Instituto Superior de Ciências Policiais e Segurança Interna

Guilherme da Silva

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXV Curso de Formação de Oficiais de Polícia

Importância do Sistema Estratégico de Informação:

Proposta de Implementação na Polícia Nacional de Angola

Orientador:

Superintendente: José Joaquim Antunes Fernandes

Coorientador:

Subintendente: Carlos Alberto Batista Correia

Lisboa, 15 de maio de 2023

Instituto Superior de Ciências Policiais e Segurança Interna

Guilherme da Silva

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXV Curso de Formação de Oficiais de Polícia

Importância do Sistema Estratégico de Informação:

Proposta de Implementação na Polícia Nacional de Angola

Dissertação apresentada ao Instituto Superior de Ciências Policiais e Segurança Interna com vista à obtenção do grau de Mestre em Ciências Policiais

Estabelecimento de Ensino: Instituto Superior de Ciências Policiais e Segurança Interna

Curso: XXXV CFOP

Orientador: Superintendente, Prof. Doutor José Fernandes

Coorientador: Subintendente, Mestre Carlos Correia

Título: Importância do Sistema Estratégico de Informação: Proposta de Implementação na Polícia Nacional de Angola

Autor: Guilherme da Silva

Data: 15 maio de 2023

Dedicatória

Ao meu filho, Gui Jr.

Epígrafe

O modo como você reúne, administra e usa a informação determina se vencerá ou perderá.

Bill Gates, 1999

Agradecimentos

A Deus pai todo-poderoso por toda a proteção e orientação ao longo da minha formação.

Aos meus pais, Alberto Silva e Maria Fernanda, por me ensinarem o caminho da justiça e da dedicação.

À minha mana querida Joana Telma da Silva, por todo amor que tem por mim.

À minha família, amigos e colegas de trabalho, agradeço o apoio incondicional demonstrado ao longo das várias etapas deste curso. A sua presença, apoio e consideração tiveram para mim um valor inestimável.

Ao Superintendente José Fernandes e Subintendente Carlos Correia, meus orientador e coorientador, pela disponibilidade, orientação e sugestões concedidas, que muito contribuíram para o resultado deste trabalho.

Ao senhor Inspetor Nacional da Polícia de Segurança Pública, Pedro Clemente, por toda atenção, contributo e disponibilidade na elaboração da presente dissertação.

Aos Chefes Matias, Anabela, Ana Robalo e aos Agentes Afonso, Teixeira, Espalha, Fonseca, Helena e Perfeito, pela amizade e simpatia.

Um agradecimento aos docentes e ao pessoal do quadro orgânico do Instituto Superior de Ciências Policiais e Segurança Interna, pelo mérito do serviço que prestam em prol da nobre causa da formação dos Oficiais da Polícia de Segurança Pública, da qual tive a oportunidade e a honra de usufruir.

Aos meus colegas do XXXV CFOP, quero também dirigir uma palavra de apreço e consideração, pelo espírito de companheirismo e entreajuda manifestados ao longo desta formação.

Dedico um agradecimento especial ao Comando Provincial de Luanda e à Direção de Estudos e Planeamento da Polícia Nacional de Angola, ao Instituto Superior de Ciências Policiais e Criminais Serra Van-Dúnem, pela colaboração e disponibilidade prestadas através das entrevistas, esclarecimentos e indicações concedidas no âmbito do presente trabalho.

Um agradecimento ao Comissário Sandundo, por todo auxílio e colaboração prestada na elaboração da presente dissertação.

O meu reconhecimento dirige-se ainda aos Oficiais, Técnicos Superiores, Chefes e Agentes que colaboraram neste estudo.

Agradecimento especial à Francisca e Costa, por toda a Camaradagem durante a trajetória académica.

Finalmente, um agradecimento ao meu filho Gui Jr., por representar o núcleo de toda a minha motivação.

A todos o meu muito obrigado.

Resumo

As novas ameaças têm exigido das forças e serviços de segurança uma constante adaptação de modo a que estas possam preveni-las ou neutralizá-las eficazmente. No contexto tecnológico, esforços têm vindo a ser feitos no sentido de acompanhar as novas tendências e aplicar no seu leque de competências ferramentas que possam tornar eficiente a sua atividade. O sucesso das operações policiais dependem em grande parte, da partilha e disponibilidade da informação. Neste âmbito, os sistemas de informações policiais adquirem um papel fundamental, visto que estão presentes em todas as áreas da corporação, configurando-se assim num ativo crítico de informação. Neste estudo procuramos compreender o funcionamento e aplicabilidade do Sistema Estratégico de Informações da Polícia de Segurança Pública e como um sistema de informação melhoraria o trabalho operacional da Polícia Nacional de Angola. Procuramos fazer uma análise do estado atual da Polícia Nacional de Angola, em relação a partilha de informação. Para alcançar as respostas pretendidas recorremos ao método qualitativo, realizando entrevistas aos comandantes municipais do Comando Provincial de Luanda. De forma a complementar a nossa pesquisa, realizámos análise documental, sobretudo na organização e funcionamento desta corporação. Depois de submetida a análise de conteúdo, estes instrumentos permitem-nos perceber a necessidade de um sistema de informação na Polícia Nacional de Angola, bem como a necessidade de mudança do atual quadro desta corporação.

Palavras-chave: Informação; Sistema; Segurança; Polícia Nacional de Angola; Polícia de Segurança Pública.

Abstract

The new threats have required the security forces and services to constantly adapt so that they can effectively prevent or neutralize them. In the technological context, efforts have been made to keep up with new trends and apply tools that can make their activities efficient. The success of police operations depends largely on the sharing and availability of information. In this context, police information systems acquire a fundamental role, since they are present in all areas of the corporation, thus becoming a critical information asset. In this study we seek to understand the functioning and applicability of the Polícia de Segurança Pública Strategic Information System and how an information system would improve the operational work of the National Police of Angola. We sought to make an analysis of the current state of the Angolan National Police regarding information sharing. To achieve the intended answers, we used the qualitative method, conducting interviews with the municipal commanders of the Luanda Provincial Command. In order to complement our research, we conducted a documental analysis, especially on the organization and functioning of this corporation. After undergoing content analysis, these instruments allow us to understand the need for an information system in the Polícia Nacional de Angola, as well as the need to change the current framework of this corporation.

Keywords: Information; National Police of Angola; System; Security; Public Security Police.

Lista de abreviaturas

ARN – Autoridade Reguladora Nacional

APD – Agência de Proteção de Dados

CGPNA – Comando Geral da Polícia Nacional de Angola

CNCS – Centro Nacional de Cibersegurança

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

CSIRT – Computer Security Incident Response Team

DINFOP – Direção de Informações Policiais

EUA – Estados Unidos da América

EUSEI – Equipa Única do Sistema Estratégico de Informações

FAA – Forças Armadas Angolanas

GNS – Gabinete Nacional de Segurança

LPDP – Lei de Proteção de Dados Pessoais (

MININT – Ministério do Interior

NATO – Nort Atlantic Treaty Organization

NPP – Número de Processo de Polícia

NUIPC – Número Único Identificativo de Processo-Crime

OGE – Orçamento Geral do Estado

PCSD – Política Comum de Segurança e Defesa

PESI – Plano Estratégico dos Sistemas de Informação

PMD – Plano de Modernização e Desenvolvimento

PSP – Polícia de Segurança Pública

PNA – Polícia Nacional de Angola

RASI – Relatório Anual de Segurança Interna

RFSEI – Regulamento de Formação do Sistema Estratégico de Informações

SADC – Southern Africa Denvelopment Community

SEI – Sistema Estratégico de Informações

SIOP – Sistema de Informação Operacionais de Polícia

SI – Sistema de Informação

SCOT – Sistema de Contraordenações de Trânsito

SIGAE – Sistema Integrado de Gestão de Armas e Explosivos

TI – Tecnologias de Informação

TIC – Tecnologia de Informação e Comunicação

UE – União Europeia

ur – Unidades de Registo

Índice

Índice de Figuras

Índice de Gráficos

Índice de Tabela

Introdução

O tema que nos propusemos estudar tem uma dimensão interdisciplinar que envolve as Ciências Policiais, Gestão e Direito, relevante à adequação do Sistema Estratégico de Informação (SEI) da Polícia de Segurança Pública (PSP), na Polícia Nacional de Angola (PNA), com a devida adaptação, o que configuraria uma ferramenta útil de gestão para o serviço policial e, ao mesmo tempo, requereria uma modificação legislativa, tendo em conta o contexto angolano. Hodiernamente, o mundo está muito conectado, operando em cadência acelerada e em constante mudança por vivermos em plena era da revolução tecnológica. Essa mesma revolução traz consigo ameaças, quer no ambiente digital, quer nas áreas de soberania nomeadamente segurança interna, defesa, informações e justiça (Elias, 2018).

Zúquete (2021) refere que a segurança dos sistemas de informação não pode ser entendida como a segurança de cada uma das suas componentes isoladas, mas sim como algo que tem uma abrangência maior em termos de políticas e mecanismos, assim a segurança de um sistema distribuído, consiste em subdividir o mesmo em subgrupos de redes e máquinas e enquadrá-los em domínios de segurança, definindo que sujeitos e em que circunstâncias os mesmos podem ter acesso a cada perímetro de segurança, tanto para efeitos de administração como para fins de exploração. Os mecanismos de segurança podem ser barreiras de controlo de acesso presencial ao computador, mecanismo de autenticação eficazes das pessoas que fazem parte do grupo autorizado, mecanismos de registo adequados, eficazes e protegidos (Zúquete, 2021).

O desenvolvimento tecnológico e o uso de ferramentas de elevado potencial por parte da sociedade e organizações portuguesas, motivou a PSP a envolver-se nessa modernização, dada a mais-valia que constitui para a prossecução da atividade policial promovendo a agilização de processos que, por sua vez, contribuem no acréscimo da atividade policial, destacando-se também os critérios de economia, eficácia e eficiência organizacional (Cucu, 2019).

Neste contexto, a escolha do tema foi no intuito de perceber como funciona o SEI e como se adequaria na Polícia Nacional de Angola (PNA), visto que em Angola aumenta cada vez mais o número de furtos, com crescente evidência no furto de viaturas. Infelizmente a PNA depara-se com dificuldades em recuperar as viaturas furtadas sobretudo quando são

transportadas para uma província diferente de onde ocorreu o ilícito (Jornal de Angola, 2022). Com a existência de uma ferramenta como o SEI melhoraria a eficiência serviço policial, na medida que a comunicação de crimes estaria disponível para todos os comandos a nível nacional.

Importa salientar que as redes digitais constituem-se também como um novo ambiente de criminalidade, verificando-se assim uma desterritorialização das ameaças e riscos, fazendo do mundo virtual, uma nova dimensão para expansão das atividades ilícitas, destacando-se aqui os *hackers* que exploram vulnerabilidades nos sistemas e das infraestruturas críticas com objetivos de aceder a dados e/ou causar danos ao sistema de modo a perturbar o seu normal funcionamento (Elias, 2019). Destaca-se, por outro lado, a necessidade de políticas bem definidas e uma vez cumpridas estará facilitada a prevenção de crimes (Jornal de Angola, 2022).

Contexto da Investigação

A PSP é definida, segundo a Lei nº 53/2007, de 31 de agosto, como uma força uniformizada e armada, com natureza de serviço público e dotada de autonomia administrativa, tendo como missão o asseguramento a legalidade democrática, a garantia da segurança interna e dos direitos dos cidadãos, nos termos da constituição e da lei, conforme previsto no artigo 1.º do diploma acima referido. Para além das diversas atribuições partilhadas da PSP, tais como segurança e ordem pública, a prevenção e investigação criminal e a ordenação e fiscalização de trânsito, a PSP tem atribuições exclusivas em todo território nacional (Polícia de Segurança Pública, 2002).

A estrutura organizacional da PSP comporta cinco eixos, nomeadamente: liderança, motivação e comunicação; formação e capacitação física; proximidade, visibilidade e reatividade; imagem institucional; e por último tecnologias de informação e comunicação e capacitação logística. É neste último eixo que vai incidir o nosso trabalho, visto que muitos dos processos produtivos da PSP, quer da sua vertente operacional, quer na logística, estão baseados em ambientes digitais (PSP, 2020). É de extrema importância manter e dotar as áreas operacionais e de suporte dos meios materiais e infraestruturas adequados, dando assim lugar à execução do previsto na Lei de Programação das Infraestruturas e Equipamentos das Forças e Serviços de Segurança do Ministério da Administração Interna. Assim configuram-se como objetivos para alcançar este fim: investir na consolidação do SEI da PSP, adaptando-

o ao princípio da necessidade de conhecer e aceder; investir na consulta do SEI em mobilidade; interligar o SEI e as diversas bases de dados nacionais e internacionais aumentando, nomeadamente, a capacidade de sinalização de suspeitos, viaturas e objetos procurados ou de interesse; reforçar a capacidade de investigar os crimes cometidos em ambiente digital e de ciberpoliciamento (PSP, 2020).

Tecnologicamente, o SEI é executado através de uma aplicação tipo *browser*, sendo que a sua base de funcionamento assenta sobre a *Web*, encontra-se dividido em módulos, que agrupam conjuntos de funcionalidades pertencentes a atividades operacionais da PSP. Esta divisão tem em vista permitir uma maior facilidade de navegabilidade na aplicação e uma melhor compreensão dos conceitos associados a cada funcionalidade disponibilizada. Desta forma, fazem parte dos módulos do SEI: repositório de informação; gestão de ocorrências; gestão dos meios; pedidos das entidades externas; estatísticas e relatórios; investigação criminal; informações policiais, entre outros (Pereira, 2019).

A implementação e desenvolvimento do Sistema de Informação na PSP assenta em grande parte no Plano Estratégico de Informação (PESI 2002) desenvolvido em 2002, do qual tem como expoente máximo o surgimento do Sistema Estratégico de Informação, Gestão e controlo Operacional. Pela necessidade de condensar numa única ferramenta toda a informação o qual suporta o funcionamento da PSP, surgiu assim o SEI, implementado em 2004, que tem sofrido alterações que visam manter esta ferramenta atual (PSP,2021).

A Polícia Nacional de Angola (PNA) é definida como uma força militarizada, uniformizada e armada, com natureza de força de segurança pública, dotada de autonomia operacional, administrativa, financeira e patrimonial, conforme figura no Decreto Presidencial nº 152/19 de 15 de maio, no seu artigo 2º. A PNA configura-se como uma polícia unitária ou monista, por possuir um único corpo de polícia para todo território nacional, o que significa que esta mesma polícia está sob a dependência de um órgão político (Lei nº 6/20 de 24 de março; Claro, 2018).

A inexistência de um Sistema de Informação limita, até certa forma, a atuação da PNA como por exemplo a interligação de fatos ilícitos cometidos em sérié por um mesmo individuo, esta organização policial dificilmente consegue interligar os múltiplos ilícitos com o mesmo agente e, por outra, não existe uma base de dados que possa ser acedida em tempo real sobre todas as ocorrências reportadas tal como acontece no SEI.

Assim, pretendeu-se levar a cabo um estudo exploratório sobre o SEI, sobretudo no módulo de gestão de ocorrências, procurando identificar a sua dimensão e funcionalidades, permitindo desta forma elaborar uma proposta para a PNA.

Objetivos do Estudo

A investigação nas ciências sociais não é feita ao acaso pois o sucesso de um programa de pesquisa depende do procedimento seguido. Importa, acima de tudo, que o investigador seja capaz de conceber e pôr em prática um dispositivo para elucidação do real objetivo (Quivy & Campenhoudt, 2005), uma vez que tais objetivos "originam uma lista de conhecimentos e competências a adquirir" (Sarmento, 2013, p. 13) e que nos permitirão dar resposta à pergunta de partida formulada. Neste sentido pretendemos atingir o seguinte objetivo: conhecer o funcionamento e aplicabilidade do Sistema Estratégico de Informações (SEI). Em termos de objetivos específicos deste trabalho pretende-se: (a) Compreender a importância da segurança cibernética nas organizações; (b) Identificar as principais ameaças a que está sujeito o SEI; (c) Analisar a importância do módulo de gestão de ocorrências como uma valência do SEI; (d) Compreender como o SEI melhoraria o trabalho operacional da PNA.

Estrutura da investigação

No que toca à estrutura da investigação, este trabalho é constituído pela presente introdução, seguida de quatro capítulos, encerrando-se com uma conclusão onde é feito um resumo do trabalho, sendo formuladas as devidas considerações.

No capítulo I, é feita uma contextualização conceptual que reflete o enquadramento sociológico, Política de Segurança dos Sistemas de Informações, Sistema de Informação na PSP, Riscos para os Sistemas de Informação, a Estrutura Orgânica da PNA e as Informações na PNA. No enquadramento sociológico faz-se uma abordagem sistemática do conceito de sociedade e informação. Relativamente à Política de Segurança dos Sistemas de Informações, aborda-se numa primeira fase o conceito de Tecnologia de Informação seguindo-se uma descrição conceptual da globalização da internet.

No capítulo II é feito um enquadramento legal, onde é feita uma abordagem geral dos diplomas legais ao nível da União Europeia e nacional sobre a segurança no espaço virtual. Abordamos também sobre o surgimento do SEI, como são tratados os dados pessoais

dos cidadãos e os módulos que fazem parte deste sistema, por fim falamos sobre a proteção de dados em Angola.

No capítulo III é dedicado ao método, é demonstrada a metodologia usada, o *corpus*, instrumentos de recolha de dados e os respetivos procedimentos.

E por fim, no IV capítulo onde fizemos a apresentação, análise e discussão de resultados do estudo exploratório efetuado no âmbito da importância do SEI. O objetivo do estudo passa por conhecer o funcionamento e aplicabilidade dos SI em geral, e do SEI em particular.

Capítulo I- Contextualização

1.1. Sociedade e globalização

O homem é um ser social cercado de tecnologias, que o circunscreve numa dependência em diversas áreas da sua existência, seja ela biológica, social e cultural. Assim, a vivência humana é marcada por rápidas transformações, vividas numa escala mundial. Com o surgimento da globalização, foram desenvolvidos vários processos que aproximaram os países e os povos, sendo possível o desenvolvimento de multiplicidades de relações muito por conta do rápido desenvolvimento tecnológico das últimas décadas .

Até há poucos anos, os teóricos da comunicação definiam como *mídia* de massa apenas a imprensa, o cinema, o rádio e a televisão. No início da década de 90, os sistemas eletrónicos interativos, baseados em computação e telefonia, eram vistos como os novos meios de comunicação emergentes mas, atualmente, a internet já é tratada como uma nova ferramenta mais abrangente às massas. A rede de computadores que forma a internet saiu das redes em pesquisas de universidades e outras instituições para se tornar um sistema de comunicação que abrange expressivas parcelas da população em grande parte do mundo, o que a transformou em parte da cultura de massa (Silveira, 2004).

A internet é *mídia* com caraterísticas de interatividade radicalmente diferentes dos demais meios de comunicação. O paradigma da comunicação de massa pressupõe um comunicador (emissor) gerando e transmitindo uma mensagem, através de um código, para um recetor com fins de informação, entretenimento, controle, persuasão, etc. Ainda que o comunicador não pressuponha um recetor passivo, este tem relativamente poucas escolhas no momento da comunicação, pois os conteúdos geralmente são pré-determinados e selecionados. Já o modelo de comunicação da internet pressupõe uma interatividade, em que se exige maior atividade do recetor, muitas vezes no próprio momento em que a transmissão está a decorrer. Em alguns casos, o recetor torna-se, simultaneamente, comunicador ou, pelo menos, tem o poder de influenciar o comunicador do próprio instante da geração e transmissão da sua mensagem. Além disso, o recetor pode selecionar a abrangência e a profundidade com os temas tratados (Silveira, 2004)

Atualmente, assiste-se a uma crescente integração técnica e partilha de voz, dados e imagem e a uma significativa redução de custos, resultante das crescentes inovações tecnológicas em curso. Na perspetiva dos cidadãos, cada vez é mais exigente a necessidade

de informação e de comunicação, como fatores de competitividade dos negócios e interligação entre as pessoas (Lopes *et al*, 1998).

A internet interliga globalmente um vasto conjunto de equipamentos que têm em execução aplicações que permitem aos utilizadores a comunicação em rede. Assim, o domínio e a compreensão do funcionamento da internet, dos seus serviços, dos princípios de comunicação e protocolos, constitui uma mais-valia na identificação de ameaças à cibersegurança e na implementação de correspondentes medidas de mitigação (Antunes & Rodrigues, 2018).

O mundo atual é altamente conectado, opera em ritmo acelerado e em constante mudança. O facto de vivermos em plena revolução tecnológica e as transformações da nossa sociedade serem permanentes, tem provocado um enorme impacto na forma como os Estados e as respetivas áreas de soberania, se adaptam ao mundo cada vez mais reticular e desafiador dos paradigmas, cabendo ao Estado a produção de informações sobre a segurança (Elias, 2018). Cabe à administração pública, em relação à segurança, reconduzir as diversas áreas do domínio da previsão e da antecipação de riscos e ameaças, alicerçando assim uma consciência coletiva de serviço público (Feiteira *et al*, 2015). O carácter público da segurança significa que a mesma se tornou um bem a ser garantido a todos os indivíduos, independentemente da posição social que ocupam. Ou seja, é responsabilidade do Estado, uma vez que a ideia de provisão da segurança diz respeito ao controle de comportamentos considerados criminosos, por esta mesma comunidade política, tanto no sentido da vigilância, para que os mesmos não ocorram, como na punição dos indivíduos que os cometem (Barreto, J. M & Barreto, J. M, 2019).

Assim, o ciberespaço é um ambiente virtual ao nível global utilizado para os mais diversos efeitos, desde lazer e partilha de conhecimento, até para a prática de uma vasta panóplia de crimes, para a disseminação de ideologias radicais, que questionam e combatem os sistemas políticos, económicos e sociais vigentes, para a radicalização e recrutamento para o terrorismo, entre muitas outras práticas que questionam a soberania dos Estados e colocam em risco a segurança das comunidades e dos cidadãos (Elias, 2018). Conforme plasmado no Relatório Anual de Segurança Interna de 2022 (RASI/2022) o investimento em cibersegurança tem sido apontado como a melhor estratégia de prevenção, uma vez que continua a verificar-se ataques com grande impacto a estruturas devidamente preparadas. Deste modo, há sempre vulnerabilidades e será necessário identificá-las mitigá-las e criar mecanismos para as conter, tendo consciência de que os principais vetores de ataque são a

exploração das vulnerabilidades das infraestruturas, a extensão/exposição de credenciais e a realização de campanhas de *phishing* que permitem, subsequentemente, a distribuição de *malware*/*ransomware* com técnicas cada vez mais sofisticadas.

Assim, podemos entender como crime cibernético o ato atípico, antijurídico, culpável e antiético, cometido sempre com utilização de *softwares* e *hardware*, para transmissão de dados através da internet, com o objetivo de copiar dados sem autorização, prejudicar outrem, atentar contra a liberdade individual, a privacidade, e a honra, etc. o crime cibernético diferencia-se do crime informático na medida em que este último é entendido como todas as ações típicas, antijurídicas e culpáveis praticados com a utilização de computadores e/ou de outros recursos da informática, o que significa que o crime cibernético é uma espécie do crime informático, uma vez que se utilizam computadores para aceder à internet (Neto, 2009).

Podemos assim afirmar que o reverso da cibersegurança é a privacidade na internet. A falta de privacidade leva a que haja uma exposição desmensurada e um aumento da vulnerabilidade a ataques informáticos. Por outras palavras pode dizer-se que quanto menos privacidade existir na internet maior será a propensão para que possam existir ataques informáticos e se coloque em risco a segurança (Ramos, 2015).

Almeida e Silva (2020) caraterizam o perfil do cibercriminoso como sendo geralmente um individuo, entre 15 e 32 anos, sexo masculino com inteligência acima da média, educado, audacioso e aventureiro, e que sempre alegam o desconhecimento da legalidade cometido movido pelo anonimato oferecido pela internet, tem preferência por ficção científica, música, xadrez, jogos de guerra e não gostam de desportos de impacto. Como o cibercriminoso é aquele que não se apresenta fisicamente e pode agir de qualquer parte do planeta, levam os criminosos a acreditar que estão imunes às leis.

As organizações de criminalidade, geralmente recrutam jovens universitários, engenheiros informáticos e outros peritos em sistemas de informação, procuram como alvo as instituições financeiras, estabelecem alianças com organizações criminosas de tráfico de droga, de armas e de seres humanos, ou transformam-se em organizações que exploram a criminalidade sexual, a pedofilia, as burlas e os tráficos de diversa ordem, visando sobretudo o lucro (Elias, 2018).

Em suma, podemos concluir que a sociedade não é um elemento estático, pois está em constante transformação e, como tal, a sociedade contemporânea encontra-se num

processo de mudança em que as novas tecnologias são as principais responsáveis pelo potencial que apresentam no acesso e na difusão da informação. Este é o novo paradigma de organização e de funcionamento da sociedade contemporânea, a sociedade da informação

1.2. Política de segurança dos sistemas de informações

Entre os avanços tecnológicos preconizados pela humanidade destacam-se, atualmente, as evoluções tecnológicas dos modos de comunicação, que se basearam na digitalização da comunicação, sustentadas em tecnologias de informação e de comunicação (TIC). A disseminação das Tecnologias de Informação e Comunicação, nas organizações sociais e económicas é, como referimos anteriormente, o fenómeno central em que assenta a sociedade de informação (Cucu, 2019).

Hodiernamente, a sociedade da informação carateriza-se pelo uso intensivo de tecnologias de informação e comunicação. Neste sentido muitas instituições empresariais defendem a prevalência da rede, face à hierarquia formal, como o modo organizacional e de obtenção de melhores oportunidades de mercado, destacando também o uso do digital como forma de mediação tecnológica que constituem a infraestrutura básica das organizações.

Destaca-se, neste contexto, a Estratégia para a Transformação Digital na Administração Pública, que condensa a visão do governo na utilização das TIC na Administração Pública, compreendendo iniciativas comuns a toda a Administração do Estado e iniciativas especificas em cada área sectorial (Elias, 2018)

As políticas de segurança de informação associam-se aos mecanismos de segurança, na medida em que a primeira define o foco da segurança e o que deve garantir, e os mecanismos de segurança são tecnologias que permitem pôr em prática a política de segurança. Um domínio de segurança consiste num universo de recursos (máquinas, redes, etc.) e pessoas sujeitas à mesma política de segurança (Zúquete, 2013). De uma forma prática, podemos dizer que se um determinado computador só pode ser acedido por um conjunto restrito de pessoas é uma política de segurança. A definição das pessoas que fazem parte do grupo é também uma política de segurança. É, igualmente, política de segurança se estivermos a considerar o acesso físico direto, presencial ou remoto. Já os mecanismos de

segurança, neste contexto, podem ser barreiras físicas de controlo de acesso presencial ao computador, mecanismos de autenticação eficazes das pessoas que fazem parte do grupo autorizado, mecanismos de registo adequados, eficazes e protegidos (Zúquete, 2013).

O número considerável de equipamentos ligados e a sua heterogeneidade, bem como o número elevado de utilizadores com acesso à internet têm tornado este espaço mais complexo e com necessidade de permanente monitorização. De um modo geral, é possível referir que a internet se tem tornado num espaço cada vez menos seguro para a comunicação e partilha de dados e trabalho colaborativo.

Não seria possível falar de segurança dos sistemas de informação sem abordar o conceito de Tecnologias de Informação, que é definida por Alecrim (2001) como o conjunto de todas as atividades e soluções providas por recursos computacionais que visam permitir a obtenção, o processamento, o acesso, o gerenciamento e o uso das informações. As Tecnologias de Informação surgem como elemento de conceção e suporte da comunicação em atividades que vão desde o simples arquivo de dados e a utilização de programas de *Office Automation,* até ao correio eletrónico e às possibilidades de trabalho à distância. O conceito de Tecnologias de Informações surge enquanto conjunto de conhecimentos, refletidos quer em equipamentos e programas, quer na sua criação e utilização a nível pessoal e empresarial (Sousa, 2009).

Segundo Antunes e Rodrigues (2018) a cibersegurança pode ser entendida como o conjunto de tecnologias projetos e práticas desenhados para proteger as redes, os computadores e outros dispositivos eletrónicos, programas e dados, de potenciais ataques ou ameaças. Importa ainda salientar que o conhecimento do enquadramento histórico da internet e o seu funcionamento contribui para uma melhor compreensão da atividade dos computadores e dos programas na internet, este conhecimento pode potenciar, em certa medida, a mitigação de problemas relacionados com a cibersegurança. Assim, entende-se que a cibersegurança está diretamente relacionada com três aspetos fulcrais, nomeadamente a confidencialidade que está relacionada com a prevenção da utilização não autorizada da informação; a integridade está relacionada prevenção na modificação não autorizada da informação e, por último, a disponibilidade que está relacionada com a prevenção da retenção não autorizada de informação ou recurso (Mamede, 2006).

É também razoável pensar que a utilização da internet, como meio globalmente utilizado para partilha da informação e condutividade dos seus utilizadores, não deveria levar

ao aparecimento de crimes e atividades ilícitas. As inúmeras vantagens, que a internet e os seus serviços trouxeram para a melhoria da qualidade de vida dos seus utilizadores, deveriam ser potenciadas em prol de um desígnio maís abrangente, que seria, neste caso, o bem comum e o desenvolvimento global dos países. Em boa medida, olhando para os 50 anos de internet, é possível referir que este desígnio foi alcançado, tendo provocado um enorme desenvolvimento dos países e da humanidade em geral (Antunes & Rodrigues, 2018).

Contudo, como todas outras áreas, o que é bom e tem enormes vantagens, também revela o seu lado obscuro. O modelo aberto e descentralizado com que a internet foi crescendo e acolhendo todas as pessoas e instituições, não lhes impondo qualquer controlo ao nível de critérios de admissão, permitiu que nela fossem entrando os mais diversos tipos de utilizadores e com as mais variadas motivações. Desde logo, os que passaram a utilizar a internet como meio para agilizarem e melhorarem a forma como realizam as suas atividades profissionais, mas também os que viram na internet um mundo de oportunidade para praticar o mais variado conjunto de crimes. O aumento considerável de transações que passaram a ser realizadas na internet acelerou o aparecimento de novas oportunidades para o crime e para realização de ações ilícitas. Nesta senda, os sistemas judiciários tiveram de ajustar as suas leis à tipologia de crimes que surgiu com a internet. Para o cidadão comum, o conhecimento sobre as leis relacionadas com este tipo de criminalidade significa mais cidadania, mais conhecimento e, em certa medida, mais prevenção e segurança na utilização da internet e dos seus serviços (Antunes & Rodrigues, 2018).

A segurança de uma organização, por exemplo, deve ser analisado num contexto alargado, tendo em consideração as diferentes perspetivas, tais como: dados, operações, aplicações e acesso físico, entre muitas outras. Neste sentido, reflete-se a multidisciplinariedade associada à mesma, tentando-se concertar todas as vertentes que contribuem para a sua implementação. No entanto, assiste-se com frequência à limitação desta abrangência, por parte dos responsáveis de segurança da organização, que se restringe às questões associada à segurança física, sendo a área da informática, quando existe, que decide e implementa as restantes medidas de segurança, sem uma política que reflita os requisitos de negócio, nem tão pouco, procedimentos de auditoria. Ou seja, acaba por não existir um plano único, integrado, de segurança como se toda a parte informática da organização não fosse tão importante ou não contivesse a informação essencial para o negócio, como o edifício que a mesma está situada. E o maior paradoxo desta situação é que a inexistência de um plano integrado de segurança pode levar, por si só, à inexistência de

potenciais lacunas graves. Fazendo uma analogia, podemos colocar a seguinte questão: para quê colocar grades nas janelas de uma casa cuja porta das traseiras é em vidro e não tem qualquer outra proteção? O mesmo se passa com a integração da segurança empresarial como um todo. Apesar da maior tendência ser garantida (Antunes & Rodrigues, 2018).

A globalização da Internet e a sua utilização massiva potenciou, ainda mais, esta necessidade de vigilância das atividades que aí se praticam, tentando assim identificar as que são ilícitas e prever atos criminosos que atentam contra a segurança dos cidadãos e de países. Esta vigilância permanente da internet e a consequente tentativa de impedir a realização de atividades ilícitas e criminosas, levou ao surgimento de uma zona oculta do ciberespaço, onde os recursos não estão intencionalmente indexados, são de acesso difícil e condicionado, a anonimização do utilizador é obrigatória e o seu secretismo é valorizado (Antunes & Rodrigues, 2018).

1.3. Sistema de Informação na PSP

A informação sempre assumiu uma grande importância na atividade policial. Com a evolução da polícia os métodos de tratamento da informação foram melhorados, tornando-se num ativo imprescindível para a atividade policial.

As tecnologias de informação são uma constante no nosso quotidiano e nas mais diversas áreas de interesse, ao ponto de não nos lembrarmos, na indisponibilidade ou na falta delas, de como eram resolvidas e geridas as nossas vidas antes de as integrarmos.

A arquitetura tecnológica implementada na PSP assenta numa estratégia descentralizada de processamento, mas de acesso descentralizado, consubstanciado operacionalmente num Sistema de Informação (SI) designado de Sistema Estratégico de Informação, Gestão e Controlo Operacional, geralmente conhecido como SEI. Para a sua evolução e desenvolvimento tecnológico continua a ser importante assegurar os recursos adequados que permitam dar continuidade às necessidades da atividade operacional e, simultaneamente, à sua evolução dinâmica. A interligação com os sistemas de informação de outras entidades nacionais e com os sistemas de informação policial internacionais, numa perspetiva facilitadora para os utilizadores, simplificando a sua utilização, é essencial. O que

se pretende é que o utilizador tenha apenas de recorrer a esta ferramenta e, através dela, obter o máximo de informação considerada relevante para os fins procedidos pela PSP (Canelas, 2017).

O surgimento do SEI decorredo Plano Estratégico dos Sistemas de Informação (PESI) fruto no continuado processo de modernização da Polícia de Segurança Pública. O grande objetivo do SEI é dotar todo o dispositivo da PSP de um sistema de informação capaz de suportar os seus processos operacionais e que, em simultâneo, seja catalisador da desejada uniformização e racionalização de procedimentos, bem como de uma nova forma de atuar mais eficaz e eficiente (Accenture/PSP, 2004).

O SEI tem respaldo legal no n.º1 do artigo 1.º do Decreto Regulamentar n.º 5/95 de 31 de janeiro, ainda que a sua designação seja Sistema de Informações Operacionais de Polícia (SIOP/PSP).

Estamos, cada vez mais, cativos dos sistemas inteligentes, serviços de conetividade, equipamento de rede e integração de dados, nomeadamente: computadores, tablets, smartphones, entre muitos outros equipamentos que partilham informações e até executam tarefas. A PSP percorreu, nas últimas décadas, um caminho sem retorno com o objetivo de responder a esta realidade. Naturalmente este é um processo em constante mutação e evolução ao qual a PSP terá de se adaptar sob pena de deixar de cumprir a sua missão à luz do patamar de exigência dos cidadãos, cada vez mais elevado (Canelas, 2017).

1.4. Riscos para os Sistemas de Informação

Existem inúmeros conceitos de risco, no entanto a abordagem é demasiadamente focada, mostrando-se insuficiente para o complexo domínio da segurança. O risco, na visão de Torres (2015) não é mais do que o efeito de um evento incerto, seja ele positivo ou negativo, face aos objetivos da organização.

É impossível imaginar as grandes organizações do século XXI, sem os processos informatizados que coordenam as suas atividades. São várias aplicações de sistemas de informação, seja para trabalhar nos registos, análises, planeamento e tomada de decisões em todos os níveis da organização. O objetivo dos sistemas de informação é de orientar a tomada

de decisão nos três níveis de responsabilidade, nomeadamente nível estratégico; tático e operacional (Rodrigues, 2000; Gouveia, 1996)

A era da informação e do conhecimento, associada às novas tecnologias, à ciência e inovação e à globalização, têm consequências enormes no âmbito da segurança, com novos instrumentos de comunicação, novos centros e órgãos de conselho, novos órgãos de gestão e operacionais. (Telo *et al*, 2018).

Um Sistema de Informação é constituído por pessoas, procedimentos e equipamentos que recolhem, processam e distribuem informação com objetivos específicos, sendo que qualquer sistema é constituído por *inputs*, processamento e *outputs*. O Sistema de Informação processa os *inputs* e produz *outputs* que são disponibilizados ao utilizador final ou a outros sistemas. Em algumas situações também tem sido incluído um mecanismo de *feedback* que controla a operação (Lucas *et al*, 2009).

Uma organização depende em maior ou menor grau do seu Sistema de Informação, sendo este responsável pelo fluxo de dados. Um sistema existe com o propósito de alcançar os objetivos a que se propõe, no intuito de alcançar esses objetivos, o sistema interage com o ambiente envolvente (adjacente às fronteiras do sistema). As fronteiras delimitam e comunicam com a área adjacente do próprio sistema. Assim, os sistemas que interagem com o meio envolvente recebendo e produzindo dados são designados por sistemas abertos, por sua vez, o sistema que não interage com o exterior é designado por sistema fechado (Guimarães & Évora, 2004; Gouveia,1996)

Ao longo deste século, as organizações policiais estão sob pressão para institucionalizar a tecnologia da informação. Por um lado, as pressões internas resultam de novos modelos de gestão que colocam maiores exigências à eficiência e responsabilidade. Por outro lado, as pressões externas são caraterizadas pela exigência do público de que as organizações policiais se assemelham a mais burocracias profissionais. (Varano *et al*, 2007)

A missão do Sistema de Informação é de sintetizar, os objetivos e características principais, enquanto ferramenta essencial ao funcionamento da organização a que se destina nas diversas dimensões consideradas, nomeadamente operacionais de gestão e de suporte. Neste sentido, procurou-se que a missão do Sistema de Informação da PSP traduzisse de forma clara o seu foco principal que é a informação e que, simultaneamente, identificasse os atributos essenciais para que os processos definidos para manuseamento dessa informação

suportem de forma adequada a atividade da PSP, conforme as atribuições que lhe estão conferidas por lei (Accenture, 2002).

Os principais aspetos considerados neste enunciado da missão, os quais se consideram essenciais enquanto premissas de base e fundamentais para os futuros sistemas e tecnologias de informação na PSP, são:

- Foco na informação enquanto ativo fundamental da organização que deve ser gerido de forma adequada, independentemente da sua origem (Interna/externa), do seu suporte físico ou dos fins a que se destina;
- Suporte à atividade operacional, envolvendo as áreas nucleares no cumprimento das atribuições cometidas à PSP;
- Atualizações, coerência e integração da informação, garantidos pela existência de repositórios únicos de informação, acedidos diretamente para efeitos de consulta e atualização de dados;
- Informação acessível quando e a quem dela necessita, pela exploração de uma rede de comunicações abrangente e de dispositivos de acesso alternativo;
- Segurança ao nível da rede de comunicação e das transações aplicacionais, imprescindíveis em qualquer sistema de informação policial;
- Suporte à gestão, nomeadamente para a produção de indicadores estatísticos de suporte à decisão e para administração dos recursos financeiros, materiais e humanos da PSP;
- Asseguramento da criação, manutenção e disponibilização da informação necessária e relevante à atividade operacional e de gestão da PSP, garantindo a sua atualização coerência integração e acessibilidade em tempo útil e de forma segura (Accenture, 2002).

Os impactos dos sistemas de informação podem ser dramáticos no ambiente organizacional e podem anular os benefícios potenciais se o processo de mudança organizacional ocasionada pela implementação do Sistema de Informação não for bem conduzido. As mudanças comportamentais ocasionadas pela introdução de Sistemas de Informações, passam a ter um papel preponderante nas discussões referentes aos impactos no ambiente organizacional, aos conflitos advindos da sua implementação e aos efeitos profundos que podem ocasionar em questões como, as referentes a ganho ou perda de autonomia, centralização ou perda dos mecanismos de controle, flexibilidade *versus*

inflexibilidade, criação ou diminuição de poder e conflito de governança (Decoster & Sun, 2014).

Segundo Moresi (2000) a convergência das tecnologias da informação e dos sistemas de informação tem afetado os processos de trabalho das organizações. Assim, antes de implantar qualquer sistema desta natureza, é de vital importância desenvolver uma análise que permita determinar os principais requisitos do projeto. Uma das tarefas críticas de qualquer sistema de informação é a disponibilização da informação correta às pessoas certas e com oportunidade. Cada tomador de decisão, dentro de uma organização, necessita apenas de uma pequena porção de informação para apoiá-lo neste processo. O propósito da atividade de disseminação é determinar as necessidades de informação e disponibilizá-las com oportunidade. Cada vez mais, esta atividade envolve a disponibilização da informação em diferentes formatos.

Em suma os sistemas de informação configuram-se como uma mais-valia para a eficiência no funcionamento de qualquer instituição, sendo que há riscos associados a este desempenho, que vai desde a suscetibilidade a um eventual ataque cibernético, até à resistência à mudança por parte dos colaboradores.

1.5. Estrutura orgânica da Polícia Nacional da Angola

A Polícia Nacional de Angola (PNA) é definida segundo a Lei n.º 6/20 de 24 de março, e Decreto Presidencial n.º 152/19 de 15 de maio, como uma instituição nacional, policial, permanente, regular e apartidária, organizada na base da hierarquia e da disciplina, incumbida da proteção e asseguramento policial do país, no estrito respeito pela constituição e a lei, bem como pelas convecções internacionais de que Angola faz parte. A PNA é uma instituição militarizada, uniformizada e armada com natureza de força de segurança pública dotada de capacidade jurídica, de autonomia operacional, administrativa financeira e patrimonial.

A PNA carateriza-se como uma instituição independente com um orçamento próprio, a partir de doações financeiras globais inscritas no Orçamento Geral do Estado (OGE) e aprovado por despacho conjunto dos Ministros das Finanças e do Interior. Segundo o

disposto no artigo 6.º do Decreto Presidência n.º 152/19 de 15 de maio, esta força de segurança é integral e compreende três níveis de comando: o Comando-Geral, o Comando Provincial e o Comando Municipal.

A Polícia Nacional depende organicamente do Ministério do Interior (MININT), obedecendo à hierarquia de comando a todos os níveis da sua estrutura, segundo o disposto no artigo 3.º do mesmo diploma.

O Comando Geral da Polícia Nacional (CGPN) superintende na administração, preparação, manutenção e emprego das forças da PNA. É dirigido por um Comandante-Geral coadjuvado por dois Comandantes-Gerais adjuntos, um para a Ordem Pública e outro para a área de Proteção e Intervenção, que asseguram a realização das inspeções e visitas de ajuda e controlo aos diversos órgãos da PNA.

O estado atual da PNA revê-se na execução do Plano de Modernização e Desenvolvimento (PMD), em curso desde 2003, que define os principais rumos que a PNA se propõe seguir nos próximos dez anos, num processo permanente de crescimento e aperfeiçoamento dos meios e métodos técnicos de gestão da atividade policial, com base em conhecimento científicos e práticos, para que a corporação se adeqúe às exigências de um Estado de Direito e à democracia, no combate à criminalidade (Neto, 2010).

Com o fim da guerra civil em Angola, alcançaram-se resultados significativos no respeitante à otimização do funcionamento interno da PNA, às medidas de restruturação orgânica em curso, com particular destaque para a criação de divisões de polícia e de Unidades Especializadas, bem como o reequipamento realizado, contribuíram para a melhoria substancial da ação das forças policiais (Neto, 2010).

1.5.1. Estrutura Orgânica Do Comando Provincial de Luanda

A província de Luanda ocupa cerca de 18.815 km^2 do território nacional, possuindo cerca de 7.469.874 de habitantes, o que corresponde a 27% da população do país. A estrutura da Polícia da província de Luanda, que há muito se encontra desajustada face à nova divisão administrativa da província e o grande crescimento populacional (Despacho n.º 044 GAB.CGPNA/2020).

Conforme o Decreto Presidencial n.º 18/16 de 17 de outubro, que altera e cria a nova Divisão Administrativa da Província de Luanda, e o Decreto Presidencial n.º 293/14, de 21 de outubro, que aprova a organização e funcionamento dos órgãos da administração local do Estado, o Comando Provincial de Luanda (CPL) está constituído por 1 Gabinete do Comandante Provincial; 2 gabinetes dos segundos comandantes, 17 Departamentos Provinciais, 9 Comandos Municipais; 5 Unidades de grande porte, 106 Esquadras, 16 Postos Policiais; perfazendo 156 infraestruturas que integram 42.244 efetivos (Despacho n.º 044 GAB.CGPNA/2020).

À luz das transformações operadas na composição estrutural e funcional, o CPL adequa-se à nova realidade, devendo funcionar com quatro níveis de comando, nomeadamente: Comando Provincial; Comando Municipal; Esquadra Policial; Posto Policial, garantindo, dessa forma, uma maior segurança, na base de uma Polícia cada vez mais próxima da comunidade e capaz de resolver as situações de crimes que assolam o cidadão (Despacho n.º 044 GAB.CGPNA/2020).

1.5.2. Informações na Polícia Nacional de Angola

A PNA é a instituição nacional permanente, regular e apartidária, organizada na base da hierarquia e da disciplina, incumbida da proteção e asseguramento policial do país, no estrito respeito pela Constituição e pelas leis, bem como pelas convenções internacionais de que Angola seja parte (art.º 210.º, CRA).

A PNA é constituída por serviços e unidades territoriais, que atuam em todo território nacional sob a direção de um Comandante-Geral, que é simultaneamente, o órgão máximo da instituição que responde diante do Presidente da República, e o responsável da PNA diante do Ministro do Interior pelas atividades da Polícias em todos os seus domínios (art.º 8.º do DP n.º 152/19, de 15 de maio).

Nos termos do artigo 24.º, do Decreto Presidencial n.º 152/19, de 15 de maio, que aprova o Estatuto Orgânico da Polícia Nacional de Angola, foi criada a Direção de Informações Policiais (DINFOP), órgão que tem a incumbência de planificar, pesquisar, recolher, centralizar, analisar, classificar, disseminar e coordenar todo o sistema e circuito

de produção de informações de interesse policial, visando auxiliar o processo de tomada de decisão (Direção de Informações Policiais, 2020).

Segundo o Despacho n.º 034/ GAB. CGPNA/2020, que aprova o regulamento orgânico da DINFOP, este órgão tem as seguintes atribuições:

- apoiar a atividade de investigação e instrução criminal desenvolvida pela PNA;
- potenciar com informações a atividade de patrulhamento e vigilância desenvolvida pelas unidades centrais e comandos territoriais da PNA, na prevenção das reais ameaças e riscos contra a segurança pública;
- pesquisar analisar e difundir informações de interesse da PNA, avaliando permanentemente as ameaças, riscos e vulnerabilidades;
- orientar e rever periodicamente as necessidades e o esforço de pesquisa, análise e difusão de informações de natureza policial, em função da dinâmica do fenómeno da criminalidade;
- definir, desenvolver e controlar ciclos de informação da PNA, bem como as ações e formas de materialização; cooperar com as demais instituições similares do MININT, do Sistema de Segurança Nacional e das polícias congéneres da SADC e da comunidade internacional, na gestão da base de dados, sobre indivíduos procurados internacionalmente por práticas de atos ilícitos.

Capítulo II- Enquadramento jurídico

2.1. Enquadramento legal

Com o desenvolvimento tecnológico e o crescimento do ciberespaço, associado aos múltiplos benefícios que a sua utilização proporciona, a comunidade internacional percebeu que emergiram alguns fenómenos que comprometiam a utilização segura daquele meio. As semelhanças e disparidades das ameaças sofridas entre os vários países europeus aos seus interesses comuns, acabou por vir demonstrar, através da perceção da natureza global dos riscos, que o sistema nacional e internacional em matéria de segurança é algo fluido e maleável e os riscos invisíveis da sociedade mundializada devem ser entendidos como um efeito colateral para vida e a integridade física dos cidadãos (Fernandes, 2014).

Foi neste contexto que a comunidade internacional, e em especial os estados, se debruçaram sobre esta problemática, constatando a necessidade de adoção de medidas no sentido de dirimir os riscos inerentes à utilização do espaço virtual. Entre as diversas vertentes de ação, destaca-se a criação de diversas iniciativas legislativas que visam a regulação e ordenamento da utilização daquele espaço virtual, contribuindo desta forma para o tornar mais seguro. Vejamos, de seguida, alguns dos normativos legais que mais relevam no âmbito da segurança da informação, a nível europeu e nacional.

2.1.1. Legislação europeia

A legislação da União Europeia (UE) é essencial, pois permite-nos perceber o enquadramento que proporciona no âmbito da problemática da segurança da informação, e ainda pelo facto de servir de base para a produção de muita da legislação portuguesa. Neste sentido, apresentaremos diversos diplomas que se afiguram relevantes no contexto do presente estudo:

Diretiva 91/250/CEE do Conselho, de 14 de maio. Esta Diretiva reporta-se à proteção jurídica dos programas de computador, envolvendo também os direitos de autor e incluindo o respetivo material de conceção. A sua aprovação suportou-se, entre muitas outras considerações, nos investimentos em recursos técnicos, humanos e financeiros, na

importância crescente do papel desempenhado pelos programas de computador, nos de autor, que a pressão "programa de computador", e que a utilização desses programas deve obedecer a critérios que não violem os direitos de autor. Destaca-se assim a salvaguarda de algumas exceções, nomeadamente a possibilidade de dispor de uma cópia de apoio, os testes e estudo do programa e mesmo possibilidade de corrigir erros do programa.

Diretiva 2013/40/EU do Parlamento Europeu e do Conselho, de 12 de agosto. Esta Diretiva tem como objetivo aproximar o direito penal dos Estados-Membros no domínio dos ataques contra os sistemas de informação, estabelecendo regras mínimas relativas à definição de infrações penais e as sanções aplicáveis, e melhorar a cooperação entre as autoridades competentes, nomeadamente a polícia e outros serviços especializados dos Estados-Membros responsáveis pela aplicação da lei, bem como as agências e organismos especializados competentes da união, tais como a Eurojust, a Europol e o seu Centro Europeu de Cibercriminalidade, e a Agência Europeia para a Segurança das Redes e da Informação (ENISA).

Diretiva (EU) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho. Esta Diretiva é relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a UE. Para o efeito estabelece a obrigação de os Estados-Membros adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação; Cria um grupo de cooperação a fim de apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros e de segurança informática (rede de CSIRT) a fim de contribuir para o desenvolvimento da confiança entre os Estados-Membros e de promover uma cooperação operacional célere e eficaz; estabelece requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais; estabelece a obrigação de os Estados-Membros designarem as autoridades nacionais competentes, os pontos de contacto únicos e as CSIRT com atribuições relacionadas com a segurança das redes e dos sistemas de informação.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril. Este regulamento estabelece a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Para além do reforço da proteção jurídica dos direitos dos titulares dos dados, o RGPD exige novas regras e procedimentos do ponto de vista tecnológico.

Convenção sobre a Cibercriminalidade do Conselho da Europa, de 23 de novembro de 2001. Esta convenção é um tratado internacional de direito penal e direito processual penal firmado no âmbito do conselho da Europa para definir de forma harmónica, os crimes praticados através da internet e as formas de persecução. Ali estão previstas informações contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos; infrações relacionadas com computadores; infrações relacionadas com o conteúdo; infrações respeitantes a violações do direito de autor e direito conexos.

Estratégia da União Europeia para a Cibersegurança. Esta estratégia apresenta a visão da UE no contexto da cibersegurança, sendo ali referidas cinco prioridades estratégicas: (1) Garantir a resiliência do ciberespaço; (2) Reduzir drasticamente a cibercriminalidade; (3) Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da Política Comum de Segurança e Defesa (PCSD); (4) Desenvolver os recursos industriais e tecnológicos para a cibersegurança; (5) Estabelecer uma política internacional coerente em matéria de ciberespaço para a UE e promover os valores fundamentais nesse espaço.

2.1.2. Legislação Nacional

A Constituição da República Portuguesa (CRP) é uma norma jurídica que serve de base para construção de todo ordenamento jurídico de Portugal. Assim, essa norma estabelece direitos fundamentais no seu artigo 35.º com epígrafe (Utilização da Informática), na qual faz menção ao direito que os cidadãos têm de aceder aos dados informáticos respeitantes a eles mesmos, e que a informática não pode ser utilizada para tratamento de dados referentes a convicções filosófica ou política, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do seu titular, e ainda é referido neste diploma a proibição de acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei, e também a permissão de um enquadramento do que é permitido acerca da segurança da informação detida pelas organizações, nos mais variados aspetos.

A Lei n.º 41/2004, de 18 de agosto- Lei da Proteção da Privacidade no Setor das Comunicações Eletrónicas transpõe para o ordenamento jurídico português a Diretiva n.º 2002/58/ CE, do Parlamento Europeu e do Conselho Europeu, de 12 de julho de 2002,

relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas. Aplica-se igualmente ao tratamento de dados pessoais no contexto das redes e serviços de comunicações eletrónicas acessíveis ao público, especificando e complementando as disposições da Lei n.º 67/98, de 26 de outubro - Lei de Proteção de Dados Pessoais.

Lei n.º 32/2008, de 17 de julho , Lei sobre a conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações eletrónicas. Está Lei regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicação eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de junho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

A Lei n.º 109/2009, de 15 de setembro-Lei do Cibercrime transpõe para o ordenamento jurídico português a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à convenção sobre Cibercrime do Conselho da Europa. Esta lei proporciona o enquadramento legal em termos penais e processuais dos crimes praticados no âmbito da Informática, apresentando a tipificação desses crimes e a respetiva moldura penal

A Lei n.º 46/2018, de 13 de agosto – Regime Jurídico da Segurança no Ciberespaço estabelece o regime Jurídico da segurança do ciberespaço, transpondo a Diretiva (EU) 20016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a UE.

A Lei 2/94, de 19 de fevereiro visa institucionalizar os mecanismos de controlo de fiscalização da parte nacional do Sistema de Informação Schengen. Esta lei tem como objetivo preservar a ordem e a segurança públicas, incluindo a segurança do Estado, bem como a aplicação das disposições da convenção sobre a circulação das pessoas nos territórios das partes contratantes. Determina que a comissão nacional de proteção de dados pessoais

informatizados seja a autoridade nacional de controlo do Sistema, passando dois dos seus representantes a integrar a autoridade de controlo comum. Cria também o centro de dados que serve o sistema de informação Schengen, o qual fica dependente do serviço de estrangeiros e fronteiras e a funcionar sob orientação de um responsável nomeado por despacho do ministro da administração interna. E por fim insere também disposições sobre o direito de acesso aos dados do sistema.

O Decreto-Lei n.º 252/94, de 20 de outubro, Proteção Jurídica de Programas de Computador, transpõe para a ordem jurídica portuguesa a Diretiva n.º 91/250/CEE, do conselho europeu, de 14 de maio, relativa a proteção jurídica de programas de computador. No artigo 1.º faz menção à proteção conferida aos programas de computador que tiveram carácter criativo, análoga à que é atribuída às obras literárias, equiparando a programa de computador, o material de conceção preliminar daquele programa. A reprodução, transformação e autoria, os direitos do utente, os direitos de pôr em circulação e do titular originário, a apresentação, a vigência e a tutela, são algumas das temáticas abrangidas por esta Lei.

O Decreto-Lei n.º 69/ 2014, de 09 de maio Termos de Funcionamento do Centro Nacional de Cibersegurança (CNCS) do Gabinete Nacional de Segurança (GNS) procede à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, que aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança. Importa destacar que o Centro Nacional de Cibersegurança (CNCS) tem por missão contribuir para que o país use o Ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

O Decreto Regulamentar n.º 5/95, de 31 de janeiro, base de Dados Pessoais da Polícia de Segurança Pública, regulamenta a manutenção de uma base de Dados pela PSP do Sistema de Informações Operacionais de Polícia (SIOP/PSP). Dispõe sobre o tipo de dados recolhidos, atualização acesso à informação, comunicação, transmissão, conservação, direito a informação e segurança da mesma e sigilo profissional. Este diploma estabelece no seu artigo 12.º algumas disposições relativas à segurança da informação.

A Resolução da Assembleia da República n.º 88/2009, de 15 de setembro, aprova a convenção sobre o cibercrime, adotada em Budapeste em 23 de novembro de 2001.

A Resolução do Conselho de Ministros n.º 5/90, de 28 de setembro, contém normas para a segurança nacional, salvaguarda a defesa das matérias classificadas, segurança Informática. No artigo 1.º estabelece que a segurança informática visa garantir que o tratamento dos dados e programas esteja em conformidade com a classificação de segurança dos documentos que lhe deram origem, sempre que a salvaguarda dos interesses nacionais, de países aliados, organizações ou alianças de países de que Portugal faça parte justifique a sua aplicação. Por outro lado, pretende responsabilizar os diretores dos estabelecimentos, empresas, organismos ou serviços pela proteção de dados e programas, instalações, material informático, do pessoal, das comunicações de sabotagem, espionagem e ainda pelo implemento de medidas que garantam a fiabilidade do equipamento e suportes lógicos, integridade da informação e a continuidade dos trabalhos.

A Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho – Estratégia Nacional de Segurança no Ciberespaço.,, visa aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas.

A Resolução do Conselho de Ministros n.º 41/2018, de 28 de março, Regulamento Geral de Proteção de Dados, aprova os requisitos técnicos mínimos das redes e sistemas de informação que são exigidos ou recomendados a todos os serviços e entidades da Administração direta e indireta do estado, recomendando a aplicação desses requisitos técnicos também às redes e sistemas de informação do setor empresarial do Estado. Determina ainda que cada serviço e entidade da administração direta e indireta do Estado deve avaliar a conformidade dos requisitos técnicos das redes e sistemas de informação em uso com as finalidades e princípios de segurança que se pretendem alcançar com os requisitos estabelecidos pela presente resolução.

2.2. Surgimento do Sistema Estratégico da PSP

Segundo o Decreto-Lei n.º 243/2015, de 19 de outubro, a eficácia e o prestígio das forças de segurança está dependente, naturalmente, da previsão e concretização de medidas adequadas a responder cabalmente às exigências atuais relacionadas com desempenho das suas atividades. Para além de um elevado número de atribuições partilhadas com as outras forças policiais nacionais em domínios como a segurança e ordem pública, a prevenção e investigação criminal e a ordenação e fiscalização do trânsito, a PSP tem como atribuições exclusivas em todo o território nacional tais como: o controlo do fabrico, armazenamento, comercialização e licenciamento do uso de armas, munições e explosivos que não pertençam às Forças Armadas e forças de segurança; a garantia da segurança pessoal dos membros dos órgãos de soberania e de altas entidades nacionais ou estrangeiras, bem como de outros cidadãos em situação de ameaça relevante (art.º 3 da Lei n.º 53/2007 de 31 de agosto).

Essa diversidade de atribuições exige da PSP uma qualidade elevada de execução, pois assume um grau crítico alto, com repercussão direta na vida das populações. Não alheia a estes fatores, até por estarem intimamente relacionados com as suas áreas nucleares de atuação, a PSP preparou um programa de ação intitulada “Polícia 2000”, no qual concebe uma estratégia própria que visa contribuir de forma decisiva para a concretização dos objetivos globais de criação de uma sociedade mais segura (Accenture, 2002).

Alinhado com os objetivos estratégicos do Governo neste domínio, o programa Polícia 2000 assenta na qualidade da ação policial, cuja maximização se entende estar diretamente relacionada com a otimização de três pilares essenciais nomeadamente a satisfação do cidadão, eficácia e eficiência (Accenture, 2002).

No sentido de traduzir esta orientação estratégica em ações concretas, a PSP identificou para si três objetivos fundamentais com correspondência direta em três subprogramas de ação:

- objetivo 1- Reduzir o crime e o sentido de insegurança dos cidadãos, prosseguindo uma política de prevenção criminal e de manutenção da ordem, tranquilidade e segurança pública de qualidade; subprograma- Redução do crime, insegurança urbana e manutenção da ordem, segurança e tranquilidade públicas;
- objetivo 2 - Recuperar a confiança dos cidadãos na PSP, através de um efetivo policiamento de proximidade, orientado para os problemas de cada comunidade,

caraterizado pela transparência da atividade desenvolvida e pela cortesia, profissionalismo e responsabilidade dos agentes policiais; subprograma-policiamento de proximidade;

- objetivo 3 - prosseguir uma filosofia de gestão baseada na qualidade; subprograma-qualidade.

Cada um desses subprogramas é constituído por um vasto conjunto de medidas cuja implementação permitirá alcançar os objetivos traçados e, consequentemente, orientado à instituição no sentido da concretização da sua estratégia (Accenture/PSP, 2002).

Neste sentido o SEI foi implementado em maio de 2004, fruto do desenvolvimento de um projeto para a produção de um sistema de informação na PSP, cujo objetivo é assegurar a criação, manutenção e disponibilização da informação necessária e relevante à atividade operacional e de gestão da PSP, garantindo a sua atualização, coerência, integração e acessibilidade em tempo útil e de forma segura, funcionando como uma ferramenta complementar e de suporte para as diversas atividades policiais de carácter operacional ou de apoio (Pereira, 2019). Na visão de Lemos (2011), este sistema de informação foi materializado em função da realização do Euro 2004. Na sua opinião este foi o argumento ideal para obtenção de financiamento para o projeto em causa. No contexto prévio a implementação deste sistema verificava-se que vários comandos tinham os seus próprios sistemas, ou não, e havia uma descoordenação quanto aos procedimentos administrativos. Os processos eram desenvolvidos individualmente e a partilha de informação era praticamente nula por não haver uma base de dados centralizada (Accenture/PSP, 2002).

Deste modo, em 2002 foi desenvolvido o PESI no qual estabelecia que a missão do sistema de informação que viesse a ser criado seria assegurar a criação, manutenção e disponibilidade da informação necessária e relevante à atividade operacional e de gestão da PSP, garantido a sua atualização, coerência, integração e acessibilidade em tempo útil e de forma segura. O SEI surgiu como resposta que garantia estas questões. Este sistema foi criado para centralizar toda a informação da PSP e servir de núcleo de interoperabilidade entre outros sistemas que, entretanto, se vieram a desenvolver tais como SIGAE, SCOT.

O PESI estabeleceu assim as seguintes diretrizes para a conceção do SEI:

- Criação de um repositório único de dados;
- Estruturação da informação de forma lógica e orientada a conceitos;

- Maximização da utilização de ligações e associações tipificadas entre itens de informação;
- Potenciação da utilização de diversos tipos de informação;
- Registo da informação uma única vez;
- Definição, uniformização e operacionalização de procedimentos;
- Racionalização dos circuitos de informação internos;
- Recurso a dispositivos de acesso alternativos;
- Apresentação da informação de forma simples, consistente e amigável;
- Alinhamento com as tendências de mercado em matéria tecnológica;
- Utilização de novos canais de interação com os cidadãos e a sociedade em geral.

Estavam assim traçados os objetivos deste sistema. No âmbito dos recursos humanos à disposição do sistema podemos distinguir quatro grupos: os utilizadores, coordenadores, apoio e desenvolvimento. No grupo dos utilizadores inserem-se todos os elementos que utilizam o SEI como ferramenta de trabalho e são os principais responsáveis pela introdução de dados de todo o género do SEI, sejam pessoas, objetos, locais, ocorrências, etc. assim, configura-se como a maior "fatia" dos recursos humanos que caraterizam este sistema e, por conseguinte, uma peça fundamental para que o SEI tenha esta vasta qualidade de informação. Todos estes elementos, atualmente, recebem formação especifica para a sua função, estando distinguidos os módulos específicos ministrados e enumerados no Regulamento de Formação SEI (RFSEI) (Pereira, 2019).

Na categoria dos coordenadores, podem-se distinguir dois tipos de coordenação: central e a local. Na primeira a PSP dispõe da Equipa Única do SEI (EUSEI), implementada em 2011 e na dependência direta da Direção Nacional da PSP. De entre outras funções destacam-se: exercer, de forma integrada, a supervisão do SEI; estabelecer as prioridades de desenvolvimento e de evolução do SEI; supervisionar a qualidade dos dados do SEI; ser o ponto de contacto com os Oficiais de ligação SEI; colaborar na gestão do *Help Desk* nacional; acompanhar a utilização do SEI pelo dispositivo (Pereira, 2019).

A nível local existem os Oficiais de ligação SEI (OLSEI), tendo por função: contribuir para a qualidade do SEI e dos seus dados; propor alterações ao SEI; gerir *Help Desk* local, respondendo às solicitações apresentadas, devendo reencaminhá-las para o *Help Desk* nacional quando não estejam no âmbito das suas competências.

A criação de equipas de apoio técnico especializado aos utilizadores foi uma das diretrizes mais vincadas no PESI. Neste sentido, na terceira categoria enquadram-se os elementos que fornecem apoio aos elementos policiais no manuseamento do SEI. Este serviço funciona a nível local e nacional. Como já referido anteriormente, o OLSEI é responsável pela gestão do *Help Desk* local, devendo este ser o ponto de comunicação com o *Help Desk* Nacional nos casos em que o problema apresentado extravasa os seus conhecimentos. Deste modo, as competências comuns a estes dois serviços são: responder a questões funcionais, questões logísticas e de suporte à infraestrutura e configurações do SEI; esclarecer as dúvidas e problemas na utilização do SEI. Esta quarta categoria enquadra os elementos pertencentes ao Gabinete de Sistemas de Informação, cujas missões atribuídas pela PSP, enquanto responsáveis pelo desenvolvimento do SEI, são: corresponder às solicitações da EUSEI, no que respeita à manutenção do sistema ou novos desenvolvimentos; gerir a base de dados do SEI, no que respeita à sua manutenção, segurança e *backups*; desenvolver, na vertente técnica, os protocolos de interligação com entidades externas (Pereira, 2019).

O Regulamento de Formação do Sistema de Estratégico de Informação (RFSEI) refere que no âmbito tecnológico, o SEI é executado através de uma aplicação do tipo *Browser*, o mesmo que é utilizado regularmente para aceder à internet, sendo o SEI uma aplicação baseada em tecnologia *Web*. O sistema divide-se em vários módulos, cada um com múltiplas funcionalidades, direcionadas para as várias tarefas existentes, são eles: Estatística e Relatórios; Gestão de Grandes Eventos; Gestão Operacional de Meios; Gestão de Processos Policiais; Gestão de Celas e Detidos; Gestão de Informações Policiais; Licenciamento e Fiscalização; Repositório de Informação e Catálogo.

2.2.1. Módulos do SEI

O SEI encontra-se dividido em módulos que congregam todas as funcionalidades pertencentes a diversas atividades operacionais da PSP. Esta divisão proporciona maior facilidade de navegação na aplicação, conseguindo-se também para uma melhor compreensão dos conceitos associados a cada funcionalidade disponibilizada. Além dos módulos, existem também aplicações que servem de suporte ao SEI nomeadamente: Gestão

de Utilizadores e Perfis; a Integração de Aplicações; o Sistema de Informação Geográfica e Administração de Aplicações (Accenture, 2004a). Apresentaremos de seguida alguns módulos que consideramos mais relevante.

Módulo Repositório de Informações e Catálogo

O Repositório de Informações e Catálogo engloba um conjunto de mecanismos necessários para criação, atualização, eliminação, pesquisa e consulta dos itens de interesse, nomeadamente: organizações; pessoas; veículos e objetos. Que constituem a base de todo o modelo de dados operacional e respetivas ligações. Esta aplicação permite relacionar as várias entidades do repositório de informação e ainda identificar várias ocorrências dentro de uma entidade segundo determinado certo critério (Accenture, 2004b).

Mais do que uma aplicação, o Repositório de Informações e Catálogo deve ser entendido como um conjunto de mecanismos e serviços aplicacionais padronizados, que permitirão a independência e isolamento da informação que gerem relativamente às restantes aplicações operacionais que deles farão uso para efeitos de consulta ou atualização de componentes (PESI, 2002).

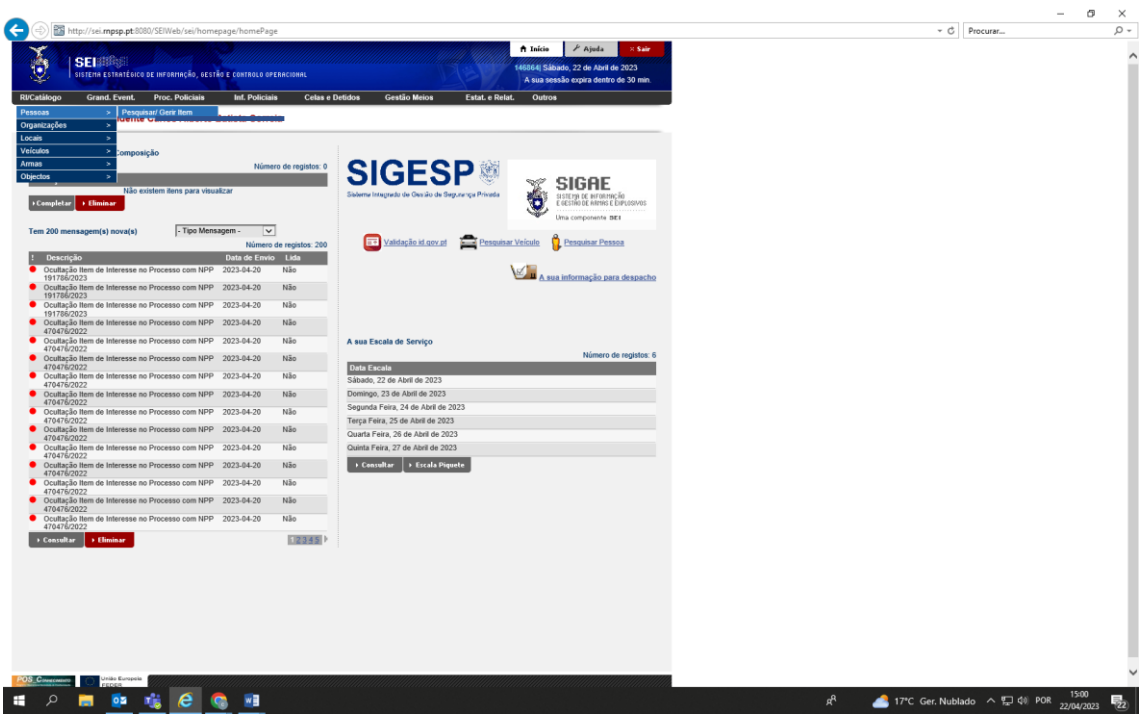


Figura 1 - Interface do Módulo Repositório de Informações e Catálogo (Fonte: Sistema Estratégico de Informação)

Módulo de Gestão Operacional de Meios

Esta aplicação assume uma importância capital na atividade operacional da PSP, engloba essencialmente duas vertentes:

- Assegurar a presença de elementos policiais onde efetivamente são mais necessários, já que só conhecendo quais os locais mais problemáticos da zona de ação de cada unidade será possível fazer um planeamento correto das atividades operacionais;
- Suportar a constituição de turnos, patrulhas e serviços, bem como a atribuição de meios logísticos aos mesmos.

Como principais funcionalidades esta aplicação é composta por um sistema de informação geográfica e também por um Planeamento de escala. A primeira permite que, perante determinada emergência, os meios considerados mais apropriados e que se encontrem mais próximos do local possam ser canalizados para lá. Por sua vez o Planeamento de Escalas permite a disponibilização de mapas das zonas de intervenção onde serão visualizados os locais mais críticos nos diversos tipos de ocorrências relativamente às áreas de atuação das diversas subunidades da PSP. Associado à "mancha" de distribuição deverá estar uma componente estatística que permite saber quantas ocorrências se deram no local em causa. Esta funcionalidade assume importância na medida em que só assim será possível obter o "peso" relativo a um local na totalidade da zona em questão, de forma a canalizar ações de policiamento preventivo para esses locais (PESI, 2002).

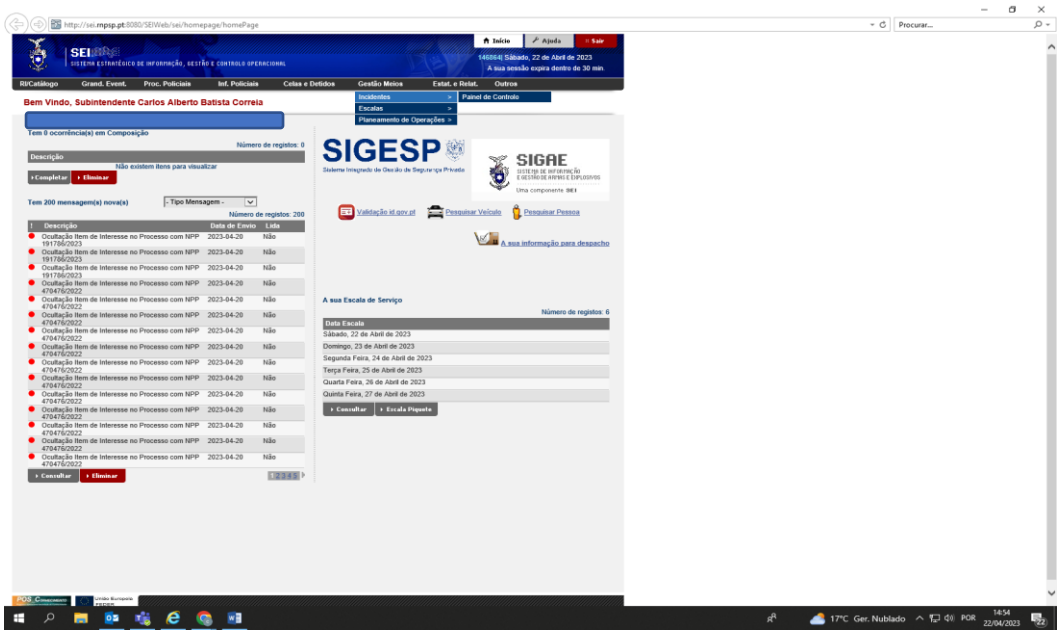


Figura 2 - Interface do Módulo Gestão Operacional de Meios (Fonte: Sistema Estratégico de Informação)

Módulo de Gestão de Grandes Eventos

O grande foco deste módulo é a gestão da informação relativa a grandes eventos nos quais a PSP tem maior intervenção, permitindo que a informação gerida nos restantes módulos seja classificada como estando relacionada com determinado grande evento, quer para fornecimento a entidades externas quer para controlo interno (Cucu, 2019).

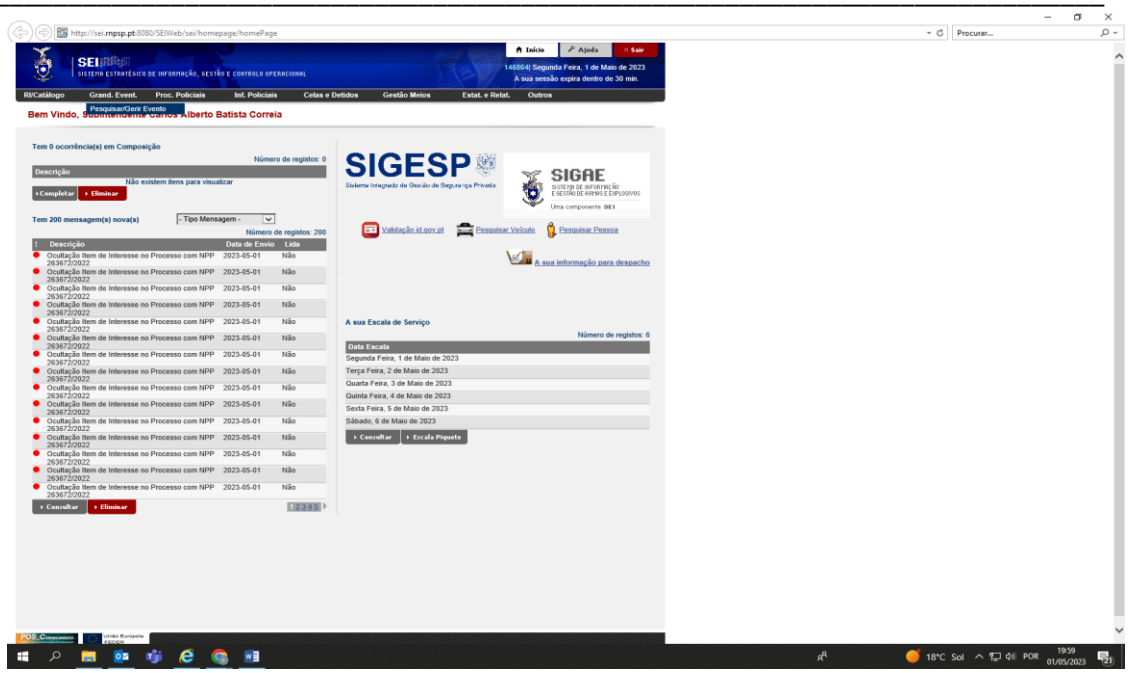


Figura 3 - Interface do módulo Grande Evento (Fonte: Sistema Estratégico de Informações)

Gestão de Ocorrências

O módulo de Gestão de Ocorrências é um dos componentes de um módulo operacional mais abrangente denominado "Gestão de Processos Policiais". Pretende-se que este módulo permita o registo das ocorrências e gestão de processos dos vários tipos relevantes no âmbito da atividade operacional da PSP, tais como crimes, contraordenações e outros (Accenture, 2004d).

Tendo em vista a uniformização do tratamento de ocorrências, definiu-se que será criado um processo sempre que se conclua o registo de uma ocorrência no sistema. Neste sentido, o registo de uma ocorrência no sistema é considerado a "fase zero do processo" só sendo possível a emissão do respetivo expediente após a conclusão do registo da ocorrência. Cada processo será identificado internamente no sistema por um Número de Processo de Polícia (NPP), número único por ano, a nível nacional, atribuído automaticamente pelo sistema. (Accenture, 2004d)

O NPP é interno e completamente independente do Número Único Identificativo de Processo-Crime (NUIPC), definido pelo Ministério Público para a identificação oficial de

processos-crime. O NUIPC poderá ser atribuído manualmente pelo utilizador ou gerado automaticamente pelo sistema, sendo a opção da responsabilidade do utilizador. No SEI, a atribuição do NUIPC ao processo apenas ocorre quando se termina o registo de uma ocorrência (Accenture, 2004d).

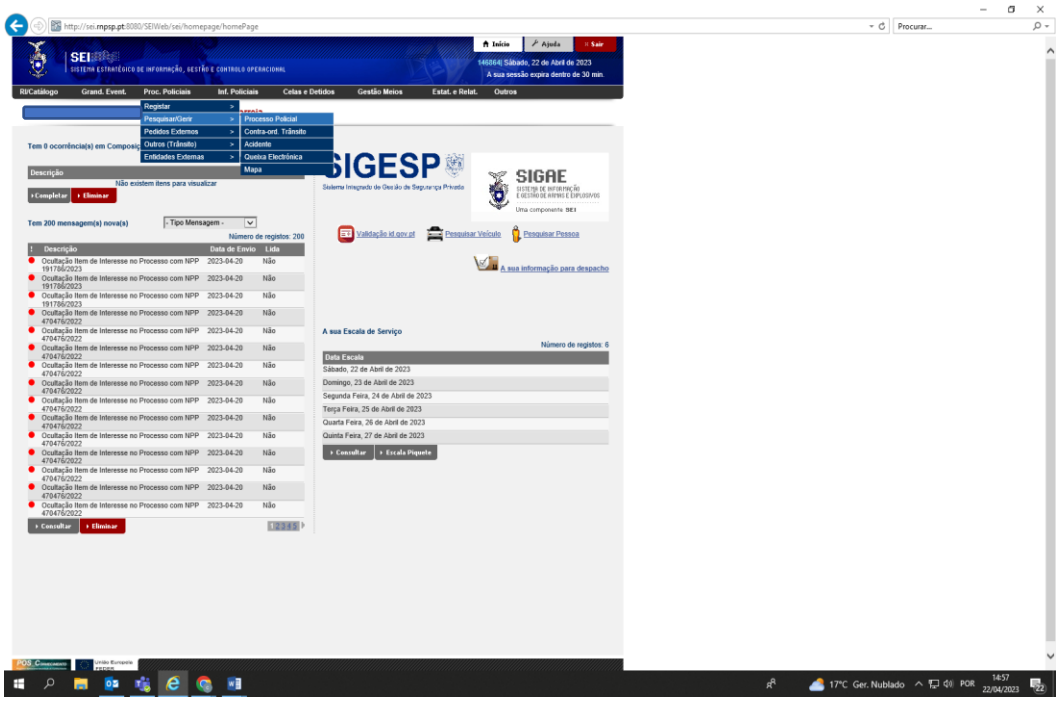


Figura 4 - Interface do Módulo Gestão de Ocorrência. (Fonte: Sistema Estratégico de Informação)

Módulo de Gestão de Celas e Detidos

Este módulo tem como fim a gestão de informação referente a celas e detidos, nas áreas de detenção das unidades da PSP. Deste modo, o módulo divide-se em duas grandes áreas:

- Gestão de Áreas de Detenção- que envolve a informação e gestão das celas e detidos, nas áreas de detenção das unidades da PSP.
- Gestão de Detidos- que envolve funcionalidades para registo de detidos, pesquisa, consulta e alteração de informação sobre detidos, afetação do detido a áreas de detenção e respetivas celas, registo de acontecimentos específicos como por exemplo contactos, refeições, cuidados médicos (Accenture, 2004a).

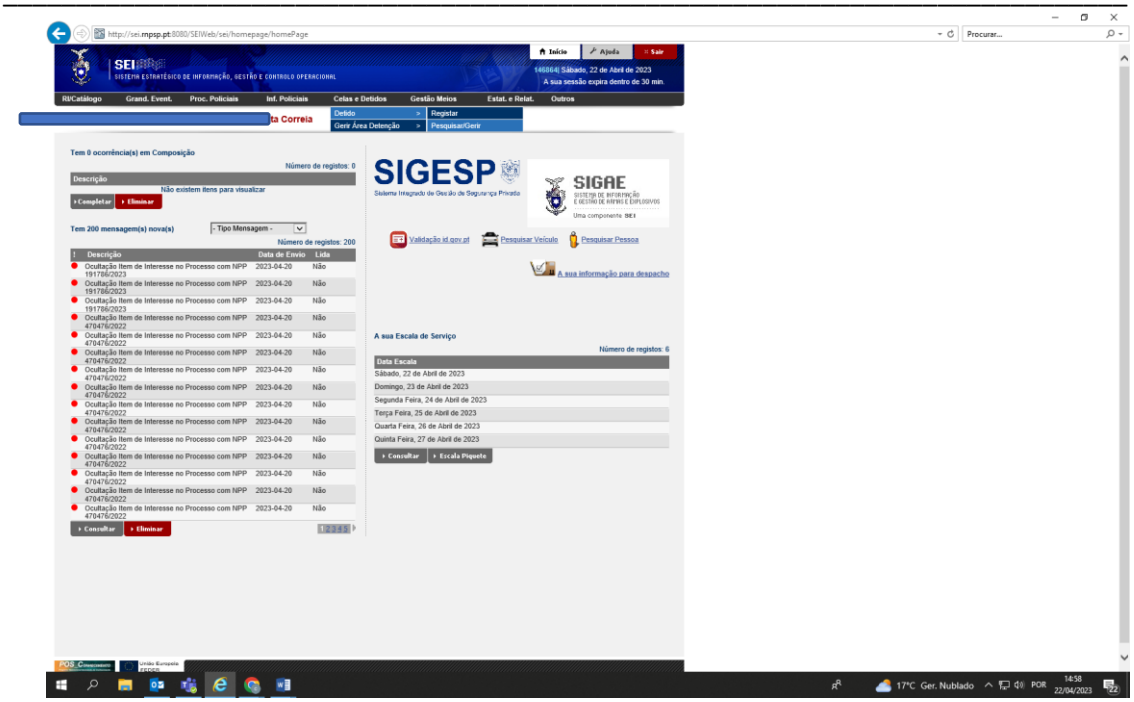


Figura 5 - Interface do Módulo Gestão de Celas e Detidos. (Fonte: Sistema Estratégico de Informação)

Módulo de Informações Policiais

Este módulo permite aos elementos policiais, criar e difundir informações para as restantes unidades policiais do país, suportando o objetivo do SEI de promover e viabilizar a efetiva integração e partilha de informação na PSP. Desta forma, sendo a partilha de informação uma área sensível da atividade operacional da PSP, esta funcionalidade encontra-se enquadrada pelas seguintes regras:

- Credenciação – Apenas têm acesso à informação os elementos policiais que estejam explicitamente credenciados para o efeito;
- Princípio da necessidade de conhecer- Apesar de um elemento policial ter credenciação para uma determinada informação, apenas deve ter acesso ao conteúdo se existir a necessidade de a conhecer.

Contudo, o SEI está configurado para suportar estes princípios, de modo a garantir a eficiência das especificidades operacionais da PSP (Accenture, 2004b).

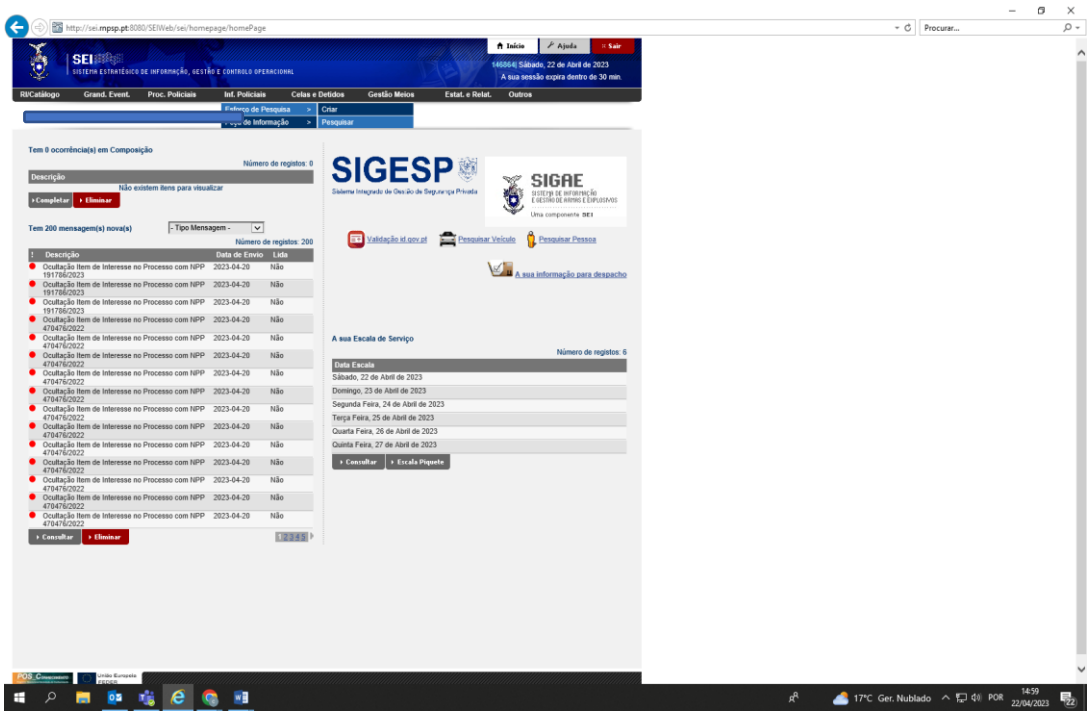


Figura 6 - Interface do Módulo Informações Policiais (Fonte: Sistema Estratégico de Informação)

2.3. Proteção dos Dados Pessoais no SEI

A dialética entre as exigências de segurança da comunidade e do respeito pelos direitos fundamentais é uma questão sensível. Esses direitos podem ser postos em causa pelo desenvolvimento da informática. Apesar dos perigos que a informática envolve, a justiça não pode dispensar a sua relevância, em especial quando esteja em causa a segurança de pessoas e bens (Eiras, 1992).

A tutela dos cidadãos relativamente aos bancos de dados reveste três vertentes: dos cidadãos em relação ao Estado; dos cidadãos em relação aos outros cidadãos e dos cidadãos perante outros Estados (Eiras, 1992).

Segundo o Relatório do Centro Nacional de Cibersegurança Portugal 2022, (CNCS) em relação à gestão do acesso aos dados pessoais na internet, os cuidados mais comuns foram a restrição ou recusa do uso dos dados pessoais para fins publicitários. Verificou-se

um decréscimo apenas em relação a indivíduos que lêem as declarações da política de privacidade antes de fornecerem os seus dados pessoais.

No SEI encontra-se reunida toda a informação resultante da atividade e funcionamento da PSP, configurando-se assim no maior repositório de informação policial de Portugal, sem o qual a eficiência operacional desta polícia estaria comprometida. Importa destacar que o SEI é uma base de dados que congrega o armazenamento de dados pessoais, sendo que o tratamento dos mesmos obedece a princípios legais.

No conceito de dados pessoais são abrangidos aspetos que usualmente servem para identificar uma pessoa (nome, apelido, morada, data de nascimento, etc) bem como qualquer conjunto de informações que permitam identificar uma pessoa por referência a um número de identificação ou através de elementos específicos relativos à sua identidade física, fisiológica, psíquica, económica, cultural ou social, incluindo a voz e a imagem da pessoa (Regulamento (EU) 2016/679; Lei n.º 67/98, de 26 de outubro, art. 3.º, a); Lei n.º 59/2019, de 8 de agosto, art. 4.º n. 2).

Considerando que os dados pessoais são informações sobre indivíduos, quaisquer meios ou processo de recolha e/ou tratamento ou divulgação suscitam a necessidade de encontrar novos modos de responder a tais desafios, por forma a assegurar que os acessos a estes dados não resultem em agressões ou constrangimentos para a pessoa em causa (Ribeiro, 2012).

A proteção de dados pessoais encerra a possibilidade de os cidadãos poderem decidir quanto à utilização que é dada aos seus dados pessoais, em conjunto com o estabelecimento de uma série de garantias para evitar que estes dados pessoais sejam utilizados de forma a causar discriminação, ou danos de qualquer espécie, ao cidadão ou à coletividade. Esta proteção específica atribuída aos dados pessoais resulta da evolução daquele que é o conceito do direito à privacidade e visa criar garantias, pela criação de normativo jurídico, visando prevenir, mediante punições, a intromissão alheia em questões do fórum privado (Canelas, 2017).

A complexidade e desenvolvimento das tecnologias de Informações que envolvem dados pessoais tem vindo a obrigar à construção de quadros normativos legais que tentam acompanhar esta revolução tecnológica, com vista a salvaguardar aquele que é um direito constitucionalmente previsto.

A Constituição da República Portuguesa (CRP) salvaguarda o direito dos cidadãos sobre o acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei conforme previsto no art. n.º 35 da CRP. O regime legal relativo ao tratamento de dados pessoais encontra-se na Lei n.º 58/2019 de 8 de agosto, prevê que qualquer pessoa que tenha sofrido um dano devido ao tratamento ilícito de dados ou qualquer disposições que viole a presente lei ou o RGPD, tem direito de obter do responsável ou subcontratante a reparação pelo dano sofrido (art. 33.º da Lei n.º 58/2019 de 8 de agosto)

Manter o registo central de dados pessoais exige previsão legal com parecer prévio da CNPD ao passo que este registo, não sendo centralizado, apenas carece de emissão de parecer daquela comissão que deixa de ser necessário assim esteja previsto e autorizado em diploma legal este tipo de registo. O processamento, armazenamento, registo de dados pessoais é uma área complexa e sensível e tal constata-se na preocupação que do ponto de vista legal se traduz na responsabilização penal de condutas que pervertem o espírito da LPDP. O tratamento e registo não centralizado de dados pessoais sem pedido de autorização à CNPD e o desvio ou utilização de dados pessoais de forma incompatível com a finalidade que determinou a sua recolha (Canelas, 2017).

2.3.1 Responsável pela proteção de dados

O Regulamento geral de Proteção de Dados (RGPD) foi aprovado pela UE, introduzindo deste modo um novo regime em matéria de proteção de dados pessoais. Foi criado para proteção do cidadão face ao tratamento de dados pessoais em larga escala por grandes empresas e serviços da sociedade de informação (Presidência do Conselho de Ministros, 2018)

A Comissão Nacional de Proteção de Dados (CNPD) é a autoridade responsável pelo controlo nacional para efeitos do RGPD, sendo esta uma entidade administrativa independente, com personalidade jurídica de direito público e poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República e fiscaliza o cumprimento do RGPD, bem como as demais disposições legais e regulamentares em matéria de proteção de dados pessoais, com o fim de defender os direitos, liberdades e

garantias do cidadão no âmbito do tratamentos de dados pessoais, conforme previsto nos artigos 3.º e 4.º da Lei n.º 58/ 2019, de 8 de agosto.

Destaca-se ainda a figura do encarregado de proteção de dados que está obrigado ao dever de sigilo profissional em tudo o que diga respeito ao exercício dessa função, e que se mantém após o termo das funções que lhes deram origem (art. 9.º da Lei 58/2019, de 08 de agosto; art 38.º n.º 5 do Regulamento (UE) 2016/679 do Parlamento Europeu e Do Conselho). Quando o responsável pelo tratamento ou o subcontratante for uma autoridade ou um organismo público, pode ser designado um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão. A atividade principal do responsável pelo tratamento dos dados consiste em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala (Art. 37º do Regulamento (UE) 2016/679 do Parlamento Europeu e Do Conselho).

O encarregado de proteção de dados não recebe instruções relativa ao tratamento dos dados por parte do responsável, nem pode ser destituído e/ou penalizado pelo responsável pelo tratamento pelo facto de exercer as suas funções, sendo que cabe-lhe informar diretamente a direção ao mais alto nível do responsável pelo tratamento dos dados (art. 38.º do Regulamento (UE) 2016/679 do Parlamento Europeu e Do Conselho).

2.4. Proteção dos pessoais em Angola

A proteção dos dados pessoais, da confidencialidade e da reserva da vida privada assume uma relevância fundamental no contexto da salvaguarda dos direitos fundamentais dos cidadãos, reconhecidos pela Declaração Universal dos Direitos do Homem e pela Carta Africana dos Direitos do Homem e dos Povos. A Consagração na Constituição da República de Angola, do direito a reserva da vida privada e da possibilidade do recurso à prevenção representa manifestamente um grande passo na adoção de um quadro legislativo nesta matéria.

O direito à privacidade traduz-se também no respeito pela reserva da vida privada dos cidadãos face ao tratamento de dados pessoais que lhes digam respeito. Muito embora

tal tratamento tenha um papel relevante para a melhoria do bem-estar dos cidadãos e para o progresso económico num contexto de dinamização e de desenvolvimento de uma maior variedade de serviços, nomeadamente no âmbito das tecnologias e da sociedade da informação, há que assegurar que o mesmo seja efetuado num contexto de respeito pela privacidade.

A CRA garante aos cidadãos o direito de recorrer à providência de *habeas data* para assegurar o conhecimento da informação sobre si constantes de ficheiros, arquivos ou registos informáticos, de serem informados sobre o fim a que se destinam, bem como de exigir a retificação ou atualização dos mesmos, nos termos da lei e salvaguardados o segredo de Estado e o segredo de Justiça, bem como a proibição de tratamento de dados relativos às convicções políticas, filosóficas ou ideológicas, à fé religiosa, à afiliação partidária ou sindical, à origem étnica e à vida privada dos cidadãos com fins discriminatórios, é igualmente proibido o acesso a dados pessoais de terceiros, bem como à transferência de dados pessoais de um ficheiro para outro pertencente a serviço ou instituição diversa, salvo nos casos estabelecidos por lei ou por decisão judicial conforme previsto no art.º 69.º da CRA.

A Lei de Proteção de Dados Pessoais, angolana, aprovada pela Lei n.º 22/11 de 17 de junho, prevê que o tratamento de dados deve ser notificado à Agência de Proteção de Dados (APD) no prazo de 2 anos. Desta forma, todas empresas estão obrigadas a cumprir o legalmente previsto na Lei, devendo ser entregues na APD, presencialmente, as notificações ou os pedidos de autorização para tratamento de dados em Angola, através de requerimento informal elaborado pelo próprio requerente, no qual devem constar todas as informações necessárias sobre o tratamento de dados que se pretende recolher (Neves, 2020).

Importa destacar que a Lei de Proteção de dados em Angola, não se aplica no âmbito da segurança do Estado, segredo de Justiça, bem como ao tratamento de dados pessoais dos membros das Forças Armadas Angolanas (FAA) pelas unidades, estabelecimento e órgãos militares ou outros sob tutela do departamento ministerial responsável pelas Forças Armadas, conforme previsto no art. 4.º n.º 2 do mesmo diploma.

2.5. Problemática de investigação

Na elaboração de um trabalho científico, o investigador deve primeiramente escolher um caminho claro, ou seja, traduzir um projeto de investigação sob a forma de uma problemática de investigação, que a sua utilidade ou pertinência dependa da sua correta formulação. Este esforço obriga o investigador a uma classificação útil, das suas intenções e perspetivas. Assim, é possível referir que a pergunta de partida se configura como um meio primário para pôr em prática uma das dimensões essenciais do processo científico, ou seja, a rotura com preceitos e noções prévias (Quivy & Campenhoudt, 2005).

Atendendo a este contexto, esta investigação procurará dar resposta a seguinte pergunta de partida:

Como seria a adequação de um sistema de informação na Polícia Nacional de Angola?

Capítulo III - Método

3.1. Metodologia

Uma vez escolhido o método por parte do investigador, este reflete-se na escolha do caminho a seguir que, segundo Quivy e Campenhoudt (2005), é exigido ao investigador que seja capaz de gerar e de pôr em prática um dispositivo para a elucidação do real, isto é, no seu sentido mais lato um método de trabalho, ou ainda nas palavras de Silva e Pinto (1989) é uma estratégia integrada de pesquisa que organiza criticamente as práticas de investigação, incidindo nomeadamente sobre a seleção e articulação das técnicas de recolha e análise de informação. Assim, o método é o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo, traçando o caminho a ser seguido, detetando erros e auxiliando as decisões do cientista (Marconi & Lakatos, 2003).

A presente dissertação consiste num estudo exploratório, que procura perceber o funcionamento e aplicabilidade do SEI e como uma ferramenta como esta melhoraria o trabalho operacional da PNA. De modo a alcançar estes objetivos, deve ser escolhido um método adequado, ou seja, é o objeto de investigação que define o método que será utilizado (Flick, 2005). Neste sentido, a presente investigação terá o teor qualitativo, tendo em conta o *corpus* que constitui o estudo, uma vez que, permite uma abordagem mais aberta e envolvente ao objeto de estudo (Flick *et al*., 2004).

3.2. Corpus

O *corpus*, segundo Bardin (1977), consiste no conjunto dos documentos tido em conta para serem submetidos a procedimentos analíticos. Neste sentido, podemos considerar o *corpus*, como o material de trabalho do investigador, ou como refere Aarts e Bauer (2000) a colocação finita de materiais, determinada de antemão pelo analista, com inevitável arbitrariedade do analista, e com a qual se irá trabalhar. Deste modo, pretendíamos realizar nove entrevistas correspondente aos nove Comandantes Municipais que compõem o CPL, por força do pouco conhecimento da matéria em questão e também a não obrigatoriedade de participação no presente estudo foi possível a realização de quatro entrevistas. Assim podemos referir que o *corpus* da nossa investigação será constituído por este conjunto de

entrevistas, sendo todas elas feitas aos Comandantes Municipais do Comando Provincial de Luanda. A escolha do CPL como objeto do presente estudo foi por ser a única província que nos garantia alguma capacidade de resposta em função da disponibilidade de internet para a comunicação.

3.3. Instrumentos de Recolha de Dados

3.3.1. Entrevista

As entrevistas apresentam-se com um ótimo instrumento de recolha de dados, visto que permitem retirar informações e elementos de reflexão muito ricos e matizados (Quivy e Campenhoudt, 2005). Havendo a necessidade de recorrer a entrevistas, para obter a informação que constituirá uma parte do *corpus*, surgiu a necessidade de se optar pelo tipo de entrevista que melhor servisse os nossos objetivos.

Deste modo, e tendo em conta o objeto de estudo, a escolha recaiu na realização de entrevistas semiestruturadas. Este tipo de entrevistas carateriza-se por conter um conjunto de perguntas abertas, que funcionam como uma linha orientadora, permitindo um diálogo fluído entre o entrevistador e o entrevistado. Assim, foi possível obter uma informação mais abrangente, o que permitiu uma melhor perceção da realidade em estudo, fruto da experiência dos entrevistados (Quivy & Campenhoudt, 2005; Sarmento, 2013).

A obtenção de informação mais abrangente prende-se com o facto de as entrevistas semiestruturadas apresentarem uma flexibilidade que permite recolher os testemunhos e interpretações dos entrevistados (Quivy & Camenhoudt, 2005). Desta forma, os entrevistados conseguem analisar o problema tendo em conta as suas interpretações de situações conflituosas e o que está em jogo (Quivy & Campenhoudt, 2005).

3.4. Procedimento

Tal como foi referido no presente trabalho, o *corpus* desta dissertação assentou em entrevistas, que foram sujeitas a uma análise de conteúdo sendo o investigador o principal instrumento de recolha de dados (Bogdan & Bilklen, 1994). Para se proceder à análise de

conteúdo das entrevistas, tivemos de recorrer a um processo de categorização, algo que exigia a criação de categorias e subcategorias.

Utilizando uma grelha categorial e um manual de codificação, procedeu-se à análise de Conteúdo propriamente dita, sendo que a mesma se suportou num procedimento fechado, em virtude de as categorias terem sido previamente definidas (Ghiglione & Matalon,2001).

De forma a garantir as regras de validade e fiabilidade, bem como os critérios de exaustividade e exclusividade, todo o processo de análise de conteúdo foi elaborado, seguindo o postulado por estes fatores. Deste modo, assegurou-se a capacidade de replicação defendida por Krippendorff (2004), o que permite tornar válidos, os resultados obtidos pela presente investigação.

Capítulo IV- Apresentação, Análise e Discussão de Resultados

Depois de efetuado o estudo da arte sobre a importância dos Sistemas de Informações, e termos escolhido e traçado o método mais apropriado para obtermos a resposta da nossa pergunta de partida, no presente capítulo, faremos a apresentação e discussão de resultados. Na análise de conteúdo do *corpus*, procedeu-se à codificação de 65 unidades de registos (u.r.), que foram enquadradas nas respetivas subcategorias das 8 categorias definidas.

Dos resultados apresentados, constata-se que existe uma distribuição generalizada das unidades de registo pelas 8 categorias delineadas, destacando, porém, a representatividade e relevância no nosso estudo. Importa realçar que para o presente estudo a percentagem de 25% entendeu-se como pouco relevante, enquanto que 50% em diante considerou-se como relevante.

4.1. Necessidade de um SI na PNA

Nesta categoria foram consideradas cinco subcategorias que mereceram a distribuição de unidades de registo, constantes no apêndice II e conforme representado no gráfico da Figura 1. O que significa que há necessidade de um SI da PNA. As subcategorias mais identificadas foram "identificação e localização" e "fluidez e eficiência na procura" o que indica que atualmente esta força de segurança não dispõe de nenhuma ferramenta que possa auxiliar na identificação de pessoas desaparecidas ou sinalizadas nem em caso de furto ou roubo de viaturas há meio de suporte eficaz ao serviço operacional. Enquanto as subcategorias "Necessidades (…) segurança pública", "crimes rodoviários" e Fornecimento de dados relevantes" foram as subcategorias menos identificadas, o que pode ser entendido como desconhecimento por parte dos entrevistados sobre a abrangência e valências de um SI numa força de segurança.

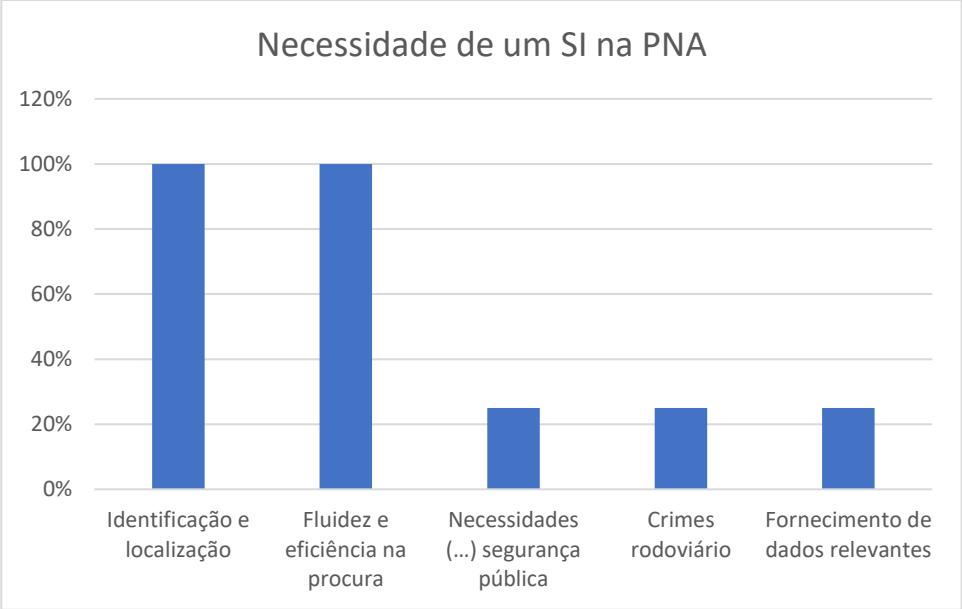


Gráfico 1 - Distribuição das unidades de registo da categoria "Necessidade de um SI na PNA".

4.2. Partilha da informação

Nesta categoria pretendeu-se perceber como é feita a partilha interna da informação criminal na PNA, deste modo, 50% dos entrevistados considera que são usadas com maior regularidade os "rádios de comunicação" e também por um "Sistema Integrado", sistema este que é também conhecido como Sistema de Gestão de Informações de Casos e Eventos Criminais (SGICEC) que é uma ferramenta do Centro Integrado de Segurança Pública (CISP). Este sistema vem para auxiliar a polícia na padronização do expediente elaborado por esta força de segurança, desde a denúncia, abertura de investigação (Issenguele & Cabombo, 2021). Infelizmente a falta de recursos materiais acaba por tornar este SI ineficiente, pois das 18 províncias que constituem Angola, apenas estão contempladas 8 delas, nomeadamente Luanda, Benguela, Huambo, Cuanza Sul, Huila, Namibe e Bengo. Ainda sobre a insuficiência de meios materiais o SGICEC, até ao momento é extensivo apenas aos Comandos Municipais e não às Esquadras, este facto torna esta ferramenta ineficiente pois as Esquadras é que lidam diretamente com a população e no nosso entender o ideal seria que o SI as abrangesse. Importa abordar sobre a subcategorias "Partilha por

Whatsapp", apesar de ser um meio de partilha insignificante (25%) importa enfatizar que é uma das maneiras usuais para partilha de informações. Considerando que se trata de uma rede social e um meio não oficial para partilha de informações de interesse policial, o uso deste meio para este fim configura-se como uma fragilidade em termos de segurança para a própria organização pois as ciberameaças exercem a sua atividade e se difundem na rede fruto da utilização massiva das tecnologias de informação (Elias, 2018).

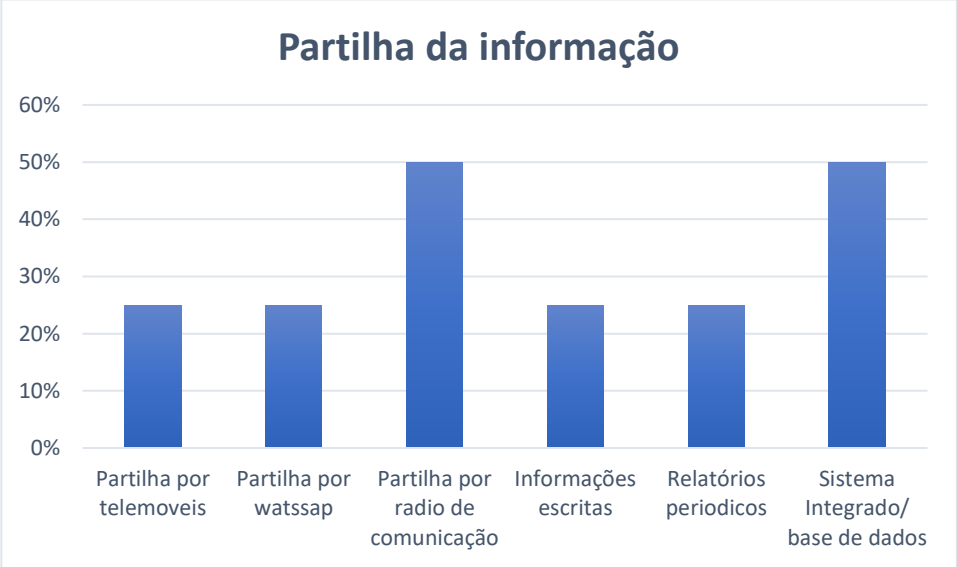


Gráfico 2 - Distribuição das unidades de registo da categoria "Partilha da informação"

4.3. Segurança da informação criminal na PNA

Segundo Torres (2015), para que haja proteção de um ativo crítico é necessário primeiramente identificá-los. O que significa que quando o objetivo último é selecionar meios para a proteção de ativos, primeiramente é preciso conhecer quais são estes ativos que vão beneficiar destas medidas protetivas. Neste sentido, com esta categoria pretendeu-se perceber como é feita a segurança da informação criminal da PNA, deste modo, 75% dos nossos entrevistados referem que as informações criminais são tratadas de modo a evitar eventual fuga de informação, obedecendo pressupostos como: registo; estudo; interpretação;

análise; conclusão e difusão. 50% dos entrevistados destacam que após o tratamento da informação, a mesma é difundida para a DINFOP/PNA, que entre as diversas atribuições que possui, é o órgão responsável pela organização, planificação, pesquisa, recolha, centralização, classificação e disseminação das informações de interesse policial, visando auxiliar a materialização das atribuições da PNA, desenvolvida pelos seus órgãos e serviços (Despacho n.º 034/ GAB.CGPNA/2020). A subcategoria "recolha da informação" faz menção sobre a fonte da informação criminal na PNA, que surge do expediente elaborado por esta força de segurança e é tramitada até ao DINFOP/PNA, conforme referido por 50% dos nossos entrevistados. Na subcategoria "secreta e confidencial" apenas 25% dos nossos entrevistados consideraram que as informações são tratadas de forma secreta e confidencial, o que pode significar um desconhecimento a respeito do tratamento das informações.

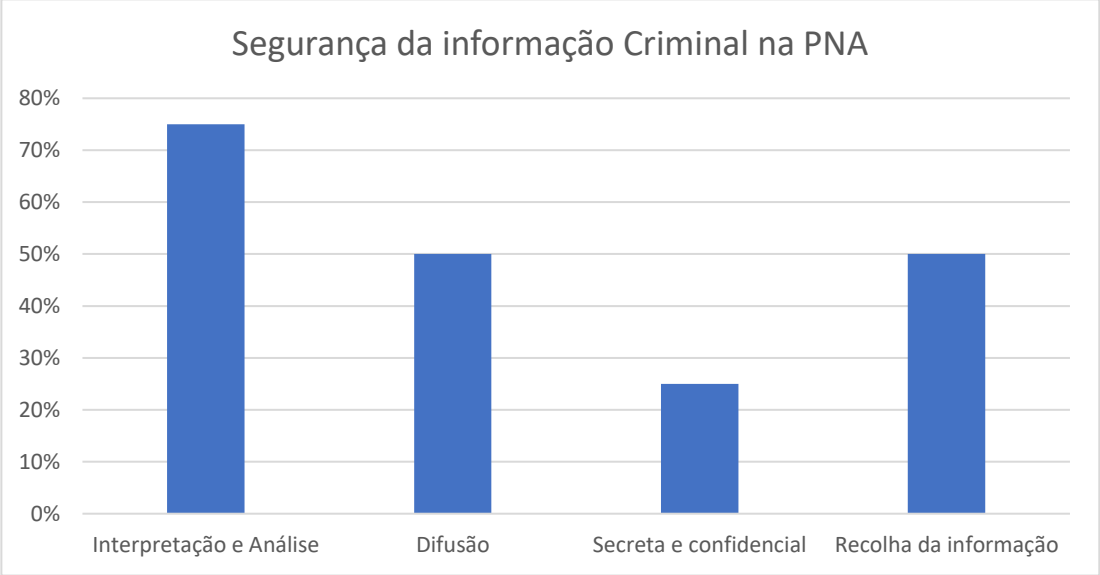


Gráfico 3 - Distribuição das unidades de registo da categoria "Segurança da informação criminal na PNA"

4.4. Abordagem Proativa/ Reativa

Há dois tipos principais de abordagem a reativa e proativa, ambas têm a sua importância na mitigação de riscos futuros. A primeira remete-nos a agir quando ocorre um acidente ou uma falha no sistema que dará origem a um processo de verificação e reparação de modo a que a falha não volte a acontecer, geralmente este processo envolve auditoria,

análise e pesquisa, documentação, implementação de medidas. Já a abordagem proativa faz menção a uma ação para que não haja incidentes, ou seja é uma prática de fiscalização diária para evitar que incidentes venham acontecer (Caetano, 2020). Na subcategoria "proativa" 100% dos entrevistados são de opinião que a abordagem mais apropriada para a segurança de um sistema de informação é a abordagem proativa, pois esta permite que não haja interrupções para resolução de problemas e também por mostrar-se mais económica a longo prazo. Quanto às subcategorias "prevenção, tratamento de informações criminais e necessidades de segurança" 50 % dos entrevistados entendem que a proatividade vem sempre como vetor primário na atividade policial, e um sistema de informação ininterrupto contribui significativamente para a proatividade policial, contribuindo assim na prevenção de ilícitos, e mitigando as necessidades de informação.

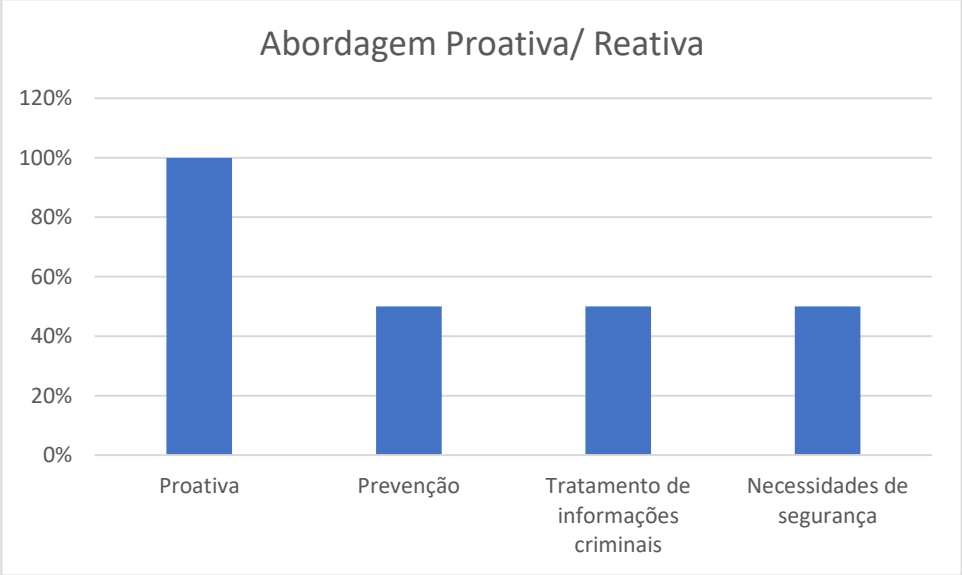


Gráfico 4 - Distribuição das unidades de registo da categoria "Abordagem proativa/reativa"

4.5. Riscos do SI

Outro grande fator que decidimos abordar no contexto do presente estudo prende-se com os aspetos de riscos que incidem sobre os SI. São assim focados os aspetos: "fator humano"; "programas mal configurados"; "falta de confidencialidade"; "fuga de informação"; "fraca gestão do sistema". No gráfico 5, destaca-se uma forte incidência de

opinião sobre as subcategorias “fator humano” e “programas mal configurados” destacando a falha humana como um fator relevante na segurança dos SI havendo assim necessidade de traçar politicas de segurança que possam assim dirimir eventuais riscos.

Gráfico 5 - Distribuição das unidades de registo da categoria "Riscos do SI"

4.6. Transformações digitais na PNA

Hodiernamente as organizações estão cada vez mais dependentes das tecnologias, cada vez mais aumenta a aposta na digitalização de serviços, processos automáticos ou algoritmos para análise de dados. Esta adesão e dependência da tecnologia traz consigo um vasto leque de ameaças que podemos catalogar de riscos digitais (Opensoft, 2023). Nesta ordem de ideia, de forma unanime, todos entrevistados afirmam que as transformações digitais dos serviços da PNA colocariam a organização à mercê de ciberataques pelo facto de se tratar de uma instituição pública com várias informações sigilosas a nível nacional.

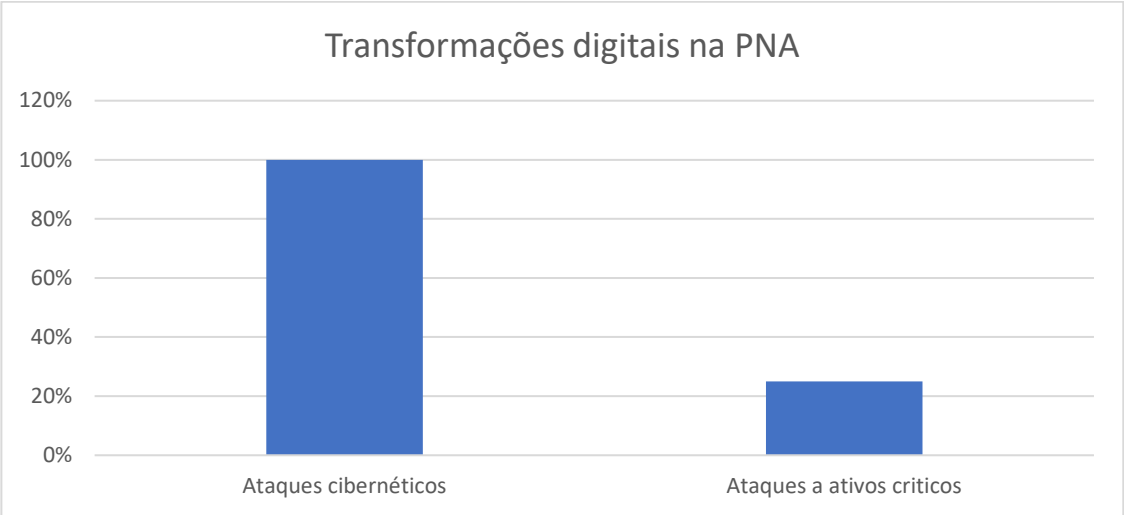


Gráfico 6 - Distribuição das unidades de registo da categoria "transformações digitais na PNA"

4.7. Vantagens do SI

As principais vantagens dos sistemas de informação incidem sobre o custo de mão de obra, otimizando desta forma tempo, tarefas e rotinas, permitem reunir em um só lugar todas as informações relevantes para a organização (características, sd). Neste sentido, 75% dos nossos entrevistados afirmam que um sistema de informação conferiria maior capacidade de identificação de suspeitos e de bens furtados ou roubados.

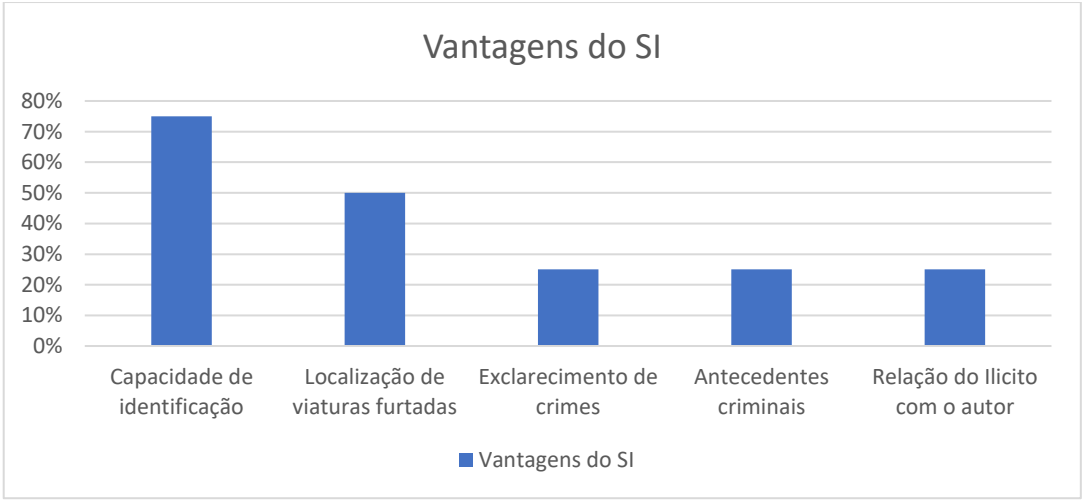


Gráfico 7 - Distribuição das unidades de registo da categoria "vantagens do SI"

4.8. Novas tecnologias na PNA

O desenvolvimento da tecnologia policial é muito importante para todos os cidadãos. Afinal, quanto mais aprimorado for o trabalho dos órgãos de segurança e fiscalização, menores serão os índices de criminalidade na sociedade, tendo em vista que a impunidade tende a diminuir (Piriquito, 2023). A PNA, cada dia mais, vai abraçando as novas tecnologias de modo a ganhar eficiência na execução das suas atribuições. Atualmente esta força de segurança conta com o auxílio de um sistema de geo-localização em tempo real dos operacionais no terreno, e também com o material informático em algumas esquadras.

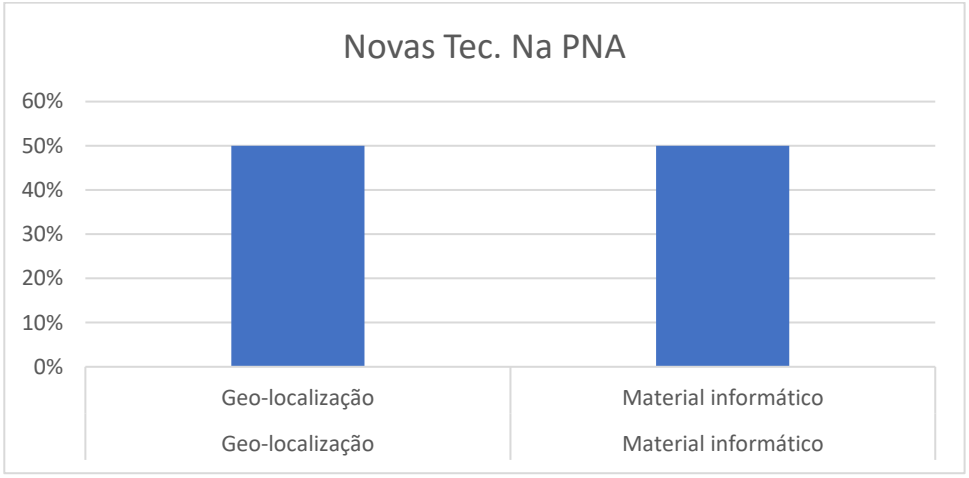


Gráfico 8 - Distribuição das unidades de registo da categoria "Novas Tec. na PNA"

Conclusão

A segurança dos sistemas de informação assume, nos dias de hoje, uma importância incontornável na sociedade. A partilha da informação a partir de meios tecnológicos torna-se num paradigma sobre o qual assentam processos de gestão da informação, gestão essa numa escala global, em grande parte devido à internet, marco tecnológico que revolucionou o paradigma do acesso e da partilha da informação. A internet tem sido apontada, por atores políticos e militares, como o quinto domínio operacional, à semelhança da terra, do mar, do ar e espaço (Craing & Valeriano, 2018 as *cited* in Geraldes, 2019).

Nos últimos anos, as fronteiras físicas entre Estados têm vindo a ser quebradas pelo caráter transacional das ameaças e riscos e os Estados, face à crescente desterritorialização da segurança acelerada ainda mais pela rede global, trocam e partilham informações planeiam e executam operações conjuntas, criam redes de peritos, por forma a prevenirem e combaterem os fenómenos que mais afetam a segurança coletiva. A internet é hodiernamente umas das forças motrizes da globalização e do progresso das comunicações, ela fornece meios inigualáveis de intercâmbio cultural, informativo e de ideias. Ela criou um nível antes inimaginável de interligação que beneficia o mundo dos negócios, governo e cidadãos. Contudo da mesma forma que a internet proporciona inúmeras vantagens, atua como um equalizador entre governos e atores não estatais (Elias, 2018).

A Internet constitui-se também como um novo ambiente de criminalidade organizada, para recrutamento e para radicalização e para a subversão e ativismo político com as mais diversas causas e conotações ideológicas. Verifica-se uma desterritorialização das ameaças e riscos, fazendo do mundo virtual, uma nova dimensão para a expansão das atividades ilícitas e para a ação das forças e serviços de segurança. A internet configura-se como um novo campo de batalha internacional (Elias, 2018).

Por mais preparação que possa haver nas organizações policiais torna-se difícil a prossecução das suas atribuições sem o suporte de um sistema de informação que possa auxiliar na salvaguarda do interesse público tendo em conta a quantidade de informação que chegam até estas. A informação sempre teve uma grande importância na atividade policial sendo que com a evolução da polícia os métodos de tratamento da informação foram melhorados, tornando-se assim num ativo imprescindível para a atividade policial.

A arquitetura tecnológica implementada na PSP tem como base uma estratégia descentralizada de processamento, mas de acesso descentralizados, consubstanciado operacionalmente no SEI. O SEI decorre do PESI, englobado no continuado processo de modernização da PSP, tendo como objetivo principal dotar todo dispositivo desta força de segurança de um SI capaz de suportar os seus processos operacionais e que, em simultâneo, seja catalisador da desejada uniformização e racionalização de procedimentos, bem como de uma nova forma de atuar mais eficaz e eficiente.

No presente trabalho ganhamos consciência da problemática que envolve os sistemas de informação que assenta essencialmente nos riscos que estão sujeitos, por um lado pelas ameaças existentes no ciberespaço, e por outro as políticas e mecanismos de segurança ineficazes, na medida que estes definem o foco da segurança que deve garantir, havendo falha neste domínio, poderá pôr-se em causa os dados existentes no sistema. Realça-se também o fator humano, sistemas mal configurados e a falta de confidencialidade como riscos aos sistemas de informação conforme demostrado no gráfico 5. Torna-se assim necessário a existência de barreiras físicas de controlo de acesso presencial aos computadores, mecanismo de autenticação eficazes das pessoas que fazem parte do grupo autorizado, mecanismos de registo adequados, eficazes e protegido, são medidas que reforçam e garantem a segurança do sistema.

Importa debruçar sobre o módulo de gestão de ocorrência que por sua vez é uma das componentes do módulo Gestão de Processos Policiais. Este módulo permite o registo de ocorrências e gestão de processos dos mais variados tipos, no âmbito da atividade operacional da PSP, tais como, crimes, contraordenações, entre outros (Cucu, 2018). O módulo Gestão de Ocorrências está interligado com o Repositório de Informações e Catálogo que por sua vez procede à alimentação do repositório de informações e acedendo à informação contida nas entidades fundamentais do repositório de informações (pessoas, veículos, objetos, locais e viaturas). O módulo de Informações Policiais por sua vez, permite aos polícias criar difundir informações para as restantes unidades policiais do país, suportando o objetivo do SEI de promover à viabilizar a efetiva integração e partilha de informação na PSP, obedecendo às regras de credenciação, e o princípio da necessidade de conhecer. A primeira defende que apenas tem acesso à informação os elementos policiais que estejam explicitamente credenciados para o efeito, já o princípio da necessidade de conhecer é referente ao ter acesso a informação apenas em caso de necessidade apesar do polícia ter credenciação que permita aceder à informação (Cucu, 2019; PESI, 2002).

Em relação às pesquisa e consulta de ocorrência, são apresentadas todas as informações relacionadas às mesmas, nomeadamente os "itens de interesse" nelas envolvidos. A partir da seleção destes é também possível passar diretamente à informação detalhada dos mesmos ou ao respetivo Catálogo, em articulação com o Repositório de Informações e Catálogo (PESI, 2002).

Como vimos no presente trabalho, as principais vantagens dos sistemas de informação incidem sobre o custo de mão de obra, otimizando desta forma tempo, tarefas e rotinas, permitem ainda reunir em um só lugar todas as informações relevantes para a organização. Segundo o que conseguimos apurar, nas entrevistas realizadas, um SI traria inúmeras vantagens, como por exemplo em caso de detenção de um cidadão, tendo um SI, seria possível agregar os antecedentes de modo a que se entregasse um dossier mais amplo para o Ministério Público. Geralmente quando um crime é cometido pelo mesmo individuo, a PNA não consegue fazer ligação com os múltiplos crimes cometidos pelo mesmo (entrevistando n.º 4).

Ao longo dos últimos tempos a PNA tem dado passos largos para o desenvolvimento tecnológico de modo a tornar eficiente o serviço policial. Todos os sistemas de informação, como o SEI, estão sujeitos a ataques cibernéticos, mas apesar desse risco é o desenvolvimento tecnológico que se confirma como o caminho mais seguro e eficiente. A inexistência de um sistema de informação, torna a comunicação lenta e em termos operacionais esse fator acaba por prejudicar a própria polícia. Para que se implemente um sistema de informação na PNA, há fatores externos à própria polícia que uma vez não solucionados tornar-se-á inviável a implementação de um sistema de informação que interligue todas as unidades policiais a nível nacional, pois para além de todo o material tecnológico necessário, infelizmente existem muitos municípios em Angola onde não há cobertura de internet o que tornaria inviável a expansão de um sistema de informação em todo país.

Apesar das várias conclusões retiradas deste estudo, houve algumas dificuldades ao longo da sua elaboração. Primeiramente o período disponível para a elaboração da presente dissertação foi manifestamente curto o que dificultou o desenvolvimento expectável nas diversas fases da investigação. Houve, também, dificuldades em obter respostas com os entrevistados, pois para a realização das entrevistas servimo-nos da Internet. Este facto configurou-se como uma complexidade a mais no presente estudo, e por último, tivemos

dificuldades na aquisição de bibliografia sobre a PNA, este facto contribuiu significativamente para o não cumprimento na íntegra do programa definido por nós.

Em suma, apraz-nos realçar que o presente estudo é uma mais-valia para o desenvolvimento tecnológico da PNA, pois foi o primeiro trabalho de investigação que abordou a temática das novas tecnologiasnomeadamente a necessidade de um SI nesta força de segurança.

Referências

Aarts, B., Bauer, M. (2000). Corpus construction: a principle for qualitative data collection. In: Martin, WB and Gaskell, G (Eds.) *Qualitative Researching: with text, image and sound*. (pp.19-37)

Accenture/PSP. (2002). *Plano estratégico de sistema de informação*. Accenture/ Polícia de Segurança Pública.

Accenture/PSP. (2004a). *SEI Sistema estratégico de informação, gestão e controlo operacional: Formação EURO 2004- guia do formando*. Accenture/ Polícia de Segurança Pública.

Accenture/PSP. (2004b). *SEI Sistema estratégico de informação, gestão e controlo operacional: informações policiais*. Accenture/ Polícia de Segurança Pública.

Accenture/PSP. (2004c). *SEI Sistema estratégico de informações, gestão e controlo operacional: gestão de grandes eventos*. Accenture/Polícia de Segurança Pública

Accenture/PSP. (2004d). *SEI Sistema estratégico de informações, gestão e controlo operacional: gestão de ocorrências*. Accenture/Polícia de Segurança Pública

Alecrim, E. (2001). *O que é Tecnologia da Informação*. O que é Tecnologia da Informação (TI)? (infowester.com)

Almeida, R. R. & Silva, R. A. (2020). *Local do crime e a importância da preservação das provas*. php4PLDCK.pdf (conteudojuridico.com.br)

Antunes, A. & Rodrigues, B. (2018). *Introdução à cibersegurança: a internet, os aspetos legais e a análise digital forense.* FCA- Editora de Informática, Lda.

Assembleia Constituinte. (2010). *Constituição da república de Angola*. I Série n.º 23 de 5 de fevereiro de 2010.

Bardin, L. (1977). *Análise de conteúdo*. Edições 70

Bardin, L. (2008). *Análise de conteúdo* (4ª ed.). Edições 70

Barreto, J. M., & Barreto, E. F. (2019). *Gestão de Segurança*. Universidade Federal da Bahia.

Bogdan, R. & Biklen, S. (1994). *Investigação qualitativa em educação: uma introdução à teoria do método.* Porto editora

Caetano, D. (2020). *Introdução à segurança da informação: gestão de risco.* CCT0894_aula04 (1).pdf

Canelas, I. C. F. N. (2017). *Sistema Estratégico de Informação o módulo de pedidos externos: dimensões da funcionalidade*. (Curso de Direção e Estratégia Policial, Instituto Superior de Ciências Policiais e Segurança Interna).

Características. (s.d.). *Sistema de informação*. Sistema de informação - usos, exemplos e características (caracteristicas.pt)

Centro Nacional de Cibersegurança Portugal. (2022). *Cibersegurança em Portugal*. Observatório de cibersegurança.

Claro, R. B. M. (2018). O Panorama securitário atual um olhar sobre a península ibérica. In E. Correia (Ed.), *políticas publicas de segurança*. (pp. 15-59). (coord. Eduardo Pereira Correia).

Coutinho, C. D. (2020). *Metodologia de investigação em ciências sociais e humanas: teoria e prática* (2ª ed.). Almedina S.A.

Cucu V. E. F. (2019). *A segurança dos sistemas de informação da PSP: O sistema estratégico de informação (SEI).* (Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna).

Decoster, S. R. A., & Souza, C. A. (2014). Fundamentos de sistemas de informação. In E. P. V. Prado & C. A. Souza (eds.), *Aplicações corporativas* (PP. 37-39). Elsevier Editora Ltda.

Decreto-Lei n.º 252/94, de 20 de outubro- *Diário da República*, Série I- A, n.º 243, 6374-6376. Presidência do Conselho de Ministros. (Regime da Proteção Jurídica de Programas de Computador).

Decreto-Lei n.º 135/99 de 22 de abril – *Diário da República*, Série I-A, n.º 94, 2126-2135. Presidência de Conselho de Ministros. (Estabelece medidas de modernização administrativa).

Decreto-Lei n.º 290-D/99, de 2 de agosto- *Diário da República*, Série I-A, I.º Suplemento, n.º 178, 4990-(2) a 4990-(11). Ministério da Ciência e da Tecnologia. (Regime Juridico dos documentos eletrónicos e da assinatura digital).

Decreto-Lei n.º 203/206, de 27 de outubro – *Diário da República*, 1.ª Série, n.º 203, 7441-7446. Ministério da Administração Interna. (Lei Orgânica do Ministério da Administração Interna).

Decreto-Lei n.º 3/2012, de 16 de janeiro – *Diário da República*, 1.ª Série, n.º 3, 174-177. Presidência do Conselho de Ministros. (Orgânica do Gabinete Nacional de Segurança).

Decreto-Lei n.º 69/2014, de 09 de Maio – *Diário da República*, I.ª Série, n.º 89, 2712-2719. Presidência do conselho de Ministros. (Termos de funcionamento do Centro Nacional de Cibersegurança do Gabinete Nacional de Segurança).

Decreto Lei n.º 243/2015, de 19 de outubro – *Diário da República*, I. ª Série, n.º 204, 9054-9086. Ministério da Administração Interna. (Estatuto do Pessoal Policial da Polícia de Segurança Pública).

Decreto Presidencial n.º 83/21 de 12 de abril *Diário da República*. I Série – N.º 63. Aprova o Estatuto Orgânico do Centro Integrado de Segurança Pública.

Decreto Presidencial n.º 152/19 de 15 de maio *Diário da República.* I Série- Nº 65, Estatuto Orgânico da Polícia Nacional de Angola. Assembleia da República.

Decreto Regulamentar n.º 5/95, de 31 de janeiro - Diário da República, Série I-B, n.º 26, 582-584. Ministério da administração Interna. (Base de Dados Pessoais da Polícia de Segurança Pública).

Despacho n.º 034/GAB.CGPNA/2020. *Regulamento orgânico da Direção de Informações Policiais da Polícia Nacional de Angola*. CGPN.

Despacho n.º 044/GAB.CGPNA/2020. *Regulamento orgânico do Comando Provincial de Luanda da Polícia Nacional de Angola*. CGPN.

Direcção de Informações Policiais. (2020). *Relatório de informação do projecto de regulamento orgânico do departamento de informações policiais do comando provincial da polícia nacional*. Polícia Nacional de Angola.

Direção Geral de Administração Interna. (2010). *Schengen legislação: sistema de informação shengen e cooperação policial*. Gabinete Nacional S.I.R.E.N.E

Eco, U. (1998). *Como se faz uma tese em ciências sociais* (ed 7ª). Editorial Presença

Eiras, A. (1992). *Segredo de justiça e controlo de dados pessoais informatizados*. Coimbra Editora.

Elias, L. (2018). *Ciências policiais e segurança interna: desafios e prospetiva*. ISCPSI-ICPOL.

Fernandes, J. J. A. (2014). Os desafios da segurança contemporânea: estado, identidade e multiculturalismo. Artes Gráficas, Lda.

Feiteira, A (2015). Administração pública da segurança. In J. B. Gouveia & S. Santos (eds.), *Enciclopédia de direito e segurança*. ALMEDINA, S.A.

Fonseca, G., Claro, J. M., Sá, L., & Fontes, J. (2002). *Legislação administrativa básica* (4ª ed.). Coimbra Editora.

Flick, U. (2005). *Método qualitativo na investigação científica*. Monitor

Flick, U., Netz, S., Silveira, T. (2004). *Uma introdução à pesquisa qualitativa*. (2ª ed). Bookman.

Gabinete do Secretário-Geral. (2022). *Relatório Anual de Segurança Interna*. Sistema de Segurança Interna.

Geraldes, S, M. (2018). *A estratégia de cibersegurança da União Europeia: catastrófica, realista e/ou otimista*. Instituto Universitário de Lisboa (ISCTE-IUL), Centro de Estudos Internacionais.

Ghiglione, R., Matalon, B. (2001). *O inquérito: teoria e prática*. Celta Editora, Lda

Gouveia, L. M. B. (1996). *Sistemas de informação*. si_texto.pdf (ufp.pt)

Guimarães, E. M. P. & Évora, Y. D. M. (2004). *Sistema de Informação: instrumento para tomada de decisão no exercício da gerência*. Sem título-1 (scielo.br).

Henriques, T. (2019*) Gestão de sistemas de informação: pessoas, equipas e mudança organizacional*. FCA Editora de Informática, Lda.

Issenguele, M. & Cabombo, A. (2021). *Sistema de gestão de informações de casos e eventos criminais*. CISP

Jornal de Angola. (2022). *Rede de roubo de viaturas liderada por estrangeiros*. Jornal de Angola - Notícias - Rede de roubo de viaturas liderada por estrangeiros

Krippendorff, K. (2004). *Contente analysis: Na introduction to its methodology* (2ª ed.) Thousand oaks, CA: Sage Publications.

Lei n.º 7/90, de 20 de fevereiro – *Diário da República*, I. ª Série, n.º 43,670-684. Assembleia da República. (Regulamento Disciplinar da Polícia de Segurança Pública).

Lei n.º 2/94, de 19 de fevereiro- *Diário da República*, nº 42/1994, Série I-A. Assembleia da República. (Regula os mecanismos de controlo e fiscalização do sistema de informação).

Lei n.º 41/2004, de 18 de agosto- *Diário da República*, Iª Série, nº 194, 5241-5245. Assembleia da República. (Lei da Proteção da Privacidade no Sector das Comunicações Eletrónica)

Lei n.º 53/2007, de 31 de agosto. *Diário da República*, I.ª n.º 168/2007, 6065-6074. Assembleia da República. (Lei Orgânica da PSP).

Lei n.º 32/2008, de 17 de julho. *Diário da República*, I.ª Série, n.º 137, 4454-4458. Assembleia da República. (Lei relativa a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações).

Lei n.º 109/2009, de 15 de setembro. *Diário da República*, I.ª Série, n.º 179, 6319-6325. Assembleia da República. (Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a decisão quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro).

Lei n.º 46/2018, de 13 de agosto. *Diário da República*, I.º Série, nº 155, 4031-4037. Assembleia da República. (Regime Jurídico da Segurança no Ciberespaço).

Lei n.º 58/2019, de 8 de agosto. Diário da República, Iª Série, N.º 151. Assembleia da República. (Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento Europeu e do conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados).

Lei n.º 59/2019, de 8 de agosto. *Diário da República*, Iª Série, mº 151/2019. Assembleia da República (aprova a lei relativa ao tratamento de dados pessoais para efeito de prevenção, detenção, investigação ou repressão de informações penais)

Lei n.º 6/20, de 24 de março. *Diário da República*. I Série- N.º 34- de 24 março de 2020

Lemos, J. M. L. (2011). *Sistemas de informação e qualidade de dados: o caso do sistema estratégico de informação, gestão e controlo operacional da polícia de segurança pública* (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Intena

Lopes, E. R., Bau, J., & Noivo, M. A. (1998). Globalização dos mercados e as políticas de internacionalização. que resposta portuguesa. In Sociedade de Geografia de Lisboa (eds.), *África século XXI os desafios da globalização e as respostas do desenvolvimento*. (pp. 13-26) Sociedade de Geografia de Lisboa.

Mamede, H. S. (2006). *Segurança informática nas organizações*. Editora de Informática, Lda

Marconi, M. D., & Lakatos, E. M. (2003). *Fundamentos de metodologia científica* (5ª ed.). Atlas S.A.

Martins, J. C. L. (2021). *Gestão de segurança da informação e cibersegurança nas organizações: sistema e método*. SILABAS & DESAFIOS- UNIPESSOAL LDA.

Moresi, E. A. D. (2000). *Delineando o valor do sistema de informação de uma organização*. *1-2000 (scielo.br)

Moutinho, J. L., Salinas, H. Sequeira, E. V., & Marques, P. g. (coords). (2020). *Homenagem ao professor doutor Germano Marques da Silva*. Universidade Católica Editora.

Neto, N. P. (2009). *Crimes cibernéticos: necessidade de uma legislação especifica no Brasil*. [Monografia, Faculdade de Ensino Superior da Paraíba]. [PDF] CRIMES CIBERNÉTICOS: necessidade de uma legislação específica no Brasil. - Free Download PDF (silo.tips)

Neto, B. M. (2010). *Informações Policiais: importância na tomada de decisão na Polícia Nacional de Angola (o caso do Comando Provincial do Kuanza-Norte).* [Dissertação de Mestrado não publicada]. Instituto Superior de Ciência Policiais.

Neves, P. S. (2020). *Proteção de Dados Pessoais em Angola: agência de proteção de dados em funcionamento*. FCB Global.

Oliveira, J. F. (2015). *Manutenção da ordem pública em democracia*. Instituto Superior de Ciências Policiais e Segurança Interna.

Opensoft (2023). *Risco digital: o que é e como geri-los na sua organização*. Risco digital: o que é e como geri-lo na sua organização? - Opensoft

Pais, L. G. (2004). *Uma história das ligações entre a psicologia e o direito em Portugal: perícia psiquiátricas médico-legais e perícia sobre a personalidade como analisadores* [Tese de doutoramento não publicada]. Faculdade de Psicologias e de ciências da Educação da Universidade do Porto.

Pereira, M. R. (2019). *Big data: O caso do sistema estratégico de informação, gestão e controlo operacional da polícia de segurança pública* [Dissertação de Mestrado não publicada]. Instituto Superior de Ciências Policiais e Segurança Interna.

Piriquito, M. (2023). Tecnologia policial: como órgãos de segurança e fiscalização se beneficiam da inovação. Tecnologia policial: como a segurança se beneficia da inovação (futurecom.com.br)

Poiares, N. & Marta, R. (2018). *Segurança interna: desafios na sociedade de risco mundial*. Instituto Superior de Ciências Policiais e Segurança Interna.

Polícia de Segurança Pública. (2002). *Plano estratégico de sistema de informação*.

Polícia de Segurança Pública. (2020) *Estratégia PSP 2020/2022*. Estratégia PSP 2020_2022.pdf

Polícia de Segurança Pública. (2021). *Informação/proposta*. Nº 132/NPID/2021.

Presidência do Conselho de Ministros. (2018). Nota de comunicação sobre o Regulamento Geral de Proteção de Dados. ficheiro.aspx (portugal.gov.pt)

Quivy, R., Campenhoudt, L. V. (2005). *Manual de investigação em ciências sociais* (5ª ed.). Gradiva.

Ramos, A. D. (2015). Cibersegurança VS a privacidade na internet: nótulas sobre um "estado de guerra" latente. In Eduardo Pereira Correia (coord.), *Liberdade e segurança*. (pp. 133-152). ISCPSI-ICPOL.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral Sobre a Proteção de Dados).

Reis, J. L., Ferreira, R., Sousa, R. D. (2022). Função sistemas de informação nas organizações portuguesas. In Isabel Ramos, Rui Dinis Sousa & Rui Quaresma (coords.), *Sistemas de informação: diagnósticos e prospetivas*. (pp. 109-145). Sílabo, Lda

Resolução de Conselho de Ministros nº 50/88, de 8 de setembro – Diário da República, I.ª Série, n.º 279, 4772-4800. Presidência do Conselho de ministros. Aprova as instruções sobre a segurança de matérias classificadas- SEGNAC 1).

Resolução do Conselho de Ministros n.º 5/90, de 28 de setembro- Diário da República, I.ª Série, I.º Suplemento, n.º 49, 806-(2) a 806-(17). Presidência do Conselho de Ministros. (Aprova as instruções sobre a segurança informática- SEGNAC 4).

Resolução da Assembleia da República n.º 88/2009, de 15 de Setembro – Diário da República, I.ª Série, n.º 179, 6354-6378. Assembleia da República. (Aprova a Convenção sobre Cibercrime).

Resolução do Conselho de Ministros n.º 41/2018, de 28 de março – Diário da República, I.ª Série, n.º 62, 1424-1430. Presidência do Conselho de Ministros. (Define orientações técnicas para a administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados).

Ribeiro, J. (2012). *Proteção de direitos individuais, privacidade e dados pessoais*. Comissão Nacional de Proteção de Dados.

Rodrigues, L. A. S. (2000). *Arquitetura dos Sistemas de Informação*. (Dissertação de Mestrado, Universidade do Minho).

Sarmento, M. (2013). *Guia prático sobre a metodologia científica para a elaboração, escrita e apresentação de teses de doutoramento, dissertações de mestrado e trabalho de investigação aplicada* (3ª ed.).

Silva, A. S., Pinto, J. M. (1989). *Metodologia das ciências sociais* (3ª ed.). Biblioteca das Ciências do Homem. Edições Afrontamento.

Silveira, M. D. P. (2004). *Efeitos da globalização e da sociedade em rede via internet na formação de identidades contemporâneas*. SciELO - Brasil - Efeitos da globalização e da sociedade em rede via Internet na formação de identidades contemporâneas Efeitos da globalização e da sociedade em rede via Internet na formação de identidades contemporâneas

Silva, A. S., Pinto, J. M. (s.d.). *Metodologia das ciências sociais* (6ª ed.). Biblioteca das Ciências do Homem. Edições Afrontamento.

Sarmento, M. (2013*). Metodologia científica para elaboração, escrita e apresentação de teses*. Universidade Lusíadas.

Santo, P. E. (2010). *Introdução à metodologia das ciências sociais génese, fundamentos e problemas*. SÍLABO, LDA.

Sharma, R. (2018). *O clube das 5 da manhã: conquiste os seus dias e transforme a sua vida*. HarperCollins Publishers Ltd.

Sousa, J. L. C. H. (2022). *O tráfico de armas ligeiras: implicações para a paz e a segurança na região dos grandes lagos*. Academia de Ciências Sociais e tecnologias.

Sousa, S. (2009). *Tecnologias de informação: o que são? Para que servem* (6ª ed). FCA Editora de Informática, Lda.

Telo, A. J., Borges, J. V., Pires, N. L. (2018). *Dar uma razão à força e uma força à razão*. Tipografia Lousanense Lda.

Torres, J. E. M. (2014). *Gestão de riscos: No planeamento, execução e auditoria de segurança*. Instituto Superior de Ciências Policiais e Segurança Interna.

Valente, M. M. G. (2019) *Teoria geral do direito policial* (6ª ed). Almedina.

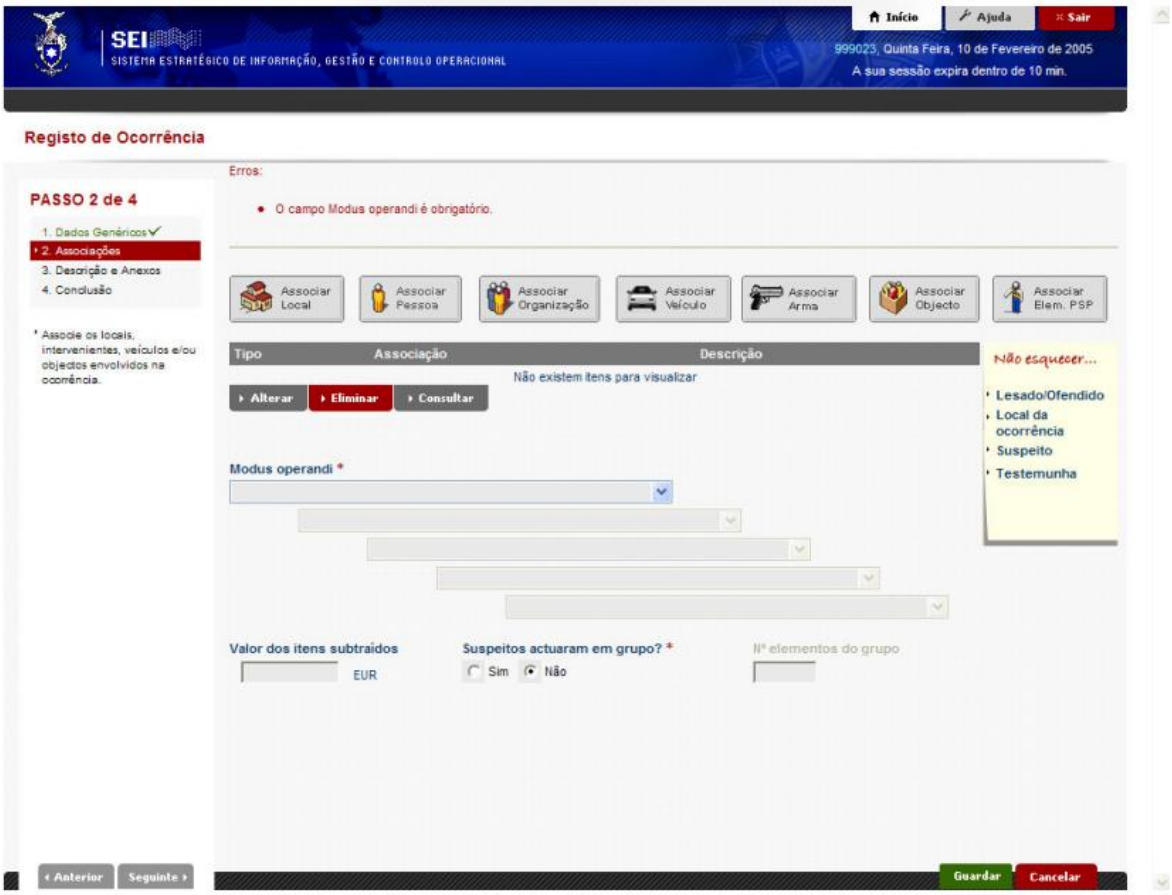
Varano, S. P., Cancino, J. M., Glass, J., & Enriquez, R. (2007). *Police information systems*. School of Justice Studies Facultly Papers. Edited by J. Schafer.

Zúquete, A. (2013). *Segurança em redes informáticas* (4ª ed.). FCA Editora de Informática

Zúquete, A. (2021). *Segurança em redes informáticas* (6ª ed.). FCA Editora de Informática

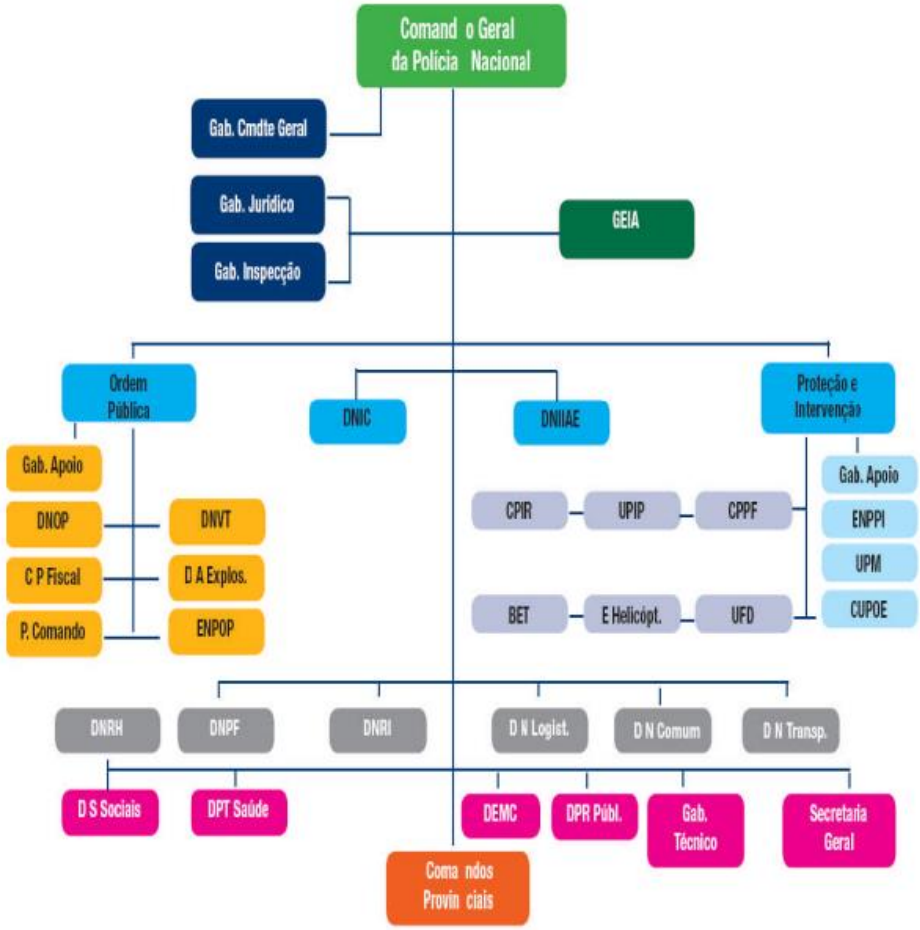
Anexo

Anexo I- Interface do Sistema Estratégico de Informação, Gestão e Controlo Operacional



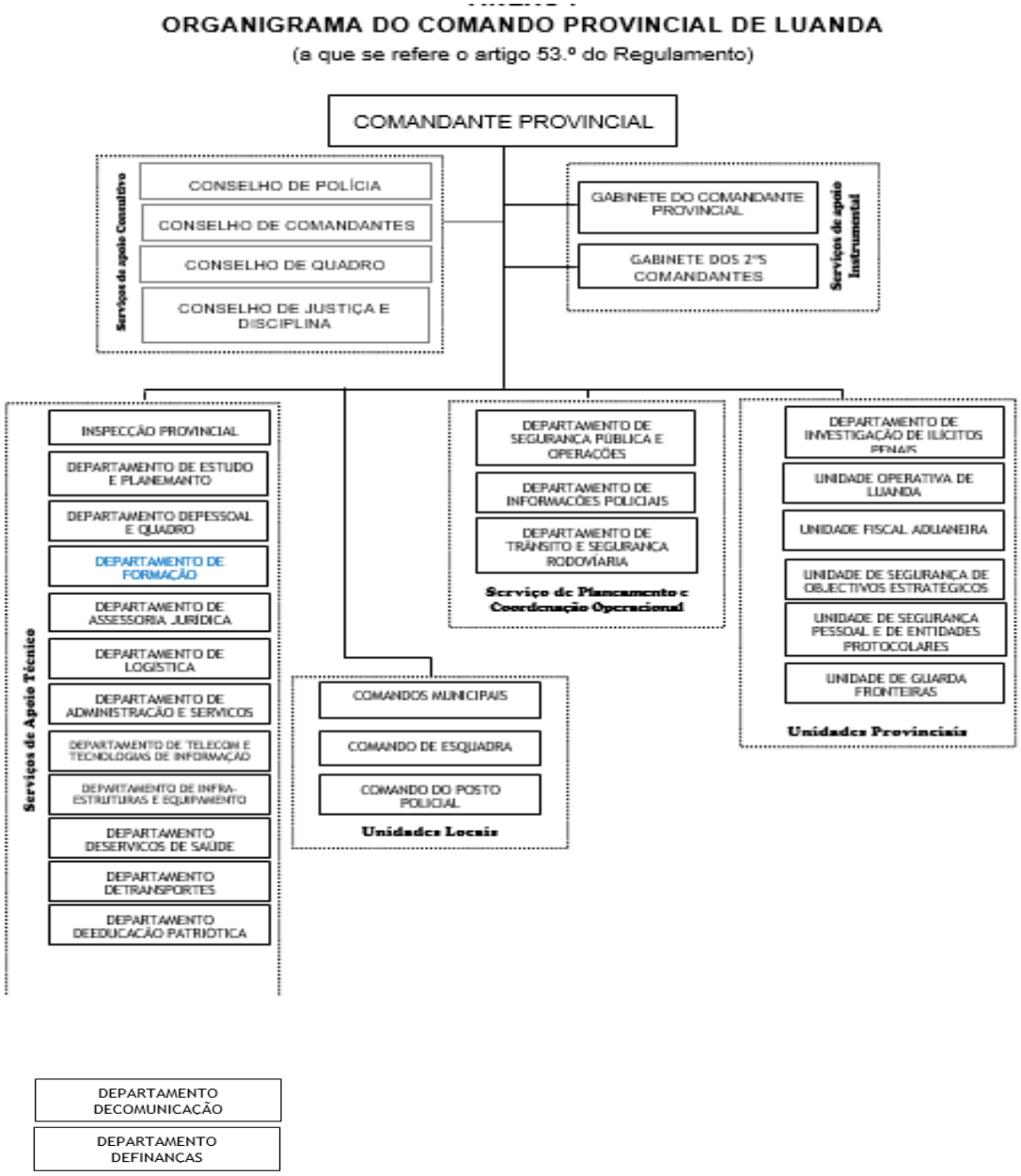
Fonte: Projeto SEI formação versão EURO

Anexo II- Organograma da Polícia Nacional de Angola



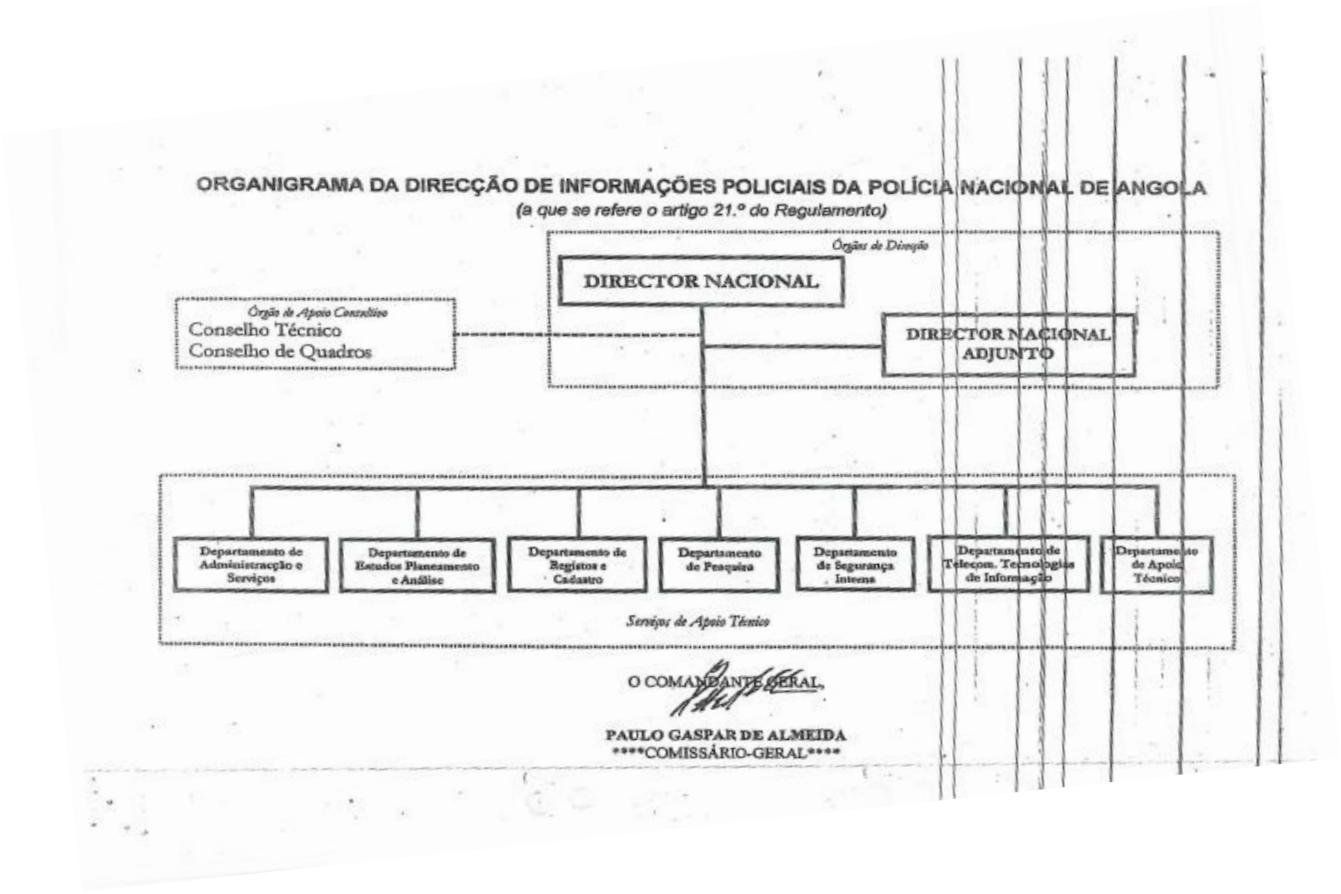
Fonte: Adaptação do Gabinete de Estudos Informação e Análise do Ministério do Interior

Anexo III- Organograma do Comando Provincial de Luanda



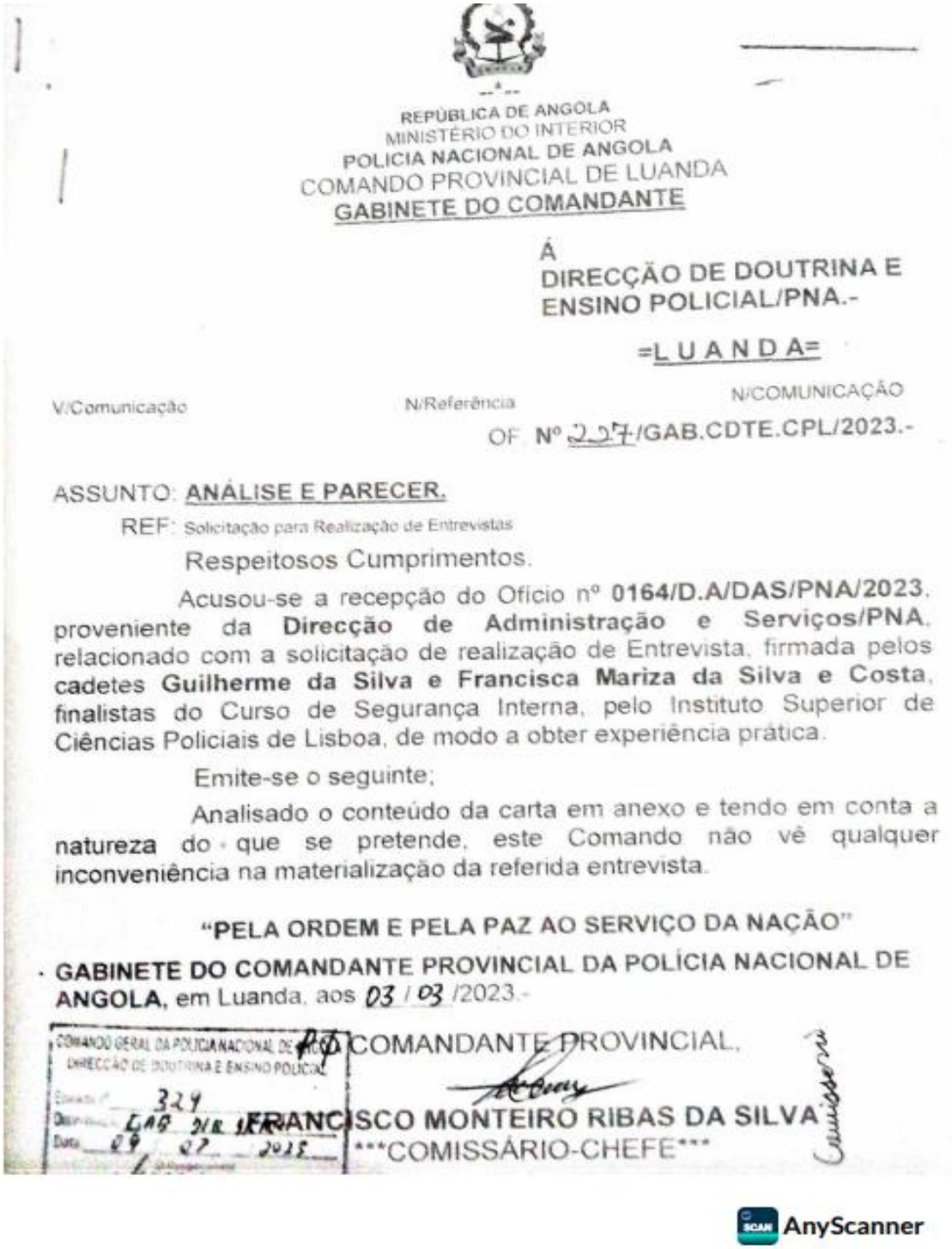
Fonte: Despacho n.º 044/GAB.CGPNA/2020. Regulamento Orgânico do Comando Provincial de Luanda da Polícia Nacional de Angola

Anexo IV- Organograma da Direção de Informações Policiais da Polícia Nacional de Angola



Fonte: Despacho n.º 034/GAB.CGPNA/2020 Regulamento Orgânico da Direção de informações Policiais da Polícia Nacional de Angola.

Anexo V- Aprovação de realização de entrevista



REPÚBLICA DE ANGOLA
MINISTÉRIO DO INTERIOR
POLICIA NACIONAL DE ANGOLA
COMANDO PROVINCIAL DE LUANDA
GABINETE DO COMANDANTE

Á
DIRECÇÃO DE DOUTRINA E ENSINO POLICIAL/PNA.-

=L U A N D A=

V/Comunicação | N/Referência | N/COMUNICAÇÃO
OF Nº 227/GAB.CDTE.CPL/2023.-

ASSUNTO: **ANÁLISE E PARECER.**

REF: Solicitação para Realização de Entrevistas

Respeitosos Cumprimentos.

Acusou-se a recepção do Ofício nº **0164/D.A/DAS/PNA/2023**, proveniente da **Direcção de Administração e Serviços/PNA**, relacionado com a solicitação de realização de Entrevista, firmada pelos **cadetes Guilherme da Silva e Francisca Mariza da Silva e Costa**, finalistas do Curso de Segurança Interna, pelo Instituto Superior de Ciências Policiais de Lisboa, de modo a obter experiência prática.

Emite-se o seguinte;

Analisado o conteúdo da carta em anexo e tendo em conta a natureza do que se pretende, este Comando não vê qualquer inconveniência na materialização da referida entrevista.

"PELA ORDEM E PELA PAZ AO SERVIÇO DA NAÇÃO"

GABINETE DO COMANDANTE PROVINCIAL DA POLÍCIA NACIONAL DE ANGOLA, em Luanda, aos 03 / 03 /2023.-

COMANDO GERAL DA POLICIA NACIONAL DE ANGOLA
DIRECÇÃO DE DOUTRINA E ENSINO POLICIAL
Entrada nº 329
Data 09 03 2023

O COMANDANTE PROVINCIAL,

FRANCISCO MONTEIRO RIBAS DA SILVA
COMISSÁRIO-CHEFE

AnyScanner

Fonte: Direção de Doutrina e Ensino Policial da Polícia Nacional de Angola

Apêndice

Apêndice I- Solicitação de recolha de dados

À

SUA Ex.ª CHEFE DAS OPERAÇÕES DO

COMANDO PROVINCIAL DE LUANDA/PNA

= L U A N D A =

ASSUNTO: SOLICITAÇÃO DE AUTORIZAÇÃO DE RECOLHA DE DADOS PARA ELABORAÇÃO DA DISSERTAÇÃO DE MESTRADO EM CIÊNCIAS POLICIAIS.

Cordiais saudações.

Em cumprimento do **Despacho nº 169/GAB.CGPN/2017**, de sua Excelência Comandante-geral da Polícia Nacional, respetivo à bolsa de estudo para a formação do efetivo da Polícia Nacional de Angola, no instituto Superior de Ciências Policiais e Segurança interna (ISCPSI), em Lisboa, na República de Portugal, o agente de 1ª classe **Guilherme da Silva**, contactável por watssap +244926317171.

Encontrando-se na fase final do curso, onde para a obtenção do título de mestre é obrigatório a elaboração de uma dissertação e considerando as limitações concernentes a deslocação ao país, a fim de se ter contacto direto, tanto com a matéria de interesse como com o público-alvo, venho por este meio, mui respeitosamente, solicitar a sua excelência, a disponibilização de materiais didáticos (de uso policial na área a dissertar), e também um mediador no exercício do contacto com os efetivos-alvos de aplicação dos instrumentos de recolha de dados (entrevista) para o estudo, nomeadamente efetivos com funções especificas em matéria de comando, conforme for a dissertação e as necessidades.

Adianta-se, no entanto que as entrevistas sejam aplicadas a todos comandantes municipais do CPL, e a temática de interesse a se dissertar é:

"Importância do Sistema Estratégico de Informações (SEI): Proposta de implementação na PNA".

Sem mais nenhum assunto reitero as minhas efusivas saudações

Com os melhores cumprimentos,

Lisboa, Instituto Superior de Ciências Policiais e Segurança Interna, aos 03 de fevereiro de 2023

Bolseiro/PNA

Guilherme da Silva

Guilherme da Silva

Fonte: elaborado pelo autor.

Apêndice II: Análise de conteúdo por questão de entrevista

Categoria	Subcategoria	Unidade de registo	Entrevistados				Unidades de enumeração	Resultados (%)
			1	2	3	4		
Necessidade de um SI na PNA	Identificação e localização	1.1	X	X	X	X	4	100%
	Fluidez e eficiência na procura	1.2	X	X	X	X	4	100%
	Necessidades (…) segurança pública	1.3		X			1	25%
	Crimes rodoviário	1.4		X			1	25%
	Fornecimento de dados relevantes	1.5			X		1	25%
Total das unidades de numeração							11	

Tabela 1- Apêndice II: Análise de conteúdo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice III: Matriz das unidades de contexto e de registo por questão de entrevista referente a primeira questão.

Entrevistado	Unidade de Contexto	Unidade de registo
1	Identificação e Localização	1.1
	Fluidez e eficiência na procura	1.2
2	Identificação e Localização	1.1
	Necessidades (…) de segurança pública	1.3
	Crimes rodoviários	1.4
	Fluidez e eficiência na procura	1.2
3	Identificação e Localização	1.1
	Fornecimento de dados relevantes	1.5
	Fluidez e eficiência na procura	1.2
4	Identificação e Localização	1.1
	Fluidez e eficiência na procura	1.2

Tabela 2 - Apêndice III: Matriz das unidades de contexto e de registo por questão de entrevista referente a primeira questão (Fonte: Elaborado pelo autor)

Apêndice IV: Análise de conteúdo por questão de entrevista

Categoria	Subcategoria	Unidade de registo	Entrevistados				Unidades de enumeração	Resultados (%)
			1	2	3	4		
Partilha da informação	Partilha por telemóveis	2.1	x				1	25%
	Partilha por WhatsApp	2.2	x				1	25%
	Partilha por radio de comunicação	2.3	x			x	2	50%
	Informações escritas	2.4	x				1	25%
	Relatórios periódicos	2.5	x				1	25%
	Sistema Integrado/ base de dados	2.6		x	x		2	50%
Total das unidades de numeração							8	

Tabela 3 - Apêndice IV: Análise de conteúdo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice V: Matriz das unidades de contexto e de registo por questão de entrevista

Entrevistado	Unidade de Contexto	Unidade de registo
1	Partilha por telemóvel	2.1
	Partilha por WhatsApp	2.2
	Partilha por Radio de comunicação	2.3
	Informações escritas	2.4
	Relatórios periódicos	2.5
2	Sistema integrado/base de dados	2.6
3	Sistema integrado/base de dados	2.6
4	Partilha por rádio de comunicação	2.3

Tabela 4 - Apêndice V: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice VI: Matriz das unidades de contexto e de registo por questão de entrevista

Categoria	Subcategoria	Unidade de registo	Entrevistados				Unidades de enumeração	Resultados (%)
			1	2	3	4		
Segurança da informação Criminal na PNA	Interpretação e Análise	3.1	x	x		x	3	75%
	Difusão	3.2	x			x	2	50%
	Secreta e confidencial	3.3		x			1	25%
	Recolha da informação	3.4		x		x	2	50%
Total das unidades de numeração							8	

Tabela 5 - Apêndice VI: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice VII: Matriz das unidades de contexto e de registo por questão de entrevista

Entrevistado	Unidade de Contexto	Unidade de registo
1	Interpretação e Análise	3.1
	Difusão	3.2
2	Secreta e confidencial	3.3
	Interpretação e Análise	3.1
	Recolha da informação	3.4
4	Interpretação e Análise	3.1
	Recolha da informação	3.4
	Difusão	3.2

Tabela 6 - Apêndice VII: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice VIII: Matriz das unidades de contexto e de registo por questão de entrevista

Categoria	Subcategoria	Unidade de registo	Entrevistados				Unidades de inumeração	Resultados (%)
			1	2	3	4		
Abordagem Proativa/ Reativa	Proativa	4.1	x	x	x	x	4	100%
	Prevenção	4.2	x		x		2	50%
	Tratamento de informações criminais	4.3		x	x		2	50%
	Necessidades de segurança	4.4			x	x	2	50%
Total das unidades de numeração							10	

Tabela 7 - Apêndice VIII: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice IX: Matriz das unidades de contexto e de registo por questão de entrevista

Entrevistado	Unidade de Contexto	Unidade de registo
1	Proativa	4.1
	Prevenção	4.2
2	Proativa	4.1
	Tratamento das informações criminais	4.3
3	Proativa	4.1
	Prevenção	4.2
	Necessidades de segurança	4.4
4	Proativa	4.1
	Necessidades de segurança	4.3

Tabela 8 - Apêndice IX: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice X: Matriz das unidades de contexto e de registo por questão de entrevista

Categoria	Subcategoria	Unidade de registo	Entrevistados				Unidades de numeração	Resultados (%)
			1	2	3	4		
Riscos do SI	Fator Humano	5.1	x		x	x	3	75%
	Programas mal configurados	5.2	x	x	x	x	4	100%
	Falta de confidencialidade	5.3		x			1	25%
	Fuga de Informação	5.4		x	x		2	50%
	Fraca gestão do sistema	5.5		x			1	25%
Total das unidades de numeração							11	

Tabela 9 - Apêndice X: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice XI: Matriz das unidades de contexto e de registo por questão de entrevista

Entrevistado	Unidade de Contexto	Unidade de registo
1	Fator Humano	5.1
	Programas mal configurados	5.2
2	Programas mal configurados	5.2
	Falta de confidencialidade	5.3
	Fuga de Informação	5.4
	Fraca gestão do sistema	5.5
3	Programas mal configurados	5.2
	Fator Humano	5.1
	Fuga de Informação	5.4
4	Fator Humano	5.1
	Programas mal configurados	5.2

Tabela 10 - Apêndice XI: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice XII: Matriz das unidades de contexto e de registo por questão de entrevista

Categoria	Subcategoria	Unidade de registo	Entrevistados				Unidades de inumeração	Resultados (%)
			1	2	3	4		
Transformações digitais na PNA	Ataques cibernéticos	6.1	x	x	x	x	4	100%
	Ataques a ativos críticos	6.2	x				1	25%
Total das unidades de numeração							5	

Tabela 11 - Apêndice XII: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice XIII: Matriz das unidades de contexto e de registo por questão de entrevista

Entrevistado	Unidade de Contexto	Unidade de registo
1	Ataques cibernéticos	6.1
	Ataques a ativos críticos	6.2
2	Ataques cibernéticos	6.1
3	Ataques cibernéticos	6.1
4	Ataques cibernéticos	6.1

Tabela 12 - Apêndice XIII: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice XIV: Matriz das unidades de contexto e de registo por questão de entrevista

Categoria	Subcategoria	Unidade de registo	Entrevistados				Unidades de enumeração	Resultados (%)
			1	2	3	4		
Vantagens do SI	Capacidade de identificação	7.1		x	x	x	3	75%
	Localização de viaturas furtadas	7.2		x	x		2	50%
	Esclarecimento de crimes	7.3		x			1	25%
	Antecedentes criminais	7.4				x	1	25%
	Relação do Ilícitos com o autor	7.5				x	1	25%
Total das unidades de numeração							8	

Tabela 13 - Apêndice XIV: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice XV: Matriz das unidades de contexto e de registo por questão de entrevista

Entrevistado	Unidade de Contexto	Unidade de registo
2	Capacidade de identificação	7.1
	Localização de viaturas furtadas	7.2
	Esclarecimento de crimes	7.3
3	Capacidade de identificação	71
	Localização de viaturas furtadas	7.2
4	Capacidade de identificação	7.1
	Antecedentes criminais	7.4
	Relação do Ilícitos com o autor	7.5

Tabela 14 - Apêndice XV: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice XVI: Matriz das unidades de contexto e de registo por questão de entrevista

Categoria	Subcategoria	Unidade de registo	Entrevistados				Unidades de numeração	Resultados (%)
			1	2	3	4		
Novas Tec. Na PNA	Geo-localização	8.1	x			x	2	50%
	Material informático	8.2	x			x	2	50%
Total das unidades de numeração							4	

Tabela 15 - Apêndice XII: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice XVII: Matriz das unidades de contexto e de registo por questão de entrevista

Entrevistado	Unidade de Contexto	Unidade de registo
1	Geo-localização	8.1
	Material informático	8.2
2	Geo-localização	8.1
	Material informático	8.2

Tabela 16 - Apêndice XIII: Matriz das unidades de contexto e de registo por questão de entrevista (Fonte: Elaborado pelo autor)

Apêndice XVIII: Entrevistas a oficiais da Polícia Nacional de Angola

A presente entrevista insere-se no âmbito da dissertação de mestrado para Obtenção do grau de mestre do curso de Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório desta dissertação é "Importância do Sistema Estratégico de Informação: Proposta de Implementação na Polícia Nacional de Angola", sendo orientador e coorientador da mesma o senhor Superintendente José Joaquim Antunes Fernandes e o senhor Subintendente Carlos Alberto Batista Correia, respetivamente.

Pretende-se com esta dissertação perceber como se adequaria o Sistema Estratégico de Informações (SEI) na Polícia Nacional de Angola (PNA), compreender como o SEI melhoraria o trabalho operacional na PNA e quais as medidas necessárias para a sua implementação.

Entrevistado nº 1

Cargo/Posto- Comandante Municipal/ Superintendente

Local- Belas

Data-16/03/23

Guião

O Sistema Estratégico de Informação (SEI), é uma ferramenta de gestão policial onde são registadas todas as ocorrências, bem como a tramitação documental (interna e externa) dos expedientes, estando interligada com outras bases de dados ao nível nacional de Portugal.

1-Acha que um Sistema de Informação como o SEI daria algum contributo para a identificação e localização de veículos furtados e pessoas procuradas/sinalizadas?

R: Daria sim contributo de identificação e localização de veículos roubados/furtados e pessoas procuradas, tendo em conta o sistema de informação nos facilitaria a fluidez na recuperação dos veículos roubados ou furtados, associado a detenção dos presumíveis autores.

2- Como é feita a partilha interna da informação criminal na PNA?

R: A partilha interna de informação é feita através de telefone, via WhatsApp, rádios de comunicação, informações escritas ou verbal e relatórios periódicos, que são remetido as operações/sala operativa, para os devidos procedimentos.

3- Como é feita a gestão da segurança da informação criminal na PNA?

R: A gestão de segurança da informação criminal é feita pelo chefe de operações, após a análise, remete-se as informações a sala operativa local, para posterior remessa ao DPO/CPL, para o devido tratamento que se impões.

4-Quais são os constrangimentos de não existir um sistema de Informação na PNA?

R: O policiamento proativo, que consiste em colocar as forças policiais em zonas ou bairros onde a criminalidade é preocupante com objetivo de prevenir ocorrências criminais.

5-Na sua opinião, quais considera serem as principais ameaças para a segurança dos Sistemas de Informação de uma força de segurança?

R: Programas mal estruturados, a falta de profissionais capacitados para lidar com a segurança de informação.

6-Considera que a transformação digital dos serviços da PNA, colocaria a organização a merce de cyber ataques?

R: Sim a transformação digital nos serviços da PNA colocaria a mercê de Cyber ataques, sendo uma instituição pública com várias informações sigilosas a nível nacional.

7-Quais seriam as principais vantagens que o um sistema de informação como o SEI traria na identificação de suspeitos?

R: As novas tecnológicas na PNA, tem vindo a ter um certo desenvolvimento com alguns sistemas já usados e implementados a nível do país tais como CIS e CESP, que é um sistema cal center e monitoramento de imagem, onde se visualiza as imagem a nível de algumas

zonas do país, onde tem coberturas e o novo sistema de radar implementado na PNA, que vai permitir controlar a velocidade em que os nossos automobilistas percorrem.

8-Sendo as comunicações uma ferramenta indispensável para o normal funcionamento de qualquer organização, na sua opinião como está a situação das novas tecnologias na PNA?

R: PNA vai fazer 47 anos, cada dia mais estamos a deixar de parte os meios que não correspondam as necessidades contemporânea. Atualmente já é possível controlar em tempo real a geo-localização em tempo real dos operacionais nos terrenos, a existência de material informático em algumas esquadras.

Apêndice XIX: Entrevistas a oficiais da Polícia Nacional de Angola

A presente entrevista insere-se no âmbito da dissertação de mestrado para Obtenção do grau de mestre do curso de Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório desta dissertação é "Importância do Sistema Estratégico de Informação: Proposta de Implementação na Polícia Nacional de Angola", sendo orientador e coorientador da mesma o senhor Superintendente José Joaquim Antunes Fernandes e o senhor Subintendente Carlos Alberto Batista Correia, respetivamente.

Pretende-se com esta dissertação perceber como se adequaria o Sistema Estratégico de Informações (SEI) na Polícia Nacional de Angola (PNA), compreender como o SEI melhoraria o trabalho operacional na PNA e quais as medidas necessárias para a sua implementação.

Entrevistado nº 2

Cargo/Posto-Comandante Municipal/ Superintendente-chefe

Local- Cazenga

Data-06/02/2023

Guião

O Sistema Estratégico de Informação (SEI), é uma ferramenta de gestão policial onde são registadas todas as ocorrências, bem como a tramitação documental (interna e externa) dos expedientes, estando interligada com outras bases de dados ao nível nacional de Portugal.

1-Acha que um Sistema de Informação como o SEI daria algum contributo para a identificação e localização de veículos furtados e pessoas procuradas/sinalizadas?

R: Sim. Daria um contributo muito grande tendo em conta a necessidade face aos problemas de segurança pública aos crimes rodoviários, roubos e furtos de viaturas bem como a identificação e localização dos presumíveis autores.

2- Como é feita a partilha interna da informação criminal na PNA?

R: A partilha de informação criminal na PNA é feita a partir de um sistema integrado ou base de dados, onde quando houver necessidade é solicitado o órgão que precisar em função de uma situação. EX: AFIS que é a base de dados de catalogação criminal de indivíduos com passagem nas esquadras de Polícia bem como o crime que cometeu e o respetivo ano.

3- Como é feita a gestão da segurança da informação criminal na PNA?

R: Quanto a gestão é feita de forma secreta e confidencial de modo a evitar vazamento de informação. Primando sempre na fiscalização controlo, recolha e tratamento da informação de salientar que a gestão começa desde os órgãos de base na recolha de informação de caracter criminal até aos órgãos de controlo do Sistema de Informação Criminal (Direção de Informações Policiais).

4-Quais são os constrangimentos de não existir um sistema de Informação na PNA?

R: Proativa. Atendendo ao contexto de nossa constituição policial bem como o contexto da nossa sociedade. Temos que ser proativo no tratamento das informações criminais

5-Na sua opinião, quais considera serem as principais ameaças para a segurança dos Sistemas de Informação de uma força de segurança?

R: Falta de segurança do sistema, confidencialidade, secreta, vazamento de informação, fraca gestão do sistema e o tratamento da informação.

6-Considera que a transformação digital dos serviços da PNA, colocaria a organização a merce de cyber ataques?

R: Sim. Caso não haja cultura e segurança do próprio sistema nacional

7-Quais seriam as principais vantagens que o um sistema de informação como o SEI traria na identificação de suspeitos?

R: Mais capacidade de gestão do sistema na identificação de presumíveis autores; identificação de potenciais delituosos; localização de bens furtados e roubados; facilidade do esclarecimento de crimes; localização e identificação de viaturas roubadas

8-Sendo as comunicações uma ferramenta indispensável para o normal funcionamento de qualquer organização, na sua opinião como está a situação das novas tecnologias na PNA?

R: Está bem apesar de estar ainda em processo de desenvolvimento precisa-se que essa ferramenta seja de acesso a todos e para todos agentes policiais.

Apêndice XX: Entrevistas a oficiais da Polícia Nacional de Angola

A presente entrevista insere-se no âmbito da dissertação de mestrado para Obtenção do grau de mestre do curso de Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório desta dissertação é "Importância do Sistema Estratégico de Informação: Proposta de Implementação na Polícia Nacional de Angola", sendo orientador e coorientador da mesma o senhor Superintendente José Joaquim Antunes Fernandes e o senhor Subintendente Carlos Alberto Batista Correia, respetivamente.

Pretende-se com esta dissertação perceber como se adequaria o Sistema Estratégico de Informações (SEI) na Polícia Nacional de Angola (PNA), compreender como o SEI melhoraria o trabalho operacional na PNA e quais as medidas necessárias para a sua implementação.

Entrevistado nº 3

Cargo/Posto-Comandante Municipal de Luanda/ Superintendente-chefe

Local- Luanda

Data-17/02/2023

Guião

O Sistema Estratégico de Informação (SEI), é uma ferramenta de gestão policial onde são registadas todas as ocorrências, bem como a tramitação documental (interna e externa) dos expedientes, estando interligada com outras bases de dados ao nível nacional de Portugal.

1-Acha que um Sistema de Informação como o SEI daria algum contributo para a identificação e localização de veículos furtados e pessoas procuradas/sinalizadas?

R: Hodiernamente é impossível idealizar qualquer força ou serviço de segurança sem estar sustentado num sistema de informações, isto porque um dos principais objetivos de um sistema de informação policial é de facultar dados relevantes e convenientes ao gestor policial ou ao investigador criminal, logo contribuir satisfatoriamente nas ações policiais.

1- Como é feita a partilha interna da informação criminal na PNA?

R: A PNA dispõe de um sistema de informação policial que permite a organização dos atos e atividade conducentes à produção das informações, cuja a finalidade é ajudar os respetivos comandantes na tomada das suas decisões e esconder dos adversários os planos de atuação e as atividades a desenvolver.

2- Como é feita a gestão da segurança da informação criminal na PNA?

R: A capital importância das atividades no trabalho de segurança das informações criminais na PNA, impõe o respeito e observância sistemática de um conjunto de princípios básicos desde o registo, estudo, interpretação, analise, integração, conclusão até a sua difusão.

4-Quais são os constrangimentos de não existir um sistema de Informação na PNA?

R: Partindo do princípio da necessidade de informação a proatividade vem sempre como o vetor primário da atuação policial, devemos sempre reunir o maior numero de informações, devemos ter ao alcance das informações para satisfazer a nossa necessidade de segurança por forma a transmitirmos o sentimento de segurança aos munícipes e não só.

5-Na sua opinião, quais considera serem as principais ameaças para a segurança dos Sistemas de Informação de uma força de segurança?

R: Todos os sistemas têm as suas vulnerabilidades, quer do ponto de vista do fator humano ou decorrentes das falhas e todos outras interferências que as novas tecnologias estão sujeitas, cada organização deve socorrer-se dos seus melhores técnicos para que não haja violação dos sistemas ou a fuga de informações assim como a quebra do sigilo profissional.

6-Considera que a transformação digital dos serviços da PNA, colocaria a organização a merce de cyber ataques?

R: Olhando para o mundo atual nenhum sistema pode-se dizer que está completamente seguro, as grandes potencias hoje os seus sistemas estão a ser hackeados cada vez mais esta sendo aperfeiçoando o sistema de obtenção de informações de cada adversário hoje ate um simples balão meteorológico pode hackear todo um sistema de informação de qualquer organização que a prior se sinta protegido, há que, inovar, actualizar, monitorar sistematicamente os sistemas para se notar intrusos no sistema.

7-Quais seriam as principais vantagens que o um sistema de informação como o SEI traria na identificação de suspeitos?

R: Ajudaria muito caso todos estivessem cadastrados ou que tivessem uma base de dados muito bem elaborado aí sim, quer identificação de suspeito ou meios roubados assim como na localização de cada um de nós.

8-Sendo as comunicações uma ferramenta indispensável para o normal funcionamento de qualquer organização, na sua opinião como está a situação das novas tecnologias na PNA?

R: Está bem apesar de estar ainda em processo de desenvolvimento precisa-se que essa ferramenta seja de acesso a todos e para todos agentes policiais.

Apêndice XXI: Entrevistas a oficiais da Polícia Nacional de Angola

A presente entrevista insere-se no âmbito da dissertação de mestrado para Obtenção do grau de mestre do curso de Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório desta dissertação é "Importância do Sistema Estratégico de Informação: Proposta de Implementação na Polícia Nacional de Angola", sendo orientador e coorientador da mesma o senhor Superintendente José Joaquim Antunes Fernandes e o senhor Subintendente Carlos Alberto Batista Correia, respetivamente.

Pretende-se com esta dissertação perceber como se adequaria o Sistema Estratégico de Informações (SEI) na Polícia Nacional de Angola (PNA), compreender como o SEI melhoraria o trabalho operacional na PNA e quais as medidas necessárias para a sua implementação.

Entrevistado nº 4

Cargo/Posto-Comandante Municipal/ Intendente

Local- Icolo e Bengo

Data- 13/03/2013

Guião

O Sistema Estratégico de Informação (SEI), é uma ferramenta de gestão policial onde são registadas todas as ocorrências, bem como a tramitação documental (interna e externa) dos expedientes, estando interligada com outras bases de dados ao nível nacional de Portugal.

1-Acha que um Sistema de Informação como o SEI daria algum contributo para a identificação e localização de veículos furtados e pessoas procuradas/sinalizadas?

R: : Sim daria Muito Jeito, atualmente tem se feito recurso ao CISP, pois é o serviço que tem por incumbência fazer estes registos, sendo que eles têm uma base de dados onde são registados todos ilícitos que ocorrem, o grande problema é que essa base de dados não é partilhada ao nível das unidades operativas de bases (esquadras), o que dificulta a partilha de informação ao nível operacional, pois deste modo uma esquadra não tem como saber o que a outra esquadra do mesmo comando municipal fez ao nível de registo de ocorrências.

2- Como é feita a partilha interna da informação criminal na PNA?

R: Geralmente é Feito um alerta via Rádio (ao nível provincial) a partir dos comandos municipais ou das operações do Comando Provincial de Luanda. Não existe uma base de dados ou sistema de informação onde ficam registadas todas as ocorrências policiais a nível nacional. A PNA precisa de um sistema que pudesse unificar todas estruturas operativa nesta organização, o que não existe.

3-Como é feita a gestão da segurança da informação criminal na PNA?

R: Existe um Sistema denominado CISP que está alocado aos comandos municipais, e neste sistema é possível fazer o adestramento do denunciante. Mas ao nível das esquadras estes serviços não existem.

4-Quais são os constrangimentos de não existir um sistema de Informação na PNA?

R: Proativa. Atendendo ao contexto de nossa constituição policial bem como o contexto da nossa sociedade. Temos que ser proativo no tratamento das informações criminais

5-Na sua opinião, quais considera serem as principais ameaças para a segurança dos Sistemas de Informação de uma força de segurança?

R: Ao meu ver existe ameaças internas e externas. os riscos internos prendem-se por exemplo com a necessidade de conhecer, seria necessário criar níveis de acesso a informação do sistema conforme as funções desempenhadas pelo utilizador. Ao nível das ameaças externas, é necessário que haja um sistema de criptografias para evitar ataques cibernéticos de modo a salvaguardar as informações do próprio sistema

6-Considera que a transformação digital dos serviços da PNA, colocaria a organização a merce de cyber ataques?

R: aos longo dos últimos tempos a PNA tem dado passos largos para o desenvolvimento tecnológico de modo a tornar eficiente o serviço policial. todos os sistemas de informação como o SEI, estão sujeitos a ataques Cibernéticos, mas apesar desse risco é o

desenvolvimento tecnológico desta PNA é o caminho que está a ser seguido, pois desta forma também contribuímos para a poupança de meios gastáveis (papel).

7-Quais seriam as principais vantagens que o um sistema de informação como o SEI traria na identificação de suspeitos?

R: Uma ferramenta como o SEI traria inúmeras vantagens, como por exemplo caso detivermos um cidadão, tendo uma base de dados daria para juntar os antecedentes de modo que se entregasse um dossier mais amplo para o Ministério Público. Geralmente quando um crime é cometido pelo mesmo individuo, a PNA não consegue fazer ligação com os múltiplos crimes cometidos pelo mesmo, nem mesmo a participação do mesmo individuo em múltiplos atos ilícitos.

8-Sendo as comunicações uma ferramenta indispensável para o normal funcionamento de qualquer organização, na sua opinião como está a situação das novas tecnologias na PNA?

R: PNA vai fazer 47 anos, cada dia mais estamos a deixar de parte os meios que não correspondam as necessidades contemporânea. Atualmente já é possível controlar em tempo real a geo-localização em tempo real dos operacionais no terreno, a existência de material informático em algumas esquadras.