Instituto Superior de Ciências Policiais e Segurança Interna

Vítor Elísio Ferreira Cucu

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXI Curso de Formação de Oficiais de Polícia

A Segurança dos Sistemas de Informação da PSP: O Sistema Estratégico de Informação (SEI)

Orientador:

Superintendente Sérgio Felgueiras

Lisboa, 03 de maio de 2019

Instituto Superior de Ciências Policiais e Segurança Interna

Vítor Elísio Ferreira Cucu

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXI Curso de Formação de Oficiais de Polícia

A Segurança dos Sistemas de Informação da PSP: O Sistema Estratégico de Informação (SEI)

Orientador:

Superintendente Sérgio Felgueiras

Lisboa, 03 de maio de 2019

Dissertação apresentada ao Instituto Superior de Ciências Policiais e Segurança Interna, com vista à obtenção do grau de Mestre em Ciências Policiais, elaborada sob orientação científica do Superintendente Sérgio Felgueiras.

Às minhas filhas,

Ângela e Sara.

Agradecimentos

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 Sérgio Felgueiras, meu orientador, pela disponibilidade, orientação e sugestões concedidas, que muito contribuíram para o resultado final deste trabalho.

Um agradecimento aos docentes e ao pessoal do quadro orgânico do Instituto Superior de Ciências Policiais e Segurança Interna, pelo meritório 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 XXXI CFOP, quero também dirigir uma palavra de apreço e consideração, pelo espírito de companheirismo e entreajuda manifestados ao longo destes cinco anos do curso.

Dedico um agradecimento especial ao Centro Nacional de Cibersegurança e ao Departamento de Engenharia Informática do Instituto Superior de Engenharia do Porto, pela colaboração e disponibilidade prestadas através das entrevistas, esclarecimentos e indicações concedidas no âmbito do presente trabalho.

O meu reconhecimento dirige-se ainda aos Oficiais, Técnicos Superiores, Chefes e Agentes que colaboraram neste estudo, pertencentes ao Departamento de Sistemas de Informação e Comunicações da Direção Nacional da PSP, aos Núcleos de Sistemas de Informação e Comunicações dos Comandos Metropolitanos da PSP de Lisboa, Porto, ao Comando Distrital da PSP de Coimbra, ao Núcleo de Deontologia e Disciplina do Comando Metropolitano da PSP do Porto, pela valiosa ajuda manifestada, concedendo entrevistas, informações, documentos e testemunhos, aspetos fundamentais para o desenvolvimento deste trabalho de investigação.

Finalmente, o meu agradecimento a todos aqueles que, direta ou indiretamente, contribuíram para o estudo que aqui se apresenta.

Resumo

As forças e os serviços de segurança, no contexto do ambiente tecnológico contemporâneo, fazem um esforço de acompanhamento das novas tendências, no sentido de identificar e incorporar, no seu leque de ferramentas, instrumentos que melhorem e potenciem o seu desempenho operacional. Parte do sucesso da ação policial, no teatro das operações, resulta da partilha e da disponibilidade da informação. Neste domínio, os Sistemas de Informação Policiais adquirem uma centralidade quase absoluta, visto que estão presentes na generalidade das áreas de atividade desenvolvidas pelas organizações policiais, constituindo-se ativos críticos de informação cuja proteção importa acautelar. São várias as ameaças que exploram as vulnerabilidades destes sistemas, existindo, por isso, um risco efetivo para a segurança da informação neles contida. Neste estudo procurámos compreender de que forma a Polícia de Segurança Pública (PSP) protege os seus sistemas de informação e, em concreto, o Sistema Estratégico de Informação, Gestão e Controlo Operacional (SEI). Pretendemos fazer um estudo das medidas de segurança implementadas pela PSP na preservação dos seus ativos informacionais, percebendo-se se a instituição promove a proteção dos seus sistemas de informação de acordo com o atual estado da arte. Para alcançar as respostas pretendidas recorremos ao método qualitativo, realizando entrevistas a especialistas e a responsáveis pela gestão da segurança dos Sistemas de Informação na instituição. Adicionalmente, realizámos pesquisas documentais, incidindo no dispositivo normativo e legal que regula a segurança da informação em ambiente digital. Depois de submetidos à análise de conteúdo, estes instrumentos permitem-nos perceber o nível de segurança dos sistemas de informação da PSP, de forma geral, e do SEI em particular.

Palavras-chave: Sistemas de Informação Policiais; Polícia de Segurança Pública; Sistema Estratégico de Informação; Cibersegurança.

Abstract

Security forces and services, in the context of the contemporary technological environment, make an effort to follow new trends, to identify and incorporate, in a range of tools, instruments that improve and enhance their operational performance. In the theatre of operations, part of the success in the police action results from the sharing and availability of information. In this domain, the Police Information Systems acquires an almost absolute centrality, since they are present in the majority of the areas of activity developed by the police organizations, constituting critical information assets whose protection it is vital to ensure. Several threats exploit the vulnerabilities of systems, and there is, therefore, an active risk to the information security contained in them. In this study, we attempt to understand how the Public Security Police (PSP) protects its information systems and, particularly, the Strategic System of Information, Management and Operational Control (SEI). We intend to make a study about the security measures implemented by PSP towards the preservation of its informational assets, realizing if the institution promotes the protection of its information systems according to the current state of the art. To reach the intended answers, we used the qualitative method, conducting interviews with specialists and those responsible for the management of information systems security in the institution. Besides, we conducted document research, focusing on the legal and normative device that regulates information security in a digital environment. After being submitted to content analysis, these instruments allow us to understand, in general, the level of security of the information systems of PSP and, particularly, of SEI.

Keywords: Police Information Systems; Public Security Police; Strategic System of Information; Cybersecurity.

Índice

Lista de Referências

Documentação Anexa

Apêndices

Lista de Siglas

ADAM - *Active Directory Application Mode*

ANS - Autoridade Nacional de Segurança

APN - *Access Point Name*

BS – *British Standard*

CCC – Centro de Comando e Controlo

CMICP – Curso de Mestrado Integrado em Ciências Policiais

CNCS – Centro Nacional de Cibersegurança

CNPD – Comissão Nacional de Proteção de Dados

COSI – Centro de Operações de Segurança Informática

CRP – Constituição da República Portuguesa

CERT – *Computer Emergency Response Team*

CSIRT – *Computer Security Incident Response Team*

DIP – Departamento de Informações Policiais

DoS – *Denial of Service*

DGSIT - Divisão de Gestão e Segurança de Infraestruturas Tecnológicas

DSSI - Divisão de Serviços e Sistemas de Informação

DNPSP – Direção Nacional da Polícia de Segurança Pública

DSIC – Departamento de Sistemas de Informação e Comunicações

ELI – Elemento de Ligação Informática

ENISA – *European Network and Information Security Agency*

EPP – Escola Prática de Polícia

GIVERH - Gestão Integrada de Vencimentos e Recursos Humanos

GNR – Guarda Nacional Republicana

IE – *Internet Explorer*

IEC - *International Electrotechnical Commission*

IGAI – Inspeção Geral da Administração Interna

IP – *Internet Protocol*

ISCPSI – Instituto Superior de Ciências Policiais e Segurança Interna

ISO - *International Organization for Standardization*

MAI – Ministério da Administração Interna

NEP – Norma de Execução Permanente

NIP – Núcleo de Informações Policiais

NSIC – Núcleo de Sistemas de Informação e Comunicações

NUIPC – Número Único de Identificação de Processo Crime

OLSEI – Oficial de Ligação SEI

OPC – Órgão de Polícia Criminal

PC – *Personal Computer*

PDA - *Personal Digital Assistant*

PDF - *Portable Document Format*

PIIC – Plataforma para o Intercâmbio de Informação Criminal

PJ – Polícia Judiciária

PSP – Polícia de Segurança Pública

RDPSP – Regulamento Disciplinar da Polícia de Segurança Pública

RGPD - Regulamento Geral de Proteção de Dados

RH – Recursos Humanos

RNSI - Rede Nacional de Segurança Interna

RNPSP – Rede Nacional de Dados da Polícia de Segurança Pública

SANS - *System Administration, Networking and Security*

SEI - Sistema Estratégico de Informação, Gestão e Controlo Operacional

SGI – Sistema de Gestão de Identidades

SGSI – Sistema de Gestão de Segurança da Informação

SIGAE - Sistema Integrado de Gestão de Armas e Explosivos

SIGESP - Sistema Integrado de Gestão de Segurança Privada

SIIC – Sistema Integrado de Investigação Criminal

SIOP - Sistema de Informações Operacionais de Polícia

SQE – Sistema de Queixa Eletrónica do MAI

SSIC – Secção de Sistemas de Informação e Comunicações

TI – Tecnologias de Informação

TIC – Tecnologias de Informação e Comunicação

UE – União Europeia

UR – Unidade de Registo

UTIS - Unidade de Tecnologias de Informação e Segurança

VPN – *Virtual Private Network*

Introdução

O ciberespaço é uma realidade incontornável da sociedade contemporânea onde, à semelhança do mundo palpável e físico, existem diversos perigos. Neste mundo virtual, a informação apresenta-se mesmo como um bem precioso que importa acautelar, tanto para as pessoas individualmente consideradas, como para a generalidade das organizações. Neste último caso, a informação representa um ativo crítico, fulcral à prossecução dos objetivos organizacionais, pelo que se torna ainda mais premente a preocupação com a sua preservação. A Polícia de Segurança Pública (PSP), enquanto organização policial, não é uma exceção na valoração que atribui à sua informação, atendendo à importância que esta representa no exercício da atividade policial.

A rápida evolução tecnológica a que se assistiu nos últimos anos e a democratização do uso de ferramentas tecnológicas tornaram-se muito atrativas nos mais variados sectores de atividade, pelo que estas ferramentas foram sendo progressivamente adquiridas e assimiladas pela generalidade dos cidadãos e das organizações. Foi neste sentido que a PSP, enquanto organização policial com uma implantação nacional, aderiu, de forma estratégica[1], a esta corrente de modernização tecnológica, incorporando no seu seio estas ferramentas de elevado potencial, pela mais-valia que constituíam para a instituição.

Neste pressuposto, nas últimas duas décadas, ocorreu, na Polícia de Segurança Pública, um processo de modernização tecnológica que se baseou essencialmente na implementação de Tecnologias de Informação e Comunicação (TIC) nas diversas áreas de atividade da instituição. Este impulso tecnológico originou uma reforma dos processos de gestão da informação que vigoravam até então na instituição, facto que contribuiu para a agilização desses processos e para a racionalização de recursos, constituindo-se, assim, um passo necessário e determinante para o progresso e desenvolvimento da corporação.

Com ponderação e parcimónia, foram feitos os investimentos necessários para a aquisição destes meios tecnológicos que, desde cedo, se mostraram acertados. Podemos referir, a título de exemplo, algumas das capacidades que estes equipamentos apresentam, relativamente ao tratamento de informação, tais como, o seu armazenamento centralizado e a sua disponibilidade permanente e plurilocalizada, de forma célere e segura. Os benefícios da utilização destes equipamentos foram ainda evidentes pelo impacto que tiveram em

[1] A PSP tem vindo a desenvolver um processo contínuo de modernização tecnológica, nele se incluindo o Plano Estratégico de Sistemas de Informação da PSP (PESI), que previu a conceção e implementação de sistemas de informação na instituição.

diversos indicadores de desempenho organizacional, tais como, a qualidade do serviço e a produtividade operacional, sem nos esquecermos de outros critérios de desempenho igualmente importantes, como a economia, a eficácia e a eficiência organizacional.

Pode-se assim afirmar que a transformação institucional a que se assistiu fundou-se essencialmente na inovação tecnológica, materializada, por exemplo, na implementação de infraestruturas críticas de informação, a nível ministerial e institucional, designadamente, a Rede Nacional de Segurança Interna (RNSI) e a Rede Nacional de dados da Polícia de Segurança Pública (RNPSP), que comportam diversos Sistemas de Informação (Ex: SEI, SIGESP, SIGAE, etc.), os quais, por sua vez, servem de suporte à informação da instituição.

Neste sentido, devemos considerar que a interligação de computadores, existentes nos vários departamentos, unidades, subunidades e serviços da estrutura orgânica da PSP, deu corpo a uma rede tecnológica complexa que, com a observância de protocolos e correspondentes especificações técnicas, permite a transmissão e a disponibilização da informação em tempo real e de forma consistente e segura. Porém, devemos admitir que, apesar desta solução tecnológica trazer imensos benefícios para a atividade policial, comporta igualmente diversos riscos que devem ser acautelados.

Nesta perspetiva, hoje em dia, é crescente a preocupação das organizações com a segurança dos seus ativos informacionais, considerando o impacto extremamente negativo que pode advir da disrupção ou perversão do normal funcionamento destes meios tecnológicos. Convém também salientar que, no que tange à segurança deste tipo de infraestruturas tecnológicas e sistemas de informação, não existem soluções perfeitas ou definitivas. Para corroborar esta ideia, atentemos à rapidez com que se preconizam os avanços nesta área tecnológica. Esta circunstância, por si só, torna, muitas vezes, estas ferramentas obsoletas e vulneráveis a diversos tipos de ameaças e riscos. Assim, deve existir uma preocupação sistemática com os diversos aspetos de segurança que vão emergindo neste meio.

Releva, portanto, para a segurança na utilização das tecnologias de informação, o facto de existirem diversas ameaças e riscos que lhes estão intrinsecamente associados, podendo alguns deles advir de fatores naturais[2] e, outros, decorrentes da ação humana[3]. Estas ameaças e riscos não devem ser ignorados, visto que, quando se concretizam, podem

[2] e.g. Catástrofes, intempéries, falhas de energia, incêndios, etc.

[3] Enquadram-se aqui os erros ou descuidos das pessoas que interagem com estas tecnologias, ou, por outro lado, os ataques cometidos, de forma deliberada, por atores mal-intencionados (*Hackers*), que exploram as vulnerabilidades desses sistemas de informação e infraestruturas tecnológicas.

comprometer seriamente a integridade, a disponibilidade e a confidencialidade da informação, o que se poderá repercutir, de forma negativa, quer no desempenho da atividade operacional, quer nos níveis de confiança que a população deposita na instituição policial.

