja suscetível de causar dano aos interesses fundamentais do Estado";

(2) O "Truecrypt" poderá ser utilizado para encriptar a informação "sensível", a par da informação "RESERVADA".

c. Gestão de Informação Classificada e "Sensível" em SIIOP-D e Correio eletrónico

(1) O SIIOP-D é um sistema de gestão documental e de processos que englobam as funcionalidades de arquivo, gestão do ciclo de vida dos documentos e gestão processual, equiparado;

(2) O SIIOP-D e o correio eletrónico, funcionando sobre a RNSI, rede que tem acesso à internet, não poderá ser acreditado para a transmissão de informação Classificada.

3. PROCEDIMENTOS

b. Registo da Informação

Toda a documentação deve ser registada no SIIOP-D, para uma gestão documental centralizada, sendo que os documentos com classificação de segurança de grau "CONFIDENCIAL" ou superior deve apenas constar no assunto a designação "documento classificado" e onde está arquivado, não sendo feita qualquer menção ou referência ao assunto do documento.

c. Circulação da Informação

(2) O SIIOP-D e o correio eletrónico não deverão ser utilizados para a circulação de documentos com classificação de segurança de grau "CONFIDENCIAL" ou superior;

(3) Utilizar o "Truecrypt" para encriptar informação "RESERVADA" e informação "sensível", não classificada, para difusão a órgãos que se encontram fisicamente distantes, sendo difícil serem servidos em tempo por mensageiro, podendo nestes casos ser utilizado o SIIOP-D ou o correio eletrónico.

Quadro n.º 21 - Segurança da Informação: Classificação, registo e procedimentos

<table>
<tr><td rowspan="2"></td><td colspan="2" rowspan="2">Classificação da informação</td><td rowspan="2">Registo da informação</td><td colspan="3">Procedimentos de circulação</td></tr>
<tr><td>SIIOP-D</td><td>Correio eletrónico institucional (@gnr.pt)</td><td>Sub-Registo/ Posto de Controlo (SEIF)</td></tr>
<tr><td>MUITO SECRETO NACIONAL</td><td colspan="2" rowspan="4">GESTÃO DA INFORMAÇÃO CLASSIFICADA
1. Legislação da Segurança da Informação Classificada;
2. Normas Técnicas da Autoridade Nacional de Segurança;
3. Instruções para a Segurança Militar – Salvaguarda e Defesa das Matérias Classificadas – SEGMIL 1 e as Normas Complementares ao SEGMIL 1.</td><td rowspan="3">1. SEIF
e
2. SIIOP-D - deve apenas constar no campo “assunto” a designação “documento classificado” e onde está arquivado</td><td colspan="2">Não</td><td>Não</td></tr>
<tr><td>SECRETO NACIONAL</td><td colspan="2">Não</td><td>Sim</td></tr>
<tr><td>CONFIDENCIAL</td><td colspan="2">Não</td><td>Sim</td></tr>
<tr><td>RESERVADO</td><td rowspan="3">SIIOP-D</td><td colspan="2">Sim – se utilizar o “Truecrypt”</td><td>Sim</td></tr>
<tr><td rowspan="2">NÃO CLASSIFICADO</td><td>SENSÍVEL</td><td>Informação não classificada, “que não seja suscetível de causar dano aos interesses fundamentais do Estado”</td><td colspan="2">Sim – se utilizar o “Truecrypt”</td><td rowspan="2"></td></tr>
<tr><td>DIVULGAÇÃO RESTRITA</td><td>Inscrever no documento a referência explicita a que se trata de “informação de acesso restrito à GNR, sendo a sua divulgação não autorizada suscetível de sancionamento disciplinar”.</td><td colspan="2">Sim</td></tr>
</table>

Fonte: (GNR, 2020a)

ANEXO E – ETAPAS DO PROCEDIMENTO CIENTÍFICO

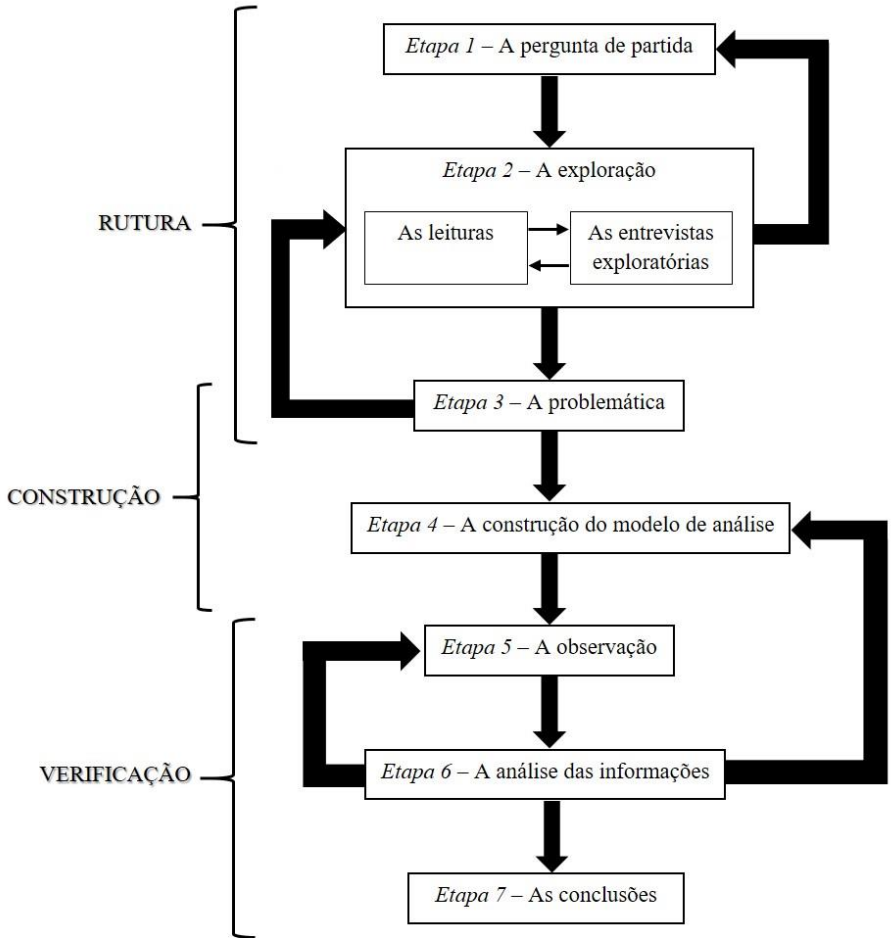


Figura n.º 9 - Etapas do procedimento científico

Fonte: (Quivy & Campenhoudt, 2017, p. 30)

ANEXO F – RELAÇÃO CONCETUAL DA ABORDAGEM QUALITATIVA

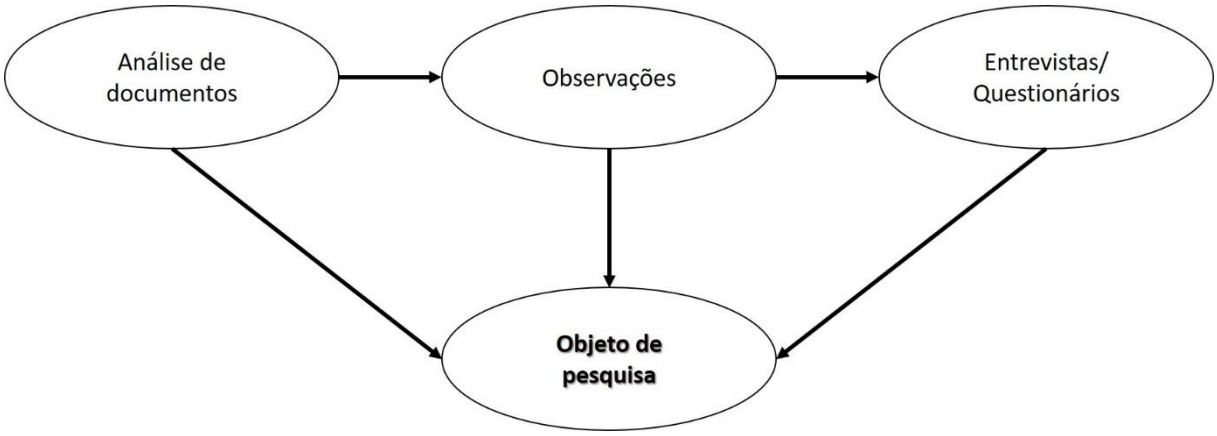


Figura n.º 10 - Relação concetual da abordagem qualitativa

Fonte: (Oliveira, 2011, p. 28)