Por um outro prisma, acresce, ainda, referir a peculiaridade da informação tratada no meio policial. Ou seja, trata-se de matéria sensível e classificada, sujeita, portanto, a segredo profissional, de justiça ou de estado, pelo que o seu acesso, tratamento e disponibilização devem merecer uma especial atenção, até porque se encontram juridicamente previstos[4]. Esta circunstância implica um cuidado adicional na adoção de medidas de proteção nos sistemas de informação e nas infraestruturas tecnológicas que comportam esta informação. Os sistemas de informação da PSP assumem, deste modo, um papel preponderante na gestão da informação na instituição, sendo fundamental promover a sua segurança e o seu correto funcionamento.

Atualmente, o sistema de informação que concentra grande parte da informação das diversas áreas de atividade da PSP é o Sistema Estratégico de Informação, Gestão e Controlo Operacional (SEI). A pluralidade das funcionalidades de que esta aplicação (SEI) dispõe abrange muitos dos processos de gestão da informação policial. Afirma-se, no meio policial, que a polícia se tornou "seicêntrica", dada a centralidade que este sistema de informação assume na generalidade das atividades da instituição, seja na área operacional, seja na área de apoio à atividade operacional. Esta circunstância, por si só, revela que este é de facto um importante ativo crítico de informação da PSP, pelo que é de todo pertinente refletir sobre a forma como este sistema de informação é protegido. A proteção dos ativos organizacionais, de uma forma geral, e do SEI, em particular, constitui naturalmente uma preocupação para a PSP, atendendo ao importante contributo que dão na prossecução da atividade policial. É neste contexto que o aprofundamento de conhecimentos técnicos, na área da segurança dos sistemas de informação, constitui uma prioridade, visto que a instituição concentra, nas Tecnologias de Informação (TI), grande parte da informação relativa à sua atividade.

Contexto da Investigação

No âmbito da dissertação final do curso de mestrado integrado em ciências policiais, pretende-se desenvolver um estudo exploratório que trata a temática da segurança dos

[4] A Resolução de Conselho de Ministros n.º 50/88, de 8 de setembro - SEGNAC 1 - contém instruções para a segurança nacional, salvaguarda e defesa das matérias classificadas.

Sistemas de Informação da PSP, mais concretamente, do Sistema Estratégico de Informação, inserindo-se o mesmo na linha de investigação da área de Tecnologia Policial, a qual se enquadra no campo epistemológico das Ciências Policiais. Contudo, dada a transversalidade do tema e das várias dimensões que o mesmo suscita, acabamos por fazer uma abordagem plurifacetada, tocando diversos aspetos de outras áreas do conhecimento, a saber, a sociologia, o direito, a gestão, a ciência política e as ciências da computação.

Note-se que a escolha do tema deriva sempre de "um mal-estar, uma irritação, uma inquietação, e que, por consequência, exige uma explicação ou pelo menos uma melhor compreensão do fenómeno observado" (Fortin, 2009, p. 48), tendo em consideração diversos "parâmetros, tais como gostar do tema e ter capacidade para obter e tratar dados" (Sarmento, 2013, p. 6). Quivy & Campenhoudt (1998) preconizam que a formulação da pergunta de partida deve atender a critérios de clareza, de exequibilidade, de pertinência e que, consequentemente, a mesma seja suscetível de ser trabalhada, atendendo à disponibilidade dos recursos do investigador, possibilitando a obtenção de elementos que respondam ao problema em causa. Neste contexto, esta investigação procurará dar resposta à seguinte pergunta de partida: "Como é que a PSP protege o Sistema Estratégico de Informação (SEI)?".

Objetivos da Investigação

Atendendo a que os objetivos de uma investigação científica "originam uma lista de conhecimentos e competências a adquirir" (Sarmento, 2013, p.13), importa dar resposta à pergunta de partida entretanto formulada. Esta será o fio condutor que ajudará o investigador a direcionar e a orientar o seu estudo, pelo que, no nosso caso em concreto, se pretendem atingir os seguintes objetivos genéricos: (a) Realçar a importância do SEI para a PSP; (b) Descrever e compreender o esquema de segurança do Sistema Estratégico de Informação (SEI); (c) Realçar a importância de uma cultura de cibersegurança na organização. Em termos de objetivos específicos deste trabalho, pretende-se: (a) Descrever a arquitetura tecnológica do SEI, os seus módulos e perfis de utilização; (b) Compreender a infraestrutura tecnológica que suporta o SEI; (c) Identificar os principais tipos de ameaças e riscos que impendem sobre o SEI; (d) Identificar as medidas de segurança adotadas pela PSP na proteção do SEI e das suas infraestruturas tecnológicas; (f) Caraterizar o tipo de resposta adotado pela PSP no caso da ocorrência de um incidente crítico no SEI.

Estrutura da Investigação

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

De seguida, fazemos uma breve apresentação dos referidos capítulos.

No Capítulo 1, é feita uma contextualização conceptual tripartida que reflete o enquadramento sociológico, o enquadramento tecnológico contemporâneo e o enquadramento policial. No enquadramento sociológico, faz-se uma abordagem sistémica do conceito de Sociedade da Informação. Relativamente ao enquadramento tecnológico contemporâneo, aborda-se, numa primeira etapa, o conceito de Tecnologias de Informação e Comunicação, seguindo-se uma descrição conceptual dos Sistemas de Informação. Por último, é feito o enquadramento policial, em que se desenvolve uma visão sustentada da Polícia na Era da Informação Digital.

No Capítulo 2, faz-se um levantamento do estado da arte da segurança dos Sistemas de Informação nas Organizações. Neste sentido, é feita uma breve nota à segurança da informação, com especial incidência nos requisitos necessários à sua concretização, dando-se ênfase ao Sistema de Gestão de Segurança da Informação. As ameaças, os riscos e as vulnerabilidades são também objeto de análise, dado que subjazem nestes conceitos os princípios que orientam as ações necessárias à construção e à consolidação dos Sistemas de Gestão de Segurança de Informação. Nesta sequência, julgou-se pertinente e oportuno abordar o plano normativo que regula a segurança da informação em ambiente digital, numa perspetiva bipartida, ou seja, a nível europeu e nacional. Por outro lado, procuramos encontrar normas técnicas que sustentem padrões confiáveis de implementação da segurança de informação em ambiente digital nas organizações, identificando-se e apresentando-se as que consideramos mais relevantes neste domínio. No plano da gestão da segurança dos sistemas de informação, apresentam-se cinco pilares de intervenção que consideramos fundamentais para a sua implementação, a saber, as políticas de segurança, os mecanismos de segurança, os recursos humanos, as auditorias de segurança e a resposta a incidentes críticos.

No Capítulo 3, apresenta-se, de forma genérica, o Sistema Estratégico de Informação da Polícia de Segurança Pública, desde a sua génese até ao seu atual estado de desenvolvimento. Neste contexto, faz-se uma breve abordagem concetual do sistema, seguindo-se uma descrição tecnológica que incide sobre dois aspetos, a arquitetura lógica e as infraestruturas tecnológicas em que este sistema se suporta. Segue-se uma descrição

funcional, com base na estrutura lógica, na qual são elencados diversos módulos de operação e perfis de utilização do SEI. Por fim, é destacada uma caraterística marcante deste sistema, reveladora da sua centralidade nas atividades da instituição, ou seja, a interoperabilidade, aspeto que viabiliza a troca e a partilha de informação com sistemas de informação de outros organismos.

No Capítulo 4, aborda-se o método. Numa primeira fase, são feitas algumas considerações metodológicas. Aborda-se de seguida o *corpus*, onde é cruzada a problemática com a fundamentação teórica e os dados. Os instrumentos de recolha são também aqui abordados, dando-se especial destaque à entrevista, pela riqueza de conteúdo informacional que proporciona. Por último é aflorado o procedimento que foi adotado ao longo da presente investigação.

No Capítulo 5, é feita a apresentação e discussão dos resultados do estudo exploratório efetuado no âmbito da segurança do Sistema Estratégico de Informação da PSP. O objetivo do estudo passa por perceber como é que a PSP concretiza a segurança dos seus Sistemas de Informação, de uma forma genérica, e do SEI, em particular.

Capítulo 1 - Contextualização

1.1. Enquadramento Sociológico

1.1.1. Sociedade da Informação

No mundo contemporâneo, o Homem, enquanto ser eminentemente social, vive rodeado de uma teia tecnológica, que o circunscreve numa interdependência nos mais variados aspetos da sua existência biológica, social e cultural. Vivemos, é certo, numa época marcada por rápidas transformações económicas, sociais, tecnológicas experienciadas à escala mundial. Com a chegada da globalização, foram desenvolvidos vários processos que aproximaram os países e os povos, sendo estabelecidos todo o tipo de relações, muito por conta do rápido desenvolvimento tecnológico das últimas décadas.

Emerge, assim, um novo paradigma de organização e funcionamento da sociedade contemporânea, centrado num novo polo dinamizador dos mercados e das economias mundiais. Essa força motriz, em torno da qual gira atualmente a organização social, é a informação. Note-se que em todos os quadrantes da vida em sociedade subjaz, na informação, o conhecimento necessário para a tomada de decisões. Essa informação pode advir da acumulação de experiências próprias, ou de terceiros, que são veiculadas através do

processo de comunicação, podendo-se revelar em certas circunstâncias, crucial para a sobrevivência humana.

São vários os meios pelos quais a informação pode ser veiculada, no entanto, no atual estádio de desenvolvimento da sociedade, as novas Tecnologias de Informação e Comunicação (TIC) assumem especial relevância neste processo, atendendo à elevada capacidade de que dispõem, no armazenamento, no processamento e na transmissão de informação. É neste contexto que emerge o conceito Sociedade da Informação, que nos remete para um paradigma de organização social, no qual as sociedades centram e organizam as suas atividades sob a égide da informação. O livro verde para a Sociedade da Informação em Portugal (1997) alude à sociedade de informação nos seguintes termos:

> A expressão 'Sociedade da Informação' refere-se a um modo de desenvolvimento social e económico em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação de informação conducente à criação de conhecimento e à satisfação das necessidades dos cidadãos e das empresas, desempenham um papel central na atividade económica, na criação de riqueza, na definição da qualidade de vida dos cidadãos e das suas práticas culturais.

Pelo acima exposto, concluímos que a sociedade não é um elemento estático, antes pelo contrário, 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. É este novo paradigma de organização e de funcionamento da sociedade contemporânea que é conhecido por Sociedade da Informação.

1.2. Enquadramento Tecnológico Contemporâneo

1.2.1. Tecnologias de Informação e de Comunicação (TIC)

De entre os avanços tecnológicos preconizados pela humanidade, destacam-se, na atualidade, as evoluções tecnológicas nos modos de comunicação, que se basearam na "digitalização da comunicação", sustentadas em Tecnologias de Informação e de Comunicação (TIC). A invasão e disseminação das Tecnologias de Informação e Comunicação nas organizações sociais e económicas é, como referimos anteriormente, o fenómeno central em que assenta a sociedade da informação. O crescimento desta mede-se não só pela capacidade de produção de Tecnologias de Informação e Comunicação, mas

sobretudo pelo consumo de Tecnologias da Informação e Comunicação pelos vários setores da vida social.

Desta forma, podemos afirmar que as TIC assumem na contemporaneidade um papel fulcral na forma como se tem acesso à informação. Importa também aqui invocar o poder informacional, no qual se funda a liderança das organizações na atualidade. Para Pinto, Rodrigues, Santos, Melo, Moreira & Rodrigues (2009), uma das fontes do poder[5] nas organizações é o poder informacional, que resulta não apenas da posição hierárquica ocupada, mas também da facilidade de acesso à informação relevante para as atividades da organização, podendo estar ligado ao cargo desempenhado. Nesta ótica, defende que quem possui informação e conhecimento privilegiado detém poder. Daí a importância que as TIC assumem em toda esta dinâmica concorrencial na busca do ouro do nosso tempo, que é a Informação. Vejamos pois em que consistem estas Tecnologias de Informação e Comunicação, recorrendo aos subsídios de diversos autores.

Para Neves (2006), as Tecnologias de Informação e Comunicação são ferramentas eletrónicas – materiais (hardware: PC' s, modems, routers, impressoras, cartões, chips….), programas e aplicações específicas de programas (software: Microsoft *word*, *Netscape navigator*, um programa de *call center*, uma folha de cálculo de um serviço de contabilidade, um formulário na Internet, etc…) – destinadas a suportar informação e a transmiti-la, compreendendo todas as tarefas necessárias a essas atividades, como processamento, arquivo, classificação, busca, envio, transmissão, transferência e receção. Para Sousa (2009), uma das caraterísticas fundamentais das Tecnologias de Informação, que reflete bem a sua importância atual, consiste no facto de um único meio eletrónico de comunicação suportar todo o tipo de informação possível de digitalizar, o que inclui desde os tradicionais documentos de texto a análises matemáticas e financeiras, passando por imagens, áudio e vídeo. Rascão (2004) afirma que TIC é o conjunto de conhecimentos, de meios materiais (infraestruturas) e de *know-how*, necessários à produção, comercialização e ou utilização de bens ou serviços relacionados com o armazenamento temporário ou permanente da informação, bem como o processamento e a comunicação da mesma.

Conclui-se que, com o passar do tempo, tem existido um grande avanço e incorporação das TIC's na vida quotidiana das pessoas e das organizações, isto na medida

[5] Para este autor são sete as fontes de poder. Dentre estas, quatro encontram-se relacionadas com o nível hierárquico que um indivíduo ocupa na organização, sendo elas: o Poder Legítimo, o Poder de Premiar, o Poder Coercivo e o Poder Informacional. As outras três fontes de poder são: o Poder Pericial, o Poder Carismático e o Poder Relacional. Estas últimas não dependem da posição hierárquica ocupada, mas essencialmente do indivíduo em si.

em que a criação e a gestão da informação bem como as comunicações, passaram a assumir uma posição central face a todas as outras atividades.

1.2.2. Sistemas de Informação

O percurso da evolução da humanidade conduziu-nos a uma organização social centrada no poder da informação, pelo que assumem especial preponderância na contemporaneidade todas as ferramentas que permitam o tratamento ágil e eficaz dessa mesma informação. As organizações cada vez mais recorrem à utilização de Sistemas de Informação para suportar o crescente fluxo de informação, tanto internas como externas, com o objetivo de facilitar e melhorar o processo de decisão (Khauaja & Campomar, 2007). É nesta dinâmica concorrencial que os Sistemas de Informação podem fazer a diferença entre o sucesso e o fracasso das organizações, nos mais variados setores de atividade.

Um Sistema de Informação pode ser definido como um conjunto de componentes inter-relacionados, trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir a informação com a finalidade de facilitar o planeamento, o controlo, a coordenação, a análise e o processo de decisão nas empresas e organizações (Laudon & Laudon, 2012). Trata-se de uma combinação estruturada de informação, recursos humanos, TI e práticas de trabalho, organizada de forma a permitir o melhor atendimento dos objetivos das empresas (Cassaro, 2011). Os Sistemas de Informação são sistemas que usam as Tecnologias de Informação e Comunicação para recolher, transmitir, guardar, recuperar ou disponibilizar informação. Usam as TIC's como mecanismos de suporte à gestão da informação imprescindíveis para que os processos de gestão da organização possam evoluir. O sistema de informação é, assim, o processo de transformação de dados em informações. Essas informações serão utilizadas na estrutura de decisão da organização. O produto da saída do sistema de informação constitui a entrada de um dado processo decisório.

A lei do cibercrime[6] define, na alínea a) do seu artigo 2.º, «Sistema informático» como qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e

[6] Lei n.º 109/2009 de 15 de setembro.

manutenção. A Convenção do Cibercrime[7] define "sistema informático" como um conjunto de equipamentos interligados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o tratamento automatizado de dados.

Em jeito de remate podem-se retirar as seguintes conclusões: um Sistema de Informação é composto por três dimensões: Organização; Tecnologia (Hardware/Software/Telecomunicações/Bases de dados) e; Pessoas. Os Sistemas de Informação integram as organizações, são partes ou componentes das organizações, encontrando-se intimamente ligados um ao outro, sendo por isso concebidos de acordo com o contexto da organização. Estes visam a prossecução dos objetivos organizacionais, e normalmente apresentam uma elevada complexidade, na medida em que são constituídos por vários componentes altamente inter-relacionados e interdependentes, não sendo lineares, visto que são interativos no tratamento da informação. Outra das caraterísticas dos sistemas de informação é que são evolutivos, ou seja, encontram-se em constante evolução moldando-se às transformações organizacionais e tecnológicas que vão sucedendo ao longo do tempo.

1.3. Enquadramento Policial

1.3.1. A Polícia na Era Digital

A informação sempre assumiu uma grande importância na atividade policial. Com a evolução das polícias ao longo do tempo, os métodos de tratamento de informação foram-se refinando e assumindo um papel cada vez mais decisivo para a atividade policial. Esta evolução no tratamento da informação catapultou as modernas polícias para a criação de serviços de inteligência policial no seu seio organizacional, os quais são responsáveis por desenvolverem atividades de produção de inteligência, que serve de apoio nos processos de tomada de decisão dos seus gestores. A qualidade do desempenho dos gestores policiais passou, assim, a ser cada vez mais condicionada pela disponibilidade do acesso à informação, visto que é nesta que subjaz o processo de tomada de decisão. De acordo com a teoria da racionalidade limitada, preconizada por Herbert Simon (1955), a racionalidade do processo decisório consiste em encontrar a opção ideal, mediante a informação disponível. Simon defende que a racionalidade está limitada a três dimensões: a informação disponível, a limitação cognitiva da mente individual e o tempo disponível para a tomada de decisão. Este processo decisório dos gestores policiais encontra-se desta forma inextricavelmente ligado à atividade da inteligência desenvolvida nas organizações policiais. É neste

[7] A Convenção do Cibercrime foi adotada em Budapeste em 23 de Novembro de 2001, e aprovada em Portugal através da Resolução da Assembleia da República n.º 88/2009, de 15 de setembro.

pressuposto que a inteligência policial vem ganhando um papel de cada vez maior destaque nas organizações policiais, assumindo-se mesmo que esta atividade passou a nortear a condução das restantes atividades policiais. Neste mesmo sentido aponta Her´s Majesty's Inspectorate of Constabulary (1999), citado por Fernandes (2014), ao afirmar que "a inteligência deve ser vista como uma atividade central que informa e dirige todas as atividades da Polícia". Nas palavras daquele autor, a inteligência é usada para apoiar a gestão estratégica e operacional da organização, isto é, a decisão dos comandantes policiais quanto ao futuro, na redução da incerteza e na graduação dos níveis dos riscos, bem como suportando a decisão quanto às táticas, técnicas e recursos a acionar com o fim de atingir um determinado objetivo policial.

Voltando-nos agora para as novas tendências de policiamento, verificamos que, na atualidade, os paradigmas de policiamento das polícias mais avançadas do mundo se baseiam na utilização de inteligência, com maior expressão no Policiamento Orientado para a Inteligência (*Intelligense Led Policing*). Este modelo de policiamento surge no início dos anos 90, perante os desafios colocados às organizações policiais de então, decorrentes de novas formas de criminalidade, orçamentos reduzidos e forte pressão política e mediática, que exigiam abordagens preventivas e maior eficácia. Foi com a complexificação da missão policial, que foram desenvolvidos estes modelos de policiamento mais centrados no tratamento da informação, pelo que, perante o aumento exponencial do volume de informação, as forças policiais se viram obrigadas a adquirir e a assimilar, no seu seio organizacional, ferramentas tecnológicas que as tornassem mais eficazes e eficientes no tratamento da informação e consequentemente, mais acutilantes no combate à criminalidade.

A conceção e implementação de sistemas de informação computadorizados nas organizações policiais constituíram, neste sentido, um passo determinante para a superação de várias dificuldades que se sentiam e que se iam avolumando com as transformações sociais e os inerentes avanços dos fenómenos criminogéneos.

Com a adoção de redes de computadores e a utilização da *Internet,* foi possível fazer o intercâmbio de informações entre departamentos policiais geograficamente dispersos, agilizando-se desta forma os processos de gestão informacionais, desmaterializando-os, tornando-os mais expeditos, eficientes e económicos.

Por outro lado, temos de admitir que esta concentração da informação policial em sistemas de informação policiais potencia a sua utilização na produção de conhecimento imprescindível aos processos de tomada de decisão. Referimo-nos por exemplo, à aplicação

de técnicas e ferramentas tecnológicas, tais como *Data Mining*[8], *Bigdata*[9], *Business Inteligence*[10], Inteligência Artificial[11], nos Sistemas de Informação Policiais, que podem dar um importante contributo para a identificação, interpretação e resolução de determinados fenómenos criminais.

São várias as funcionalidades que os sistemas de informação comportam, na atualidade. Um dos casos que se encontra em expansão no meio policial é a georreferenciação. Esta modalidade de sistemas de informação, designada por Sistemas de Informação Geográfica (SIG), apresenta uma diversidade de aplicações práticas no meio policial. Podemos referir, a título de exemplo, algumas aplicações do mapeamento de diversas variáveis operacionais, tais como, a localização dos recursos policiais, mapeamento de ocorrências, ou, a predição de fenómenos criminais (Policiamento preditivo[12]).

Uma outra caraterística marcante nos sistemas de informação policiais, na atualidade, é a sua capacidade para a interoperabilidade com outros sistemas de informação, por exemplo, de outras organizações congéneres ou serviços do Estado, permitindo assim o intercâmbio de informação relevante para as partes. Esta caraterística dos sistemas de informação no meio policial é uma das formas de materialização da cooperação das forças e serviços de segurança em matéria policial e penal.

Por último, referimo-nos a uma modalidade dos sistemas de informação que vem sendo cada vez mais explorada nas forças policiais. Referimo-nos às aplicações móveis que viabilizam o acesso à informação através da utilização de dispositivos eletrónicos móveis[13]. Esta modalidade de sistemas de informação, apresenta-se como uma grande mais-valia na atuação policial, na medida em que faculta, *in loco* e em tempo real, o acesso à informação

[8] *Data Mining* é o processo de explorar grandes quantidades de dados à procura de padrões consistentes, como regras de associação ou sequências temporais, para detetar relacionamentos sistemáticos entre variáveis, detetando assim novos subconjuntos de dados.

[9] *Big Data* refere-se a um grande conjunto de dados gerados e armazenados com os quais as aplicações de processamento de dados tradicionais ainda não conseguem lidar num tempo aceitável. O seu surgimento está relacionado com o aumento exponencial da quantidade de dados gerados a cada minuto no mundo. O *Big Data* representou uma nova era na sociedade moderna, em que os dados se tornaram cada vez mais valiosos, mudando a forma como a economia e a ciência observam os processos, extraem e geram valor desse caos de dados.

[10] *Business Intelligense* refere-se ao processo de recolha, organização, análise, partilha e monitorização de informações que oferecem suporte à gestão de negócios. É um conjunto de técnicas e ferramentas para auxiliar na transformação de dados brutos em informações significativas e uteis para analisar o negócio.

[11] Inteligência artificial é uma inteligência similar à humana exibida por mecanismos ou *software*.

[12] Policiamento preditivo é um policiamento que utiliza um conjunto de produtos resultantes da aplicação de determinadas técnicas de análise com o objetivo de prevenir a criminalidade, identificar alvos para potenciais intervenções policiais e investigar e resolver crimes com base em previsões estatísticas (Fernandes, 2014).

[13] Os dispositivos móveis mais comuns são: *Smartphone*; PDA (*Personal Digital Assistant*); Consola portátil; *Ultra Mobile PC*; *Ultrabook; Notebook; Netbook; Laptop*.

que elementos policiais necessitam para a resolução das ocorrências policiais que se encontrem em curso.

Capítulo 2 - A Segurança dos Sistemas de Informação

2.1. Segurança da Informação em Ambiente Digital

Como até aqui vimos, a informação assume nos dias que correm, um papel fulcral na atividade de qualquer organização na medida em que se torna vital para a prossecução dos seus objetivos. Neste sentido, torna-se importante proteger esta informação nos mais diversos espectros da sua existência. Uma constatação factual é que, com a evolução e utilização massificada das TIC, esta informação migrou em grande parte dos suportes físicos tradicionais para o ambiente digital, pelo que, neste contexto, a segurança da informação nestes meios tecnológicos assume especial relevância na contemporaneidade.

A interligação de sistemas de informação através de redes de computadores e da internet permite o fluxo de informação quase instantâneo à escala global, trazendo consigo claros benefícios para a sociedade. Mas por outro lado, temos de admitir que esta circunstância promove igualmente, a emergência de um conjunto de ameaças que se propagam através do meio virtual. Estas ameaças exploram as vulnerabilidades das infraestruturas tecnológicas e dos sistemas de informação e, quando concretizadas com sucesso, apresentam-se como um sério risco para os ativos de informação de particulares e de organizações. Para Vacca (2014), a garantia da segurança da informação é conseguida quando os sistemas de informação e a informação são protegidos contra ataques, através da aplicação de serviços de segurança, que assegurem os seguintes princípios básicos: disponibilidade, integridade, confidencialidade, autenticidade e não repúdio. Vejamos pois, em que consistem estes princípios.

Por confidencialidade, entende-se que a informação só é acedida por quem detiver privilégios para tal. Já a integridade significa ter a informação livre de erros e de alterações decorrentes de ação maliciosa ou negligente. A disponibilidade decorre da condição da informação poder ser acedida quando é necessária. A autenticidade é a propriedade que permite garantir que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo. Por fim, o não repúdio significa que, o autor de uma dada ação sobre a informação, não pode negar a sua autoria. Um outro atributo, que este autor não refere mas que vem sendo referido na literatura e também alvo de disposições legais, é a privacidade da informação, a qual resulta da garantia da proteção dos dados

pessoais. Saliente-se porém, que, de entre os atributos apresentados, os que detém maior expressão na literatura, são a confidencialidade, a disponibilidade e a integridade. Acrescenta ainda o mesmo autor que, a aplicação desses serviços de segurança deve ser baseada no paradigma proteger, detetar e reagir. Significa isto que, para além de incorporarem mecanismos de proteção, as organizações devem contar com ataques aos seus ativos informacionais, pelo que devem adotar procedimentos e utilizar ferramentas de deteção que lhes permitam reagir e recuperar desses ataques (ibidem).

Neste mesmo sentido aponta Tralhão (2008), ao referir que associados ao conceito de segurança estão diferentes tipos de ação como prevenção, deteção e reação. A prevenção tem como objetivo determinar o valor da informação e o risco a que esta está sujeito. A deteção consiste na monitorização de modo a determinar, quando e como ocorreu o incidente e o responsável pelo mesmo. A reação consiste em levar a cabo ações que permitam repor a situação e eliminar o risco.

Caballero, citado por Vacca (2014), afirma que a segurança da informação é um problema de negócio e como tal, toda a organização se deve estruturar para resolver os problemas de segurança, encarando-a como um objetivo estratégico da organização e não apenas numa perspetiva meramente tecnicista, destinada a mitigar um determinado tipo de ataque. Para este autor, a evolução da segurança para um paradigma baseado no risco, em oposição ao paradigma baseado na solução técnica, deixa claro que, uma organização segura não resulta apenas da proteção das infraestruturas técnicas, mas antes, de um plano transversal à organização, estrategicamente delineado.

Dhillon (2004) corrobora também esta ideia ao afirmar que, a segurança da informação envolve uma construção multifacetada, e a sua gestão exige que tenham que ser consideradas questões não apenas técnicas, mas também organizacionais, estruturais, comportamentais e aspetos sociais.

Por último, a literatura sustenta que a organização da segurança da informação nas organizações, deve ser suportada num Sistema de Gestão de Segurança da Informação (SGSI) que permita planear, desenhar, controlar, avaliar e melhorar todo o processo de implementação da segurança da informação, de forma transversal, considerando três vertentes de atuação: "pessoas", "tecnologia" e "processos"[14].

[14] Ver esquema de implementação de Sistema de Gestão de Segurança de Informação (SGSI) no anexo VIII.

2.1.1. Ameaças, Vulnerabilidades e Riscos

Gaivéo (2008) refere que associado às questões de segurança da informação, existem ameaças, vulnerabilidades e, riscos que podem afetar a atividade dos Sistemas de Informação nas organizações, pelo que é essencial proceder à sua identificação e caracterização para uma melhor resposta e proteção dos Sistemas de Informação no caso de se verificar alguma destas ocorrências. Abordemos então de seguida estes conceitos.

Para Fernandes (2014), a ameaça é uma força ou acontecimento que pode degradar o potencial existente ou alterar um determinado *status quo*. Para Couto (1988), a ameaça é qualquer acontecimento ou ação, de variada natureza, que contraria a consecução de um objetivo e que, normalmente, é causador de danos, materiais ou morais, sendo que no âmbito da estratégia consideram-se principalmente as ameaças provenientes de uma vontade consciente, analisando a relação entre possibilidades e intenções. Já a vulnerabilidade é uma condição ou um conjunto de condições que permitem que as ameaças afetem os ativos. O risco é definido como a probabilidade de materialização de um evento adverso à prossecução dos objetivos de um determinado ator. Para Stewart (2009), o risco é, em essência, a probabilidade de algo dar errado e danificar a organização ou seus ativos de informação. Para este autor, o risco para uma organização e seus ativos de informação, semelhantes às ameaças, aparece de muitas formas diferentes, apontando doze tipos de riscos para a segurança da informação, que se passam a elencar:

(1) Divulgação acidental de informação;
(2) Roubo de *hardware* ou de dados;
(3) Fenómenos naturais;
(4) Alterações de *software;*
(5) Média redundante;
(6) Erros na configuração de sistemas;
(7) Fornecedores e parceiros;
(8) Destruição inadvertida de informação crítica;
(9) Registo incorreto de dados;
(10) Perda de informação crítica;
(11) Desperdício de ativos informacionais;
(12) Falhas na disponibilidade da informação.

Devido às ramificações que o risco apresenta, uma organização deve tentar reduzir esse risco a um nível aceitável. Esse processo é conhecido como gestão de risco da informação.

2.2. Enquadramento Legal e Normativo

2.2.1. Enquadramento Legal

Com o surgimento de um novo espaço, o ciberespaço, a comunidade internacional percebeu que, associados aos incomensuráveis benefícios que a sua utilização proporcionava, emergiam também determinados fenómenos que comprometiam a utilização segura daquele meio. Foi neste sentido que a comunidade internacional, e em especial os estados, se debruçaram sobre esta problemática, constatando a necessidade de adoção de algumas medidas no sentido mitigar os riscos inerentes à utilização do espaço virtual. Uma das vertentes de ação passa por reagir com 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.

2.2.1.1. Legislação Europeia

A abordagem da legislação da União Europeia é essencial neste contexto pelo 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 serão apresentados diversos diplomas que se afiguram relevantes no contexto do presente estudo:

- Diretiva 91/250/CEE do Conselho, de 14 de maio

Esta Diretiva, aprovada em 14 de Maio de 1991, reporta-se à proteção jurídica dos programas de computador, englobando os direitos de autor e incluindo o respetivo material de conceção. A sua aprovação suportou-se, entre muitas outras considerações, nos investimentos em "recursos humanos, técnicos e financeiros", na importância crescente do papel desempenhado pelos programas de computador, nos direitos de autor, que a expressão 'programa de computador' "inclui qualquer tipo de programa, mesmo os que estão incorporados no equipamento", e que a utilização desses programas deve obedecer a critérios que não violem os direitos de autor. Referira-se no entanto que ficam salvaguardadas algumas exceções, nomeadamente a possibilidade de dispor de uma cópia de apoio, os testes e estudo do programa e mesmo a possibilidade de corrigir erros do programa.

- Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto

Esta diretiva tem como objetivos 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 (UE) 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 União Europeia. 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 desenvolver a confiança entre eles; Cria uma rede de equipas de resposta a incidentes 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 – Regulamento Geral de Proteção de Dados (RGPD)

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 Infrações 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 direitos 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 União Europeia e promover os valores fundamentais da UE.

2.2.1.2. Legislação Nacional

Abordaremos, de forma sucinta, as normas jurídicas que mais relevam no contexto da segurança da informação em ambiente digital:

- Constituição da República Portuguesa

Este normativo serve de base para construção de todo o ordenamento jurídico português, visto que ali são estabelecidos os princípios fundamentais em que se funda a República Portuguesa. Neste contexto, esta norma consagra um direito fundamental no seu artigo 35º (Utilização da Informática), no qual se estabelece que "todos os cidadãos têm o direito de acesso aos dados informatizados que lhe digam respeito …" (ponto 1), que "a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do seu titular, …" (ponto 3) e ainda que "é proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei" (ponto 4), que permitem um enquadramento do que é permitido acerca da segurança da informação detida pelas organizações, nos mais variados espectros.

- Lei n.º 67/98, de 26 de outubro - Lei da Proteção de Dados Pessoais

A Lei da Proteção de Dados Pessoais transpõe para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho Europeu, de 24 de Outubro de 1995, relativa à proteção de Pessoas singulares no respeitante ao tratamento de dados pessoais e à livre circulação desses dados. De acordo com o estabelecido no seu artigo 4º, esta lei "aplica-se ao tratamento de dados pessoais por meios total ou parcialmente

automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados".

- Lei n.º 5/2004, de 10 de fevereiro - Lei das Comunicações Eletrónicas

A Lei das Comunicações Eletrónicas transpõe para a ordem jurídica portuguesa as Diretivas 2002/19/CE, 2002/20/CE, 2002/21/CE e 2002/22/CE do Parlamento Europeu e do Conselho, de 7 de Março, e a Diretiva 2002/77/CE, da Comissão, de 16 de Setembro.

Esta lei estabelece o regime jurídico aplicável às redes e serviços de comunicações eletrónicas e aos recursos e serviços conexos, definindo ainda as competências da Autoridade Reguladora Nacional (ARN) nas funções de regulação, fiscalização e sancionamento, destas matérias ali previstas.

- Lei n.º 41/2004, de 18 de agosto - Lei da Proteção da Privacidade no Sector das Comunicações Eletrónicas

A Lei da Proteção da Privacidade no Setor das Comunicações Eletrónicas transpõe para a ordem jurídica portuguesa 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 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

Esta 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 comunicações 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.

- Lei n.º 109/2009, de 15 de setembro - Lei do Cibercrime

Esta lei transpõe para a ordem jurídica interna 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. Este diploma 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.

- Lei n.º 46/2018, de 13 de agosto - Regime Jurídico da Segurança no Ciberespaço

Esta lei estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, 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 União Europeia.

- Decreto-Lei n.º 252/94, de 20 de outubro - Proteção Jurídica de Programas de Computador

Este Decreto-Lei transpõe para a ordem jurídica portuguesa a Diretiva n.º 91/250/CEE, do Conselho Europeu, de 14 de Maio, relativa à proteção jurídica de programas de computador. O seu artigo 1º atribui proteção, "aos programas de computador que tiverem carácter criativo", análoga à que é conferida às obras literárias, equiparando a "programa de computador", o material de conceção preliminar daquele programa. A Autoria, a Reprodução e Transformação, os Direitos do Utente, a Descompilação, os Direitos de pôr em circulação e do Titular originário, a Apreensão, a Vigência e a Tutela, são algumas das temáticas abrangidas por esta Lei.

- Decreto-Lei n.º 3/2012, de 16 de janeiro – Gabinete Nacional de Segurança

Este Decreto de Lei aprova a orgânica do Gabinete Nacional de Segurança.

De entre outras atribuições do GNS, compete-lhe avaliar, acreditar e certificar a segurança de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de informação classificada e proceder à realização de limpezas eletrónicas.

- 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)

Este Decreto - Lei 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. Convém referir 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.

- Decreto Regulamentar n.º5/95, de 31 de janeiro - Base da Dados Pessoais da Polícia de Segurança Pública

Regulamenta a manutenção de uma base de dados pela Polícia de Segurança Pública 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.

- Resolução da Assembleia da República n.º 88/2009, de 15 de setembro

Esta Resolução da Assembleia da República aprova a Convenção sobre o Cibercrime, adotada em Budapeste em 23 de Novembro de 2001.

- Resolução do Conselho de Ministros n.º 5/90, de 28 de setembro (SEGNAC 4)

Esta resolução de conselho de ministros contém normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança Informática. O seu 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 e de outras atividades contra quebras de segurança, comprometimentos e ações de sabotagem, espionagem e ainda pelo implemento de medidas que garantam a

fiabilidade do equipamento e suportes lógicos, a integridade da informação e a continuidade dos trabalhos.

- Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho - Estratégia Nacional de Segurança no Ciberespaço

A Estratégia Nacional de Segurança do 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, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas.

- Resolução do Conselho de Ministros n.º 41/2018, de 28 março (Regulamento Geral de Proteção de Dados)

Esta Resolução de Conselho de Ministros 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.

2.2.2. Enquadramento Normativo

A segurança da informação não obedece a um quadro de regulação formal, pelo que, assumem desta forma especial relevância na sua construção, as normas e as boas práticas. Foi realizada uma prospeção de normas produzidas no âmbito da segurança da informação sendo identificadas e selecionadas três que se consideram de maior relevo no contexto do presente trabalho, as quais se passam expor.

(1) - BS ISO/IEC 17799:2005 – Tecnologias de Informação - Técnicas de Segurança – Código de Prática para Gestão da Segurança da Informação (*Information Technology - Security Techniques - Code of Practice for Information Security Management*)

A norma BS ISO/IEC 17799:2005 é uma norma internacional produzida pela *International Standard Organization* (ISO) e pela *International Electrotechnical Commission* (IEC), que define os procedimentos necessários a garantir a segurança da

informação. Como objetivos da norma definem-se o estabelecimento de linhas de orientação e princípios gerais para iniciação, implementação, manutenção e melhorias da gestão da segurança da informação numa organização. Nesta norma são abordadas em 10 secções as grandes áreas relativas a segurança da Informação:

1. Planeamento da prestação ininterrupta de serviço (*Business Continuity Planning*)**;**
2. Controlo de Acesso aos Sistemas (*System Access Control*);
3. Desenvolvimento de Sistemas de Manutenção (*System Development Maintenance*);
4. Segurança Física e Ambiental (*Physical and Environmental Security*);
5. Conformidade (*Compliance*);
6. Segurança dos Funcionários (*Personel security*);
7. Organização da Segurança (*Security Organization*);
8. Gestão de Computadores e Redes (*Computer and Network Management*);
9. Classificação e Controlo de Bens (*Asset Classification and Control*);
10. Política de Segurança (*Security Policy*).

(2) - BS ISO/IEC 27001:2005 – Sistema de Gestão de Segurança da Informação – Requisitos (*Information Security Management Systems – Requirements*)

A norma BS ISO/IEC 27001:2005 especifica os requisitos para o estabelecimento, implementação, operação, monitorização, revisão, manutenção e melhorias de um Sistema de Gestão de Segurança da Informação (SGSI) no contexto de todos os riscos de negócio numa organização. O SGSI é desenhado para assegurar a seleção dos controlos de segurança proporcionais e adequados à proteção dos ativos informacionais, procurando simultaneamente proporcionar confiança aos interessados. A sua estrutura tem em atenção uma abordagem de implementação baseada no Modelo PDCA (*Plan-Do-Check-Act*), encontrando-se organizada em cinco capítulos distintos mas complementares:

(1) SGSI:

(2) Responsabilidade da Gestão:

(3) Auditorias internas ao SGSI;

(4) Revisão do SGSI por parte da gestão:

(5) Melhoria do SGSI.

(3) - BS 7799-3:2006 – Diretrizes para a Gestão do Risco da Segurança da Informação (*Guidelines for Information Security Risk Management*)

A BS 7799-3 [BS 2006] apresenta um conjunto de diretrizes que visam permitir uma gestão do risco mais eficiente nas organizações, considerando todos os aspetos do ciclo de gestão de riscos de um SGSI. Este ciclo inclui valorizar e avaliar os riscos, implementar controlos para tratar os riscos, monitorizar e rever os riscos, e manter e melhorar o sistema de controlos do risco. Neste sentido, a BS 7799-3 foi especialmente desenvolvida para ser utilizada enquanto ferramenta por gestores de negócio e profissionais de segurança da informação direta ou indiretamente envolvidos com o desenvolvimento, implementação, operação, gestão, manutenção, revisão e/ou melhoria contínua do SGSI organizacional, pelo que deve ser adotada seguindo uma abordagem por processos. A estrutura da BS 7799-3 encontra-se dividida em 4 grupos de diretrizes que permitem nomeadamente:

(1) O enquadramento do conceito de risco para a segurança da informação num contexto organizacional;
(2) O processo de análise e avaliação do risco na organização;
(3) O processo de tratamento e gestão do risco, também no que respeita à tomada de decisão por parte da gestão organizacional;
(4) Atividades continuadas de gestão de risco, no âmbito do SGSI da organização.

2.3. A Gestão da Segurança dos Sistemas de Informação

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.

Para Zúquete (2014), a primeira etapa da construção da segurança de um sistema distribuído, consiste em subdividir o mesmo em subgrupos de redes e máquinas e enquadrar esses subgrupos em domínios de segurança, definindo bem 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.

2.3.1. Políticas de Segurança

Existem várias visões em torno do conceito de política de segurança. Num dos sentidos da polissemia do termo, poderá ser entendida como diretivas de gestores de topo, no sentido de criar um programa de segurança de computadores, em que são estabelecidos

os objetivos e responsabilidades. A política pode se referir também, a regras específicas de um determinado sistema de informação. Adicionalmente política pode-se dizer respeito a assuntos completamente diferentes, tais como, definir uma política de privacidade dos *emails* organizacionais ou uma política de segurança dos faxes na organização (ISO 17999). Para Tralhão (2008), uma Politica de Segurança de Sistemas de Informação (PSSI) pode ser definida, resumidamente, como um instrumento importante para proteger a organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade, constituindo a expressão formal das regras de acesso aos recursos. As políticas de segurança definem o foco da segurança e o que se deve garantir, gizando fundamentalmente os requisitos de segurança que devem ser respeitados para garantir um determinado resultado. As políticas de segurança também podem ser vistas como regras de limitação de atividades, tipicamente estáveis ao longo do tempo, numa dada organização. Zúquete (2014) refere que existe uma política-base de segurança que deve ser escrupulosamente respeitada. Trata-se do Princípio do Privilégio Mínimo, que estabelece que os sujeitos devem usufruir, num determinado instante, apenas os direitos necessários e suficientes para executar as tarefas que lhe estão atribuídas, por forma a não cometer abusos, quer de forma intencional quer de forma acidental. Neste caso, os sistemas devem estar apetrechados e configurados de forma a permitir apenas execução correta de tarefas autorizadas.

2.3.2. Mecanismos de Segurança

Os mecanismos de segurança são a tecnologia que permite pôr em prática as políticas de segurança perante cenários concretos. Estes têm um caráter evolutivo, decorrente de diversos fatores que Zúquete (2014) exemplifica nos seguintes termos:

- Atualização de componentes instalados por causa de vulnerabilidades descobertas nos mesmos (Ex. Atualizações de versões de sistemas operativos ou de servidores, vulgarmente designadas por remendos (*Patches*).
- Alteração da configuração dos mecanismos de segurança para atender a novas situações operacionais ou para colmatar vulnerabilidades descobertas na forma como concretizam as políticas de segurança;
- Utilização de mecanismos de segurança mais modernos e mais seguros do que os até então usados.
- Aplicação de mecanismos de segurança adicionais para garantir a correção e a eficácia de outros mecanismos de segurança (por exemplo, utilização de sistemas

de deteção de intrusões para complementar outros sistemas de prevenção/ limitação de atividades não autorizadas);

- Atualização dos sistemas operativos de uma ou mais máquinas do sistema a proteger.

2.3.2.1. Tipos de Mecanismos de Segurança

Existem diversos tipos de mecanismos de segurança, pelo que a sua escolha deve ser feita em função do fim a alcançar, ou seja, a política de segurança a implantar. Zúquete (2014) apresenta algumas tipologias de mecanismos de segurança:

- Mecanismos de Confinamento

Este tipo de mecanismo cria barreiras à difusão de atividades para além de barreiras de segurança. Exemplos de mecanismos de confinamento são os espaços de endereçamento dos processos na grande maioria dos sistemas operativos atuais, os ambientes de execução controlada (*sandboxing*) de aplicações potencialmente vulneráveis ou maliciosas, as *firewalls* e as zonas desmilitarizadas (DMZ) para separação entre redes;

- Mecanismos de Controlo de Acesso

Os mecanismos de controlo de acesso permitem aferir se um dado sujeito pode ou não realizar uma determinada ação sobre um determinado objeto. Exemplos de mecanismos de controlo de acesso são as proteções no acesso aos dispositivos e à configuração do sistema operativo típicas dos sistemas multiutilizador; as proteções de ficheiro na maior parte dos sistemas de ficheiros; e as proteções no acesso a outras máquinas ou redes;

- Mecanismos de Execução Privilegiada

Estes mecanismos destinam-se a conceder privilégios acrescidos a aplicações especiais que sejam executadas por utentes que normalmente não usufruem desses privilégios. Um exemplo deste tipo de mecanismo é a angariação para certas aplicações de privilégios de administração, através do mecanismo setuid (*set user id upon execution*) ou setgid (*set group id upon execution*) num sistema UNIX/Linux;

- Mecanismos de Filtragem

Os mecanismos de Filtragem servem para realizar certas formas de confinamento ou controlo de acesso. Ou seja, servem para identificar atividades

não necessárias ou autorizadas e evitar que as mesmas sejam levadas a efeito. Um exemplo deste tipo de mecanismo é a filtragem de tráfego de rede não autorizado ou não esperado através de uma *firewall*[15];

- Mecanismos de Registo

Os mecanismos de registo produzem relatórios mais ou menos exaustivos/pormenorizados de atividades solicitadas ou realizadas. Estes mecanismos são fundamentais para se analisar se o sistema que os produz está a operar corretamente e da forma esperada e para detetar causas de erros ou anomalias. É ainda crítico para fazer análise "*post mortem*" de sistemas atacados e, de alguma forma, comprometidos, servindo nesse caso para identificar a origem do problema e o *modus operandi* do atacante. Exemplos de mecanismos de registo são os ficheiros de registo (log) usados nos sistemas UNIX/Linux ou o registo de eventos (*Event Register*) dos sistemas MS Windows;

- Mecanismos de Inspeção

Os mecanismos de inspeção são mecanismos que estão de forma permanente, ou quase permanente, a observar o sistema, de modo a detetar alguma atividade não esperada, legal ou ilícita. Os mecanismos de inspeção, quando atuam em tempo real, são mecanismos complementares de todos os outros que impõe barreiras operacionais, uma vez que permitem detetar falhas na configuração destas últimas. São ainda auxiliares importantes para detetar abusos efetuados por utentes privilegiados, para os quais muitas vezes quase não existem barreiras de segurança para além de limites éticos. Um exemplo de mecanismos de inspeção são os sistemas de deteção de intrusões (IDS);

- Mecanismos de Auditoria

Os mecanismos de auditoria são normalmente mecanismos de inspeção e análise de registos que permitem tirar conclusões após ter acontecido algo de inesperado. Estes mecanismos são normalmente difíceis de autonomizar, sendo frequentemente realizados de forma semiautomática por técnicos especialmente treinados;

- Algoritmos Criptográficos e Afins

[15] Uma *firewall* é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

Os algoritmos criptográficos são um mecanismo insubstituível para proteger informação que possa ser fisicamente devassada. A utilização da criptografia é quase tão antiga quanto a escrita, não sendo, portanto, um subproduto do universo informático. Este apenas permitiu concretizar cifras mais complexas e sofisticadas e agilizou a sua aplicação a conteúdos formados por blocos de bits, enquanto antes se aplicava apenas a conteúdos textuais;

- Protocolos Criptográficos

Os protocolos criptográficos são trocas ordenadas de dados entre entidades em que parte ou a totalidade dos dados úteis trocados são cifrados. Muitos dos mecanismos de segurança para sistemas de informação distribuídos usam ou são baseados em protocolos criptográficos.

2.3.3. Recursos Humanos

Muitas das questões de segurança dos sistemas de informação, envolvem os recursos humanos da organização, que podem compreender os utilizadores, gestores, *designers* e implementadores desses mesmos sistemas. Desta forma, grande parte dessas questões de segurança prende-se com a interação desses indivíduos com o sistemas, podendo ir desde o acesso, às permissões que estes necessitam para realizar o seu trabalho. Nenhum sistema de informação pode ser devidamente protegido sem serem abordados esses problemas de segurança. Vejamos de seguida alguns dos aspetos que ganham maior relevância na segurança dos sistemas de informação, numa perspetiva associada às pessoas que com eles interagem.

- Contratação de Pessoal

A política de recursos humanos deve contemplar uma série de aspetos não técnicos relacionados com a admissão, a saída de colaboradores do quadro de pessoal da organização e a atribuição de níveis de autorização aos utilizadores. Deve também contemplar a definição de um plano de substituição de ausentes, com identificação das posições chave na organização (Mamede, 2014).

- Informação aos Novos Utilizadores

Todos os novos colaboradores que entram na organização têm de ser rapidamente informados sobre as políticas e procedimentos existentes e têm de ser comprometidos com os mesmos, usualmente através da assinatura de uma declaração em que afirma ter lido e

entendido as regras existentes e que se compromete com o cumprimento das mesmas (Mamede, 2014).

- Administração de Utilizadores

Uma administração eficaz do acesso dos utilizadores de computadores é essencial para manter a segurança do sistema. A gestão das contas de utilizadores foca-se na identificação, autenticação, e autorizações de acesso. Esta função, por um lado, pode ser potenciada através da realização de auditorias e, por outro, pela verificação periódica da legitimidade das contas correntes e das autorizações de acesso. Finalmente, deve-se também ter em consideração, a modificação ou remoção oportuna de acessos, em questões relacionadas com movimentação de pessoal, tais como funcionários que são transferidos, promovidos, despedidos ou que se aposentem (Mamede, 2014).

- Formação e Treino em Segurança Informática

A formação dos recursos humanos na área da segurança informática constitui um dos pontos mais importantes na implementação de uma política de segurança. Por um lado os administradores de sistemas devem possuir níveis de conhecimento que lhes permitam desenvolver os mecanismos que implementam o definido pela política, ao passo que os utilizadores têm de possuir um nível de sensibilização muito elevado para as questões da segurança informática (Mamede, 2014).

2.3.4. Auditorias de Segurança

As auditorias de segurança permitem avaliar a implementação das políticas de segurança e identificar lacunas e omissões nas mesmas, dando azo a mudanças e ajustes nas mesmas, adequando cada vez mais à situação pretendida. Desta forma, o processo de auditoria consiste em colocar toda uma série de questões, obter as respostas e comparar as mesmas como o definido na política de segurança. O objetivo de uma auditoria é a localização das origens de vulnerabilidades e a tomada de ações que permitam colmatar as mesmas. Mamede (2014) distingue três tipos de auditorias, conforme a seguir se expõe:

> **- Auditoria à Segurança na Perspetiva do Negócio** - A auditoria de segurança na perspetiva do negócio ir-se-á centrar, basicamente, nos requisitos relativos aos sistemas da organização, na segurança física, nos procedimentos, funções e responsabilidades e na identificação, autenticação e controlo de acesso e, ainda, nas políticas de controlo de risco.

- Auditoria na Perspetiva Técnica - A auditoria na perspetiva técnica ir-se-á centrar na segurança de aplicações e servidores web, na segurança do perímetro, na aplicação das políticas ao nível dos computadores pessoais, na configuração dos servidores, no desenvolvimento aplicacional, nas aplicações em produção, no sistema antivírus e na administração de sistemas.

- Auditoria à Administração de Sistemas – Este tipo de auditoria serve para garantir a aplicação de uma parte das políticas de segurança, realizando uma auditoria às práticas dos administradores de sistemas dentro da organização.

2.3.5. Resposta a Incidentes Críticos

Para começar tentaremos explicar o que se entende por incidente. Um incidente é um evento que interrompe o procedimento normal de operação e precipita um qualquer nível de crise. Numa abordagem mais concreta, um incidente pode ser uma penetração de vírus, o comprometimento de um sistema por intrusão ou outra, roubo de informação, um ataque de negação de serviço ou ainda qualquer atividade de origem e base não legal que exija uma resposta adequada por parte da equipa de segurança, dos administradores de sistemas ou das autoridades criminais.

Atente-se que quando ocorre um incidente, gera-se uma intensa pressão, muito por constrangimentos de tempo de recursos. Esta circunstância leva a que um incidente que afete recursos críticos, possa ser considerado inultrapassável, numa abordagem inicial. Neste sentido, deve-se atender que uma resposta cuidadosa e organizada a um incidente pode representar a diferença entre a recuperação total e o desastre total. Vejamos abordar alguns aspetos que relevam na resposta a incidentes críticos nos sistemas de informação.

- Plano de Contingência

Para prevenir potenciais contingências e desastres ou para minimizar os danos que estes causam, as organizações podem delinear algumas ações a tomar para controlar a ocorrência destes eventos. Esta atividade é genericamente denominada por plano de contingência e prende-se com a gestão de incidentes que materializam ameaças técnicas maliciosas tais como vírus e *hackers* ou que sejam decorrentes de acidentes naturais (tempestades, incêndios etc). Os objetivos de aplicação de uma metodologia de resposta a incidentes podem ser os seguintes:

- Determinação da ocorrência de um incidente;
- Registo e acumulação de informação pertinente e detalhada;

- Ativação de controlos para recolha e manipulação de evidências do incidente;
- Minimizar o impacto nos processos de negócio da organização e;
- Produção de relatórios exatos e com recomendações úteis.

Neste sentido, a resposta a incidentes exige que seja criada uma documentação, o mais exaustiva e detalhada possível. Nos casos de ações, esta documentação servirá para apresentar a atividade maliciosa à administração da organização, visto que, poderá ser necessária para atuar legalmente contra os responsáveis.

- Equipas de Resposta a Incidentes de Segurança Informática (CSIRT)

A Lei n.º 46/2018, de 13 de agosto (regime jurídico da segurança do ciberespaço), estabelece no seu Art.º 3.º, al) a, o conceito de «Equipa de resposta a incidentes de segurança informática», como sendo uma equipa que atua por referência a uma comunidade de utilizadores definida, em representação de uma entidade, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação. Em Portugal existe o CERT.PT que é um serviço integrante do Centro Nacional de Cibersegurança (CNCS) que coordena a resposta a incidentes envolvendo entidades do Estado, operadores de serviços essenciais, operadores de Infraestruturas Criticas nacionais e prestadores de serviços digitais. O CERT.PT é membro da Rede Nacional de CSIRT e representante nacional na Rede Europeia de CSIRT (*Computer Security Incident Response Team*), estabelecida pela Diretiva (EU) 2016/1148 (Diretiva SRI). No Anexo IX, é apresentada a rede de Certs existentes na Europa.

Capítulo 3 – O Sistema Estratégico de Informação (SEI)

3.1. Enquadramento Concetual

Para fazermos uma apresentação sistematizada do Sistema Estratégico de Informação, Gestão e Controlo Operacional (SEI), convenhamos que não seria apropriado fazê-lo, sem caraterizar o cenário da gestão da informação na PSP, no período que precedeu a implementação deste sistema, em 2004. Com efeito, à época, existia na instituição uma dispersão da informação por vários sistemas de informação que iam proliferando nas diversas subunidades e unidades orgânicas da PSP. Esta situação não configurava o ideal de gestão da informação, visto que, a implementação dessas soluções localizadas sem ter em conta a visão global do problema e das reais necessidades da organização no seu todo,

resultavam no crescimento desordenado e, consequentemente, na perda de eficácia, de competitividade e de oportunidades globais de melhoria (Accenture, 2002). A determinada altura, tornou-se premente a necessidade da criação de um sistema de informação único que aglutinasse todos os processos inerentes à gestão da informação operacional da instituição. A constatação desta carência viria a ser reforçada no estudo encomendado pela PSP à empresa Accenture, cujos resultados viriam a ser vertidos num relatório final em 2002, no âmbito do Plano Estratégico dos Sistemas de Informação da PSP (PESI)[16].

Perspetivou-se a partir dali, a criação de um sistema de informação cuja missão fosse "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" (Accenture, 2002). Neste pressuposto, a conceção deste sistema teria como principal objetivo dotar todo o dispositivo da PSP de um sistema de informação capaz de suportar os seus processos operacionais e que, em simultâneo, possibilitasse a uniformização e racionalização de procedimentos, bem como de uma nova forma de atuar, mais eficaz e eficiente (Accenture, 2004). Foi neste contexto que o SEI surge, em 2004, devidamente enquadrado no Plano Estratégico dos Sistemas de Informação da PSP (PESI), o qual encorpava o processo contínuo de modernização da Polícia de Segurança Pública (Accenture, 2004).

Passaram-se sensivelmente 15 anos desde então, e na atualidade, pode-se afirmar que o Sistema Estratégico de Informação (SEI) foi concebido, implementado, e desenvolvido, vindo a assumir a forma e a relevância que se auspiciava inicialmente[17]. Este sistema de informação apresenta-se como uma aplicação informática basilar para a atividade da PSP na medida em que congrega grande parte da informação relativa à generalidade da atividade operacional e de apoio à atividade operacional da instituição em áreas tão diversas como o Trânsito, a Investigação Criminal, as Informações, o licenciamento e a fiscalização, a gestão dos meios entre outras.

Em termos funcionais, pode-se referir que o acesso a esta aplicação é feito por utilizadores pertencentes aos vários níveis da estrutura orgânica da instituição, os quais, possuem um ou mais perfis de utilização do sistema, que lhe são atribuídos em função da posição que ocupam na hierarquia da organização e das funções que desempenham. Estes perfis conferem-lhes as permissões necessárias para aceder a determinados módulos de operação do sistema. A pluralidade das funcionalidades que esta aplicação (SEI) dispõe,

[16] Ver modelo concetual proposto no PESI no Anexo II.
[17] Ver interface do SEI no Anexo III.

abrange grande parte dos processos de gestão da informação policial, compreendendo vários módulos, tais como: Repositório de Informação RI/Catálogo; Gestão de Ocorrências; Gestão dos Meios; Pedidos de Entidades Externas; Estatísticas e Relatórios; Investigação Criminal; Informações Policiais, entre outros que mais à frente analisaremos em detalhe.

As regras e princípios que regem a utilização, gestão e exploração do Sistema Estratégico de Informações, Gestão e Controlo Operacional (SEI), bem como a regulamentação de matérias, direta ou indiretamente, com ele, relacionadas, e ainda, a definição do modelo de governação deste sistema, encontram-se previstas na NEP (Norma de Execução Permanente) n.º DN/ASDDN/GEP/01/03, da Direção Nacional, de 24 de janeiro de 2011, pelo que, a ela recorreremos ao longo da realização do presente trabalho, fazendo-lhe referência, sempre que se justifique.

Face ao exposto, constata-se que o SEI é um sistema de informação, vital à atividade de segurança desenvolvida pela instituição, atendendo que, o mesmo assume especial preponderância nos processos de gestão da informação que subsistem na dinâmica operacional da organização. Este facto, a nosso ver, requer um olhar atento e crítico, no sentido de se desenvolver uma estratégia focada na melhoria contínua deste sistema, que promova o seu aperfeiçoamento integral, otimizando-o por um lado, na sua utilização e, robustecendo-o por outro, na sua proteção, potenciando o seu contributo na prossecução dos objetivos operacionais da instituição.

3.2. Descrição Tecnológica

3.2.1. Arquitetura Lógica

O SEI é uma aplicação baseada em tecnologia *Web*. O princípio de funcionamento deste sistema baseia-se numa arquitetura Cliente / Servidor, materializada através de uma aplicação *web* do tipo servidor que se encontra instalada num servidor web da instituição, à qual, quando em ambiente de operação, são dirigidos diversos pedidos de processamento formulados através de uma aplicação web do tipo cliente (Browser), que se encontra instalada nos diversos computadores da rede interna da instituição, sendo-lhes devolvida a resposta, pela referida aplicação servidora, depois de processada a informação requerida.

O modelo de desenvolvimento do SEI assentou essencialmente numa arquitetura aplicacional de três níveis, que consiste numa distribuição do processamento por vários níveis lógicos e físicos, que se descrevem resumidamente de seguida do seguinte modo:

- **Camada de Dados:** Concentra os dados das aplicações, as regras estruturais da informação, os sistemas de gestão de bases de dados e os sistemas de ficheiros;
- **Camada de Lógica Aplicacional:** Implementa as regras de negócio (ex.: atribuição de NUIPC, validação de informação obrigatória, exigência de licença de porte de arma para efetuar registo de posse);
- **Camada de Apresentação:** Gera o interface com o utilizador do sistema (ou outros sistemas), que permite a recolha de informação e validações preliminares.

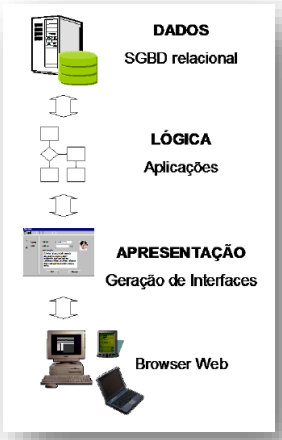


Figura 1 - Arquitetura Aplicacional do SEI.
(Fonte: PESI, 2002, Pág. 440).

Salienta-se que, este modelo de desenvolvimento permite efetuar validações lógicas de segurança nas três camadas da aplicação, que contribuem para a consistência dos dados.

3.2.2. A Infraestrutura Tecnológica

Em termos de infraestrutura tecnológica, o SEI é suportado num *Mainframe IBM 2 Series* que utiliza o *Application Server IBM Web Sphere* e uma base de dados *DB2 7.1*. A Tecnologia aplicacional é *J2EE* utilizando a *framework Accenture GRNDS*, conferindo ao SEI um elevado nível de segurança e performance. O Sistema é executado através de uma aplicação do tipo *browser*, o mesmo que é utilizado regularmente para aceder à *internet*. De momento, o *browser* utilizado pela instituição, para acesso ao SEI, é o *IE 11*[18].

3.2.2.1. A RNSI e a RNPSP

O SEI encontra-se inserido na RNSI, que serve de infraestrutura tecnológica para aquela aplicação[19]. Neste sentido, julgou-se pertinente abordar esta infraestrutura, por forma a compreendermos a sua morfologia e o seu modo de funcionamento, evidenciando-se assim a sua importância para o funcionamento e a utilização do SEI.

A RNSI é uma rede de comunicações que assenta num sistema de cooperação, partilha de serviços e gestão coordenada, de uma rede de comunicações segura, integrada e de alto débito, capaz de suportar dados, voz e imagem, disponibilizada aos vários Serviços e Forças de Segurança e demais organismos do Ministério da Administração Interna (MAI).

[18] Internet Explorer versão 11.
[19] Ver esquema de integração do SEI na RNSI no Anexo IV.

O seu objetivo é uniformizar e melhorar as infraestruturas de comunicações de dados e dessa forma, potenciar a interoperabilidade entre todos os Organismos do MAI, melhorando a interação entre pessoas e aplicações. É uma rede de comunicações IP segura, integrada, de alto débito, totalmente fiável e capaz de suportar comunicação de dados, voz e imagens, entre as instalações (sites), de todos os organismos do MAI. A RNSI é da responsabilidade da UTIS. Ainda no âmbito da RNSI, enquadram-se os registos e a gestão dos utilizadores pertencentes ao MAI, realizados através da plataforma ADAM, que dispõe de um interface denominado SGI[20] (Sistema de Gestão de Identidades), também disponível na RNSI.

A RNPSP é uma rede lógica da PSP que opera sobre a infraestrutura física da RNSI, materializando-se através da implementação de uma VPN (*Virtual Private Network*). Segundo Zúquete (2014), uma VPN atua como um cabo de rede digital que permite uma ligação externa a uma rede organizacional protegida. Por sua vez Mamede (2014), refere que uma VPN é criada através da construção dinâmica de uma ligação segura de comunicação entre dois elementos utilizando o método de encapsulamento.

3.3. Caraterização Funcional

3.3.1. Módulos Aplicacionais do SEI

O SEI encontra-se dividido em módulos que agrupam conjuntos de funcionalidades pertencentes a diversas atividades operacionais da PSP. Esta divisão por módulos confere uma maior facilidade de navegabilidade na aplicação, conseguindo-se também para uma melhor compreensão dos conceitos associados a cada funcionalidade disponibilizada (Accenture, 2004).

No Anexo VI, constam os módulos aplicacionais definidos para suportar a área operacional da PSP que são os seguintes: Estatísticas 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 Informações e Catálogo. Naquela figura são também representadas as aplicações que servem de suporte ao SEI, a saber, a Gestão de Utilizadores e Perfis, a Integração de Aplicações, o Sistema de Informação Geográfica, e a Administração de aplicações. Fazemos de seguida uma breve apresentação de alguns dos módulos que consideramos mais relevantes para a

[20] Ver interface do SGI no anexo V.

apresentação desta aplicação, de acordo com a descrição constante no manual de formação SEI.

- Módulo de Gestão de Grandes Eventos

O principal objetivo deste módulo é a manutenção da informação relativa a Grandes Eventos nos quais a PSP venha a ter uma participação ativa, permitindo que a informação gerida nos restantes módulos seja classificada como estando relacionada com determinado Grande Evento (ocorrências, informações policiais, etc.). Com base nessa classificação será possível, entre outros aspetos, proceder ao cálculo de indicadores estatísticos relacionados com o Grande Evento, quer para controlo interno, quer para fornecimento a entidades externas.

- Módulo Gestão Operacional de Meios

Este módulo é composto por outros dois módulos, a saber, o Módulo de Planeamento e Escalas e o Módulo e Coordenação de Meios. O Módulo de Planeamento e Escalas permite o processamento de todo o ciclo de vida de uma escala, desde a configuração inicial, passando pela geração automática até à realização da escala final. Já o Módulo de Coordenação de Meios é responsável pela gestão dos incidentes e dos recursos afetos a esses mesmos incidentes. O Módulo de Coordenação de Meios é assim o componente do SEI que permitirá o registo e gestão dos incidentes reportados à PSP e a análise estatística da informação desses incidentes.

- Módulo de Gestão de Ocorrências

O módulo de gestão de ocorrências é um dos componentes de um módulo mais abrangente denominado de Gestão de Processos Policiais. Este módulo permite o registo de ocorrências e gestão de processos dos mais vários tipos, no âmbito da atividade operacional da PSP, tais como, crimes, contraordenações, contravenções entre outros.

- Módulo de Gestão de Celas e Detidos

O principal objetivo deste módulo é a gestão de informação referente a celas e detidos, nas áreas de detenção das unidades da PSP. O módulo pode dividir-se em duas grandes áreas:

- Gestão de Áreas de Detenção - que inclui funcionalidades de parametrização de áreas de detenção de unidades da PSP, registo de inspeções e controlo de ocupação de celas numa área de detenção;

- Gestão de Detidos - que inclui funcionalidades para registo de detidos com detenções efetuadas fora do SEI, pesquisa, consulta e alteração de informação sobre detidos, afetação do detido a áreas de detenção e respetivas celas, registo de novos acontecimentos (contactos, refeições, cuidados médicos, etc.) e emissão de peças de expediente.

- 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. No entanto, sendo a partilha de informação uma área sensível da atividade operacional da PSP, esta funcionalidade encontra-se enquadrada pelas seguintes regras:

- Credenciação – Apenas tem acesso à informação dos 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.

Neste sentido, o SEI encontra-se desenvolvido para suportar estas premissas, de modo a corresponder às especificidades operacionais da PSP.

- Módulo Repositório de Informações e Catálogo

Neste módulo encontram-se registadas várias entidades que foram modeladas de forma a poderem ser utilizadas pelos restantes módulos do sistema. Com este repositório é possível fazer uma gestão centralizada da informação referente às entidades ali representadas, que são as seguintes: Pessoas; Organizações, Veículos, Locais, Armas e Objetos.

3.3.2. Perfis de Utilização

A segurança no acesso à informação do SEI foi um aspeto tido em consideração durante a conceção e esenvolvimento do sistema, sendo assim implementados mecanismos que reforçam a sua utilização segura. No entanto, dada a abrangência do SEI, tornou-se necessário que a aplicação apresentasse flexibilidade, de forma a corresponder às expetativas funcionais e aplicacionais dos utilizadores. Com o objetivo de simplificar a gestão de perfis e utilizadores e a maximizar a segurança no acesso à aplicação, foram definidos diversos

perfis de utilizador[21], aos quais foram concedidas determinadas permissões de operação, considerando as diversas tarefas e funções existentes na PSP.

Neste sentido, quando se criam utilizadores para aceder ao sistema, estes são categorizados e associados a um determinado perfil (ou múltiplos perfis), o que lhes confere acesso a certas funcionalidades do sistema. Cada elemento da PSP terá as respetivas credenciais de acesso, que servirão para seu uso exclusivo. Neste contexto, sempre que for criado um novo utilizador, são gerados um nome de utilizador (login) e uma senha de acesso (password). Sempre que um elemento da PSP necessitar aceder à aplicação, é necessário que esteja registado no sistema e que possua as respetivas credenciais de acesso. Em nenhuma situação será possível aceder à aplicação sem estar registado ou sem ter o conhecimento do nome de utilizador e da respetiva senha de acesso. As permissões de operação do sistema resultam do perfil que for atribuído a cada utilizador.

3.3.2.1. Gestão de Perfis

A atribuição dos perfis do SEI é feita a dois níveis, o nível local e o nível central. O nível local é menos exigente do ponto de vista dos critérios de atribuição, pois incide sobre a conceção de perfis gerais, sendo realizada por gestores de perfis SEI, devidamente credenciados, pertencentes às unidades e subunidades da PSP. O outro nível, o central, é mais criterioso do ponto de vista dos requisitos, na medida em que se circunscreve a um conjunto de perfis restritos, sendo, portanto, realizado por gestores de perfis pertencentes ao Departamento de Informações Policiais da DNPSP[22]. Convém referir que o controlo de acessos ao SEI, e aos sistemas que com ele comunicam é gerido exclusivamente pelo Departamento de Informações Policiais.

O Código de Procedimento n.º 02/DIP/2018, de 10 de julho do Departamento de Informações Policiais da PSP, define o processo de atribuição de perfis às diversas bases de dados que se encontram sob a responsabilidade do Departamento de Informações Policiais, incluindo-se neste caso o SEI[23].

3.3.3. A Interoperabilidade do SEI

Na contemporaneidade, as organizações necessitam de se relacionar e partilhar informação no sentido de melhorarem a eficiência interna e a qualidade do serviço que prestam. Neste sentido, é privilegiada a desmaterialização dos fluxos de informação, quer

[21] Conforme tabela de perfis SEI constante no anexo X.
[22] Conforme tabela de perfis SEI constante no anexo X.
[23] Conforme fluxograma constante no anexo XI.

internos, quer nas relações com o exterior, através do estabelecimento de protocolos e na implementação de mecanismos que permitem a automatização das tarefas subjacentes às trocas e partilha de informação entre a PSP e as entidades com que se relaciona com mais frequência (destacando-se a ANSR, os Tribunais, o Ministério da Justiça, a PJ e a GNR, entre outras). Ao nível da envolvente externa, registam-se outros fatores de pressão para a evolução dos meios informáticos da PSP, como é o caso concreto do Sistema Integrado de Informação Criminal (SIIC), que torna necessária a capacidade de contribuir para a partilha de informação entre órgãos de polícia criminal, sem perda de capacidade própria de resposta às necessidades específicas da PSP neste campo. Ao longo do tempo foram surgindo vários sistemas com os quais o Sistema Estratégico de Informação da PSP se teve de integrar, nomeadamente: a Queixa Eletrónica do MAI (SQE), o CITIUS do Ministério da Justiça, a Base de Dados de Violência Doméstica do MAI, o Sistema de Informação Schengen, o sistema de recolha estatística da DGPJ e a PIIC (Plataforma para o Intercâmbio de Informação Criminal, nos termos da Lei n.º 73/2009 de 12 de Agosto)[24].

Capítulo 4 – Método

4.1. Considerações Metodológicas

A escolha do método por parte do investigador, reflete-se na escolha do caminho a seguir. Nas palavras de Quivy e Campenhoudt (2005, p. 15), é exigido ao "investigador que seja capaz de conceber e de pôr em prática um dispositivo para a elucidação do real, isto é, no seu sentido mais lato, um método de trabalho". Tendo sempre em mente, que o caminho a seguir escolhido, deve possibilitar "a sua réplica por outros investigadores" (Pais, 2004, p. 251).

Neste âmbito, a presente dissertação consiste num estudo exploratório, que procura perceber como é que a PSP protege o Sistema Estratégico de Informação (SEI). Para alcançar estes objetivos, deve ser escolhido um método adequado, aliás, é o objeto de investigação que define o método que será utilizado (Flick, 2005). Neste sentido, a presente investigação, terá um teor qualitativo, tendo em conta o *corpus* que constitui o estudo, uma vez que, permite uma abordagem "mais aberta e envolvente", (Flick *et al*., 2004, p.5) ao objeto de estudo (Bardin, 2011).

[24] Ver modelo concetual da PIIC no Anexo VII.

O objetivo da presente dissertação, tal como já foi referido, prende-se com a análise das medidas de segurança implementadas na proteção do SEI, de forma a permitir a sua identificação. Deste modo, e tendo em conta que a abordagem qualitativa.

4.2. Corpus

O *corpus* consiste no "conjunto dos documentos tidos em conta para serem submetidos aos procedimentos analíticos" (Bardin, 2011, p. 126). Atendendo a esta definição, podemos considerar o *corpus*, como o «material de trabalho» do investigador, ou nas palavras de Bauer e Aarts (2000, p. 23) "a colecção finita de materiais, determinada de antemão pelo analista, com inevitável arbitrariedade do analista, e com a qual se irá trabalhar". Tendo em mente as definições apresentadas, o *corpus* da nossa investigação será constituído por um conjunto de sete entrevistas. A nível externo foram entrevistados dois especialistas na área da cibersegurança: um pertencente ao Departamento de Engenharia Informática do Instituto Superior de Engenharia Porto (DEI/ISEP) e o outro, afeto à Unidade de Desenvolvimento e Inovação do Centro Nacional de Cibersegurança (CNCS) do Gabinete Nacional de Segurança (GNS). Já a nível interno, foram entrevistados quatro oficiais da PSP, com funções de comando operacional e chefia, em unidades e serviços da PSP, ligados à conceção, gestão, exploração, manutenção e segurança dos Sistemas de Informação da PSP. Ainda a nível interno, foi entrevistado um técnico superior, com funções de chefia de um Núcleo de Deontologia e Disciplina da instituição.

4.3. Instrumentos de Recolha de Dados

4.3.1. 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, p. 22). Existindo 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 caracteriza-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, conseguiu obter-se uma informação mais abrangente, o que permitiu uma melhor perceção da realidade em estudo, fruto da experiência dos entrevistados (Quivy e Campenhoudt, 2005; Sarmento, 2013).

A obtenção de informação mais abrangente prende-se com o facto de as entrevistas semiestruturadas apresentarem uma "flexibilidade e fraca diretividade que permitem recolher os testemunhos e interpretações" dos entrevistados (Quivy e Campenhoudt, 2005, p.22). Através disto, os entrevistados conseguem analisar o problema tendo em conta "as suas interpretações de situações conflituosas […] os dados do problema" e "o que está em jogo" (Quivy e Campenhoudt, 2005, p.22).

Sendo que o objeto da presente investigação procura identificar as medidas de segurança utilizadas na proteção do SEI, nada melhor do que auscultar as figuras responsáveis pela gestão e manutenção da segurança deste sistema, onde se encontra o objeto de estudo.

4.4. Procedimento

Tal como foi referido nos pontos anteriores, o *corpus* da presente dissertação assentou em entrevistas, que foram sujeitas a uma análise de conteúdo. Para se proceder à análise de conteúdo das entrevistas, tal como foi referido, tivemos de recorrer a um processo de categorização, algo que exigiu a criação de categorias e subcategorias.

Utilizando uma grelha categorial (cfr. Apêndice H) e um manual de codificação (cfr. Apêndice I), 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 5 - A Segurança do Sistema Estratégico de Informação

Depois de termos efetuado o estudo do estado da arte da segurança dos Sistemas de Informação nas organizações e de termos escolhido e traçado o método mais apropriado para obtermos resposta à nossa pergunta de partida, neste capítulo, faremos a apresentação e a discussão dos resultados. Assim, na análise do conteúdo do nosso *corpus*, procedeu-se à codificação de 208 unidades de registo (u.r.), que foram enquadradas nas respetivas subcategorias das cinco linhas de força delineadas. As linhas de força, veiculadas através das 5 categorias, e as respetivas subcategorias são representadas no apêndice H. Neste

alinhamento, fazemos de seguida a apresentação e a discussão da distribuição das unidades de registo nas categorias assinaladas no gráfico da figura 2.

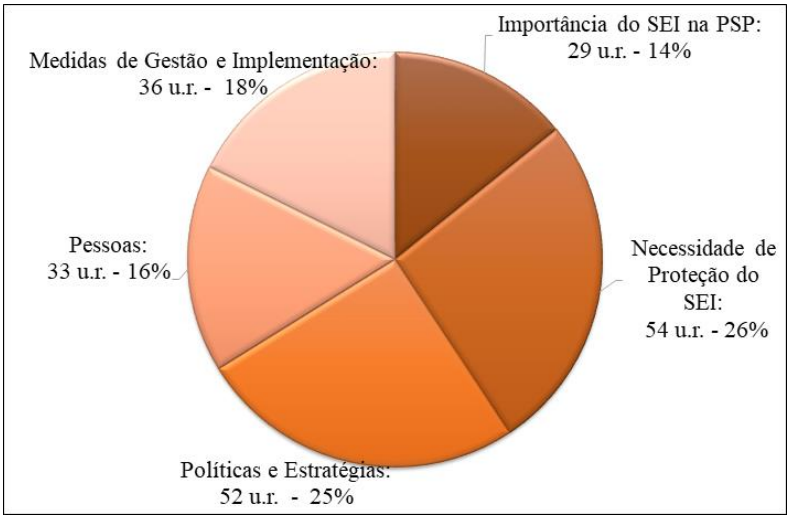


Figura 2- Gráfico da distribuição das unidades de registo pelas categorias.

Dos resultados apresentados, constata-se que existe uma distribuição generalizada das unidades de registo pelas cinco categorias delineadas, significando isto que todas elas assumem relevância e representatividade no estudo. Nota-se, no entanto, uma prevalência assinalável nas categorias "Necessidade de Proteção do SEI" e "Políticas e Estratégias". Estas duas categorias, em conjunto, abrangem 106 unidades de registo, o que representa 51% das opiniões categorizadas. Esta constatação merece-nos uma leitura atenta, na medida em que a sua representatividade evidencia uma preocupação acentuada dos entrevistados com estas duas questões. De facto, no primeiro caso, a segurança dos Sistemas de Informação é atualmente algo que vem preocupando a grande parte das organizações, sendo mesmo, em alguns casos, objeto de regulação. Podemos daqui inferir que os nossos entrevistados possuem uma consciência formada sobre esta questão, levando-os a emitir uma opinião. No segundo caso, "Políticas e Estratégias", pretendemos identificar as ações desenvolvidas ao nível da gestão de topo da PSP, para acautelar a segurança do SEI. Consideramos a incidência de opinião nesta categoria assinalável, o que nos permitirá extrair conhecimento. Acresce ainda referir as medidas estratégicas e políticas apontadas como o primeiro passo a dar na implementação de um plano de segurança, que se pretende abrangente, dos sistemas de informação nas organizações. Para Mamede (2006), as políticas de segurança têm um leque de ação muito diversificado, como, por exemplo, a segurança das instalações e da infraestrutura, questões administrativas, procedimentos para utilizadores, acesso físico, etc.. Nas restantes três categorias, assume predominância a categoria referente a "Medidas de

Gestão e Implementação". Esta categoria apresenta uma representatividade suficiente para identificarmos as medidas concretas implementadas, pela PSP, na operacionalização da segurança dos seus sistemas de informação. A categoria "Pessoas" aparece em quarto lugar, com 33 unidades de registo que nos permitem caraterizar a envolvente humana que interage com o SEI. Por último, surge a quinta categoria, "Importância do SEI", com 14 unidades de registo, que de resto nos traduz, de forma consistente, a relevância do SEI na Instituição.

5.1. Necessidade de Proteção do SEI

Nesta categoria, foram consideradas cinco subcategorias que mereceram a distribuição de unidades de registo, constantes no gráfico da Figura 3. A subcategoria mais mencionada pelos entrevistados é a subcategoria "Vulnerabilidades", o que indicia que foram sinalizadas muitas fragilidades no SEI. Por outro lado, a subcategoria menos referida foi "Sabotagens", o que pode revelar a inexistência de ações deste género em relação ao SEI ou, pelo menos, o seu desconhecimento por parte dos entrevistados.

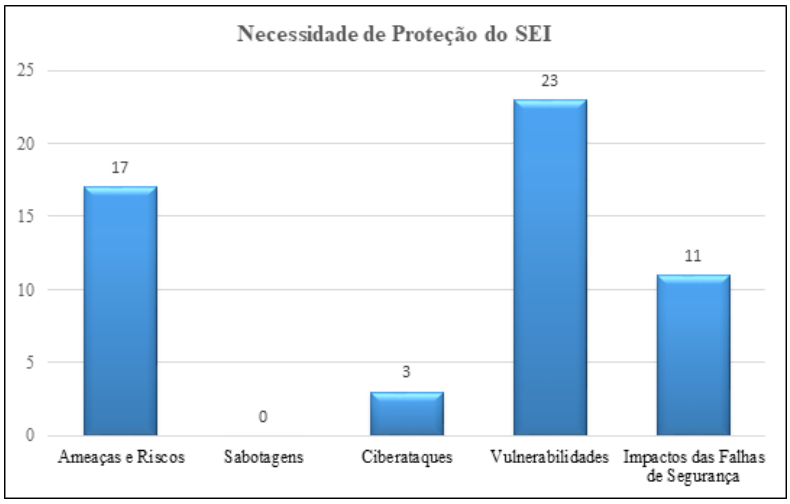


Figura 3- Distribuição das unidades de registo da categoria "Necessidade de Proteção do SEI".

- Vulnerabilidades

A subcategoria "Vulnerabilidades" apresenta uma frequência absoluta de 23 u.r.'s, significando isto que os nossos entrevistados identificam várias vulnerabilidades no SEI. Dividimos as vulnerabilidades em cinco tipos.

O primeiro tipo de vulnerabilidade reporta-se à falta de conhecimento nesta área da segurança dos Sistemas de Informação, manifestada por uma sensação de confiança absoluta na segurança da Rede Nacional de Segurança Interna do Ministério da Administração Interna, expressa por exemplo, na seguinte afirmação: "Considerando que estamos numa rede segura, não deverá acontecer" (u.r. 90). A segunda vulnerabilidade apontada prende-se

com a violação do princípio da necessidade de conhecer no SEI. O princípio da necessidade de conhecer no SEI, estabelece que apesar de um elemento policial ter credenciação para uma determinada informação, apenas deve ter acesso ao conteúdo se existir a necessidade de a conhecer. Esta violação ocorre em virtude de o sistema permitir, a qualquer utilizador, a consulta, a visualização, ou, como é dito na u.r. 28, "a possibilidade de fazermos *download* não controlado de peças de expediente". A terceira vulnerabilidade identificada tem que ver com o estado obsoleto do parque informático da PSP, ou seja, "a idade avançada dos equipamentos informáticos em operacionalidade, para os quais as atualizações de *software* já não são tão frequentes e capazes de fazer face a possíveis e atuais ameaças"(u.r. 107). A quarta vulnerabilidade é referida na u.r. 23, referente à acessibilidade das portas USB dos computadores da PSP, através das quais podem ser injetados conteúdos de forma não controlada. A quinta vulnerabilidade do SEI é identificada na u.r. 72, sendo aqui apresentadas deficiências no processo de descredenciação, ou seja, inconsistências entre os níveis dos perfis atribuídos e a situação do efetivo. Por tudo quanto foi exposto, constata-se que o desconhecimento na área da segurança informática, a violação do princípio da necessidade de conhecer, a idade avançada do parque informático, os acessos não controlados às portas USB dos PC's e as falhas no processo de descredenciação do SEI são as principais vulnerabilidades apresentadas por este sistema de informação.

- Ameaças e Riscos

No que respeita a ameaças e riscos para o SEI, são apontadas 17 u.r. Apontaremos as mais expressivas. Em primeiro lugar, surgem, como principal ameaça, os ataques de negação de serviço (DoS), que contabilizou 5 unidades de registo (cfr u.r.'s 26, 46, 178, 174 e 179), aludindo a u.r. 174, nos seguintes termos: " os ataques de negação de serviço que podem ser uma situação bastante problemática". Seguem-se as ameaças decorrentes dos erros de desenvolvimento das aplicações. Ao SEI, em concreto, é apontado um erro de desenvolvimento, que terá sido cometido depois da arquitetura já se encontrar concebida e em funcionamento. Ou seja, foi introduzida uma alteração ao sistema por forma a permitir a consulta livre das peças de expediente. O fator humano é considerado também uma das primeiras ameaças, "designadamente pelo não cumprimento das medidas básicas de segurança" (u.r.2). Neste ponto, destaca-se a informação relativa a políticas e procedimentos, a ser dada aos colaboradores, quando entram na organização, como é defendido por Mamede (2014). A obtenção e a alteração da informação são apontadas como os principais riscos (cfr. u.r.'s 25, 180, 173 e 198). Sucede que, tanto uma como outra ocorrem quando as ameaças se

concretizam, afetando a segurança da informação mais importante da instituição (informação operacional ou dados pessoais dos elementos da PSP), pela perda de confidencialidade, adulteração ou perda absoluta. Pelo que até aqui constatamos, são referidas três ameaças para o SEI, ou seja, os ataques de negação de serviço, os erros de desenvolvimento e o fator humano. São ainda apontados como riscos a obtenção e a adulteração da informação do SEI.

- Impactos das Falhas de Segurança

Esta subcategoria foi a terceira mais mencionada, enquanto alicerce da necessidade de proteção do SEI, com 11 u.r. São vários os impactos na atividade da instituição que podem advir das falhas de segurança no SEI. Pela análise efetuada, observam-se impactos de vária ordem, que apresentam reflexos diretos na atividade operacional. É referida a diminuição substancial da capacidade de resposta da PSP, ao ser dito, na u.r. 47, que a" Polícia não para, mas a Polícia tem grande dificuldade em dar resposta como dá na situação normal", o que demostra bem a importância que este sistema tem na atividade da PSP. São ainda realçadas dificuldades ao nível da gestão do efetivo, designadamente, na elaboração das escalas de serviço e na atividade do Centro de Comando e Controlo que ativa os meios policiais para as ocorrências policiais (cfr. u.r.'s 114, 115 e 51). No caso de uma falha de segurança permitir o acesso indevido à informação do SEI, esta situação acarretaria "impactos incomensuráveis à instituição" (u.r. 60), na medida em que "a maioria dos processos investigatórios ficariam seriamente comprometidos" (u.r. 62). Outro impacto, não menos importante, relaciona-se com a reputação da credibilidade institucional. A ocorrência destas falhas quebra nitidamente a confiança da população na instituição policial (cfr. u.r.'s 61 e 200). São assim considerados, como possíveis impactos das falhas do SEI, a diminuição da capacidade de resposta da PSP, as dificuldades de gestão do efetivo policial, o comprometimento dos processos investigatórios e da reputação institucional.

- Ciberataques

No que respeita a ciberataques, para três entrevistados, os sistemas de informação da PSP e o SEI, em particular, constituem alvos elegíveis para a concretização deste tipo de ameaça (cfr. u.r.'s 45,172 e 199), presumindo-se que tal se deve à natureza importante da organização (cfr. u.r. 172) e à peculiaridade da informação que estes sistemas contêm, tornando-se "não só elegível como apetecível" para a concretização de ciberataques (cfr. u.r. 199). No entanto, parece-nos reduzida a referência a este tipo de ameaça, quando, na atualidade, constitui uma das formas mais utilizadas na perpetração de ataques a sistemas de informação. Esta circunstância pode dever-se à falta de formação na área da cibersegurança

ou à falta de divulgação interna, da incidência e do *modus operandi* de ataques desta subcategoria nos Sistemas de Informação da PSP.

- Sabotagens

A lei do cibercrime[25], no art.º 5.º, estabelece, como crime de sabotagem informática, toda a ação que vise "entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático […]". Apesar de não terem sido mencionadas, pelos entrevistados, ações deste género no SEI, tal é referido como possibilidade, quando se afirma "…destruir componentes da solução, de maneira que ela fique fora de serviço, é também uma coisa muito pouco desejável" (u.r. 173). A inexpressão de ocorrências nesta subcategoria revela que os entrevistados desconhecem ou ignoram este tipo de ameaça. Contudo, este tipo de fenómeno é uma das fontes de risco apontada por Stewart (2009), ao nível, por exemplo, das alterações de *software* e do registo incorreto dos dados.

5.2. Políticas e Estratégias

Nesta secção, pretendemos aferir o que está a ser feito em termos estratégicos, no âmbito da gestão da segurança dos sistemas de informação da instituição. Neste contexto, incidiremos a nossa análise sobre os seguintes aspetos:" Políticas de Segurança"; "SGSI na PSP"; "Requisitos de Segurança"; "Cibercultura na Instituição"; "Parcerias". No gráfico da Figura 4, nota-se maior prevalência de ocorrências na subcategoria "Políticas de Segurança", revelando que as mesmas existem na instituição e são conhecidas dos nossos entrevistados. Em contrapartida, com menor adesão temos a subcategoria "Parcerias", com uma frequência absoluta de 3 unidades de registo. Este valor indicia ausência de iniciativas deste género na instituição, no âmbito da segurança dos sistemas de informação.

[25] Lei 109/2009, de 15 de Setembro.

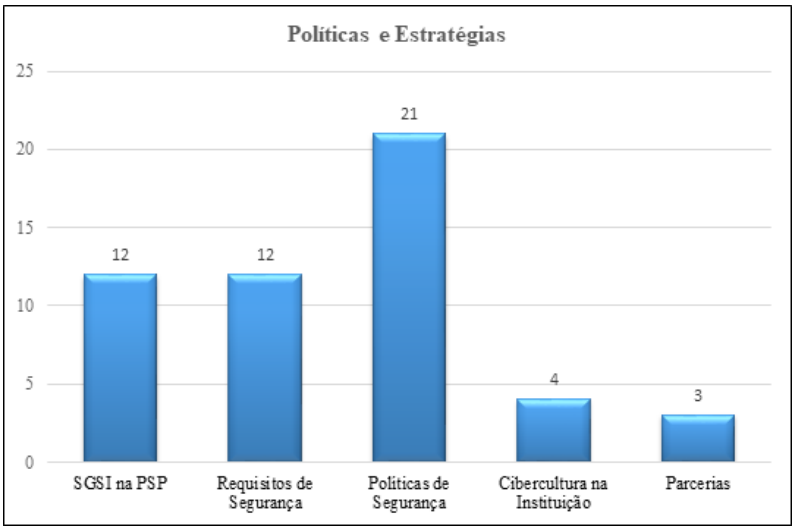


Figura 4 - Distribuição das unidades de registo da categoria “Políticas e Estratégias".

- Políticas de Segurança

A subcategoria “Políticas de Segurança” foi a que apresentou mais unidades de registo, com uma frequência absoluta de 21 ocorrências. Estas políticas de segurança são consideradas fulcrais para a implementação da segurança dos Sistemas de Informação nas organizações, pois são nelas definidas as linhas gerais de ação para a implementação e consolidação dos requisitos de segurança dos sistemas de informação. Normalmente, estas políticas são elaboradas ao nível estratégico, destinando-se a ser aplicadas a toda a organização. Neste contexto, no nosso estudo, foram assinaladas evidências da existência de normas de segurança na área das TIC, que se encontram dispersas no painel normativo interno da PSP. Aponta-se, como exemplo, o bloqueio, por defeito, das portas USB (cfr. u.r. 96), as restrições, aos utilizadores, de operações de administração (cfr. u.r. 95), o acesso limitado à internet (cfr u.r. 97), a aferição das necessidades concretas dos utilizadores, para o desbloqueio das portas USB e o acesso à internet (cfr. u.r.’s 98, 99 e 100), entre outras. Nota-se, de facto, uma preocupação da instituição em acautelar alguns aspetos de segurança dos seus Sistemas de Informação, vertida em diversas NEP’s (cfr u.r. 128). Muitas destas NEP’s são implementadas localmente e pretendem regular os procedimentos de operação, de equipamentos e sistemas, por parte dos utilizadores. Por fim, corroboramos a ideia latente nas evidências de que esta dispersão de normativo é de difícil gestão, contrariando as boas práticas que aconselham a implementação de políticas de segurança únicas e transversais à organização (cfr u.r.’s 185 e 186).

- SGSI na PSP

Com efeito, foi aconselhada, no capítulo 2, a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) nas organizações, o qual deve incidir sobre três vetores, a saber, as pessoas, os processos e as tecnologias. Vejamos, pois, como a PSP acolhe esta sugestão. Quanto à responsabilidade da implementação deste sistema, afirma-se "a implementação de um sistema de gestão deve ser feita pelas pessoas que controlam a organização e, basicamente todos os restantes elementos da organização numa postura de grande transparência." (u.r. 175). Esta envolvência de toda a estrutura organizacional, acompanhada da implementação das normas, dá mais garantias de bons resultados, tornando o sistema mais robusto e criando maior sensibilidade na organização, em torno desta questão (cfr. u.r.176). Em contrapartida, a inexistência de um SGSI, nas organizações, cria, por um lado, uma grande exposição a um conjunto variado de ataques e, por outro lado, gera uma incapacidade de prevenir, detetar, reagir e recuperar de um incidente (cfr. u.r.'s 177 e 201). Neste sentido, o SGSI permite perceber a segurança do Sistema de Informação de forma mais abrangente (cfr. u.r. 202). Da análise das evidências, foram sinalizadas doze unidades de registo sobre este item, sendo generalizada a opinião de que a PSP não dispõe de um Sistema de Gestão de Segurança de Informação, devidamente implementado e consolidado (cfr. u.r.'s 34, 35, 36, 41, 86, 94 e 120). São notadas ações isoladas, que denotam alguma preocupação em torno deste tema, sem que o mesmo seja efetivamente abordado de forma sistémica. Convém também aqui referir que o Ministério da Administração Interna (MAI) instituiu uma Política de Segurança de Informação, nela dispondo que os serviços previstos no Dec-Lei n.º 203, de 27 de Outubro, dos quais a PSP é parte integrante, devem manter um SGSI, por forma a assegurar a integridade, a disponibilidade e o acesso à informação que lhes permita a prossecução dos respetivos objetivos.

- Requisitos de Segurança

Vimos no Capítulo 2 que os requisitos de segurança que mais contribuem para a segurança da informação são a confidencialidade, a integridade e a disponibilidade. Estes princípios são tidos como uma das exigências a alcançar com, implementação e manutenção do SGSI. Neste sentido, procuraremos perceber de que forma as opiniões dos entrevistados se posicionam relativamente à observância destes requisitos no SEI. Desde logo foram referidos quatro princípios na construção do SEI, ou seja, a credenciação, a acessibilidade, a disponibilidade e a fiabilidade, o que em certa medida revela que existiu uma preocupação com os requisitos de segurança da informação, na conceção do sistema (cfr. u.r. 9). Outro

dos princípios subjacentes foi o da necessidade de conhecer (cfr. u.r. 10). Já na atualidade, constata-se que o SEI apresenta deficiências no cumprimento dos requisitos de confidencialidade (cfr. u.r.'s 15, 17 e 74). No que respeita à disponibilidade, as evidências apontam no sentido de que a mesma é assegurada, visto que o SEI está permanentemente disponível na maior parte do ano (cfr. u.r. 14). Por outro lado, a integridade dos dados não é totalmente assegurada, devido à existência de algumas incoerências e duplicações. Neste aspeto, é apontada a questão dos itens semelhantes, situação que assenta na criação de entidades duplicadas no SEI, e que não está prevista concetualmente, uma vez que a existência de entidades deve ser única no sistema. De resto, esta situação merece o respetivo tratamento, através da retificação dos dados, em sede de qualidade (cfr u.r.'s 16, 73 e 85).

Finalmente, aponta-se, como um requisito de segurança não preenchido, a falta de credenciação do SEI pela Autoridade Nacional de Segurança (ANS). Esta falha inviabiliza a utilização do SEI no âmbito de matérias classificadas (cfr. u.r.'s 18 e 70). Consideramos esta credenciação extremamente necessária, na medida em que, por um lado, contribuiria para o reforço de segurança do SEI e, por outro lado, permitiria a rentabilização da sua utilização.

- Cibercultura na Instituição

Outro vetor de intervenção estratégico na segurança do SEI passa por criar e sedimentar uma cultura de cibersegurança na instituição. Contudo, perceciona-se que, pela escassez de evidências neste domínio, existe ainda um longo caminho a percorrer. Não obstante os esforços realizados, são insuficientes os indícios que nos permitam concluir pela existência de iniciativas estruturadas e sistematizadas neste domínio. Ao invés, é mencionado que o efetivo possui uma fraca sensibilidade para estas questões, o que evidencia a ausência de uma cultura institucional generalizada e consolidada nesta área, tornando-se necessário reformar mentalidades (cfr. u.r.'s 84, 152 e 146). Ao que parece, esta realidade institucional não foge muito do panorama a nível nacional (cfr. u.r. 197).

- Parcerias

O estabelecimento de parcerias também se pode apresentar como uma mais-valia na prossecução da segurança dos sistemas de informação. O contacto privilegiado com as comunidades, científica, académica e empresarial, neste setor, poderá contribuir para o recrutamento de conhecimento útil para a instituição. Ao nível de parcerias interinstitucionais, não são referidas quaisquer iniciativas, não significando isto a sua inexistência. Contudo, foi mostrada a disponibilidade de cooperação por parte do Centro

Nacional de Cibersegurança, o que poderá constituir uma vantagem para a instituição. Foi disponibilizada colaboração ao nível da gestão e da reação dos incidentes, da sensibilização de quadros, do apoio em referenciais e melhores práticas de segurança e, por fim, do incremento da maturidade (prevenção, deteção, reação e gestão da segurança) nas organizações (cfr. u.r.'s 207, 206 e 208).

5.3. Medidas de Gestão e Implementação

Avançamos agora para o estudo das "Medidas de Gestão e Implementação" da segurança nos Sistemas de Informação da PSP, de forma geral, e do SEI, em particular. Abordaremos, assim, cinco aspetos considerados relevantes para o estudo em curso, a saber, "Resposta a Incidentes Críticos", as "Auditorias de Segurança", os "Mecanismos de Segurança", as "Medidas de Contrainteligência" e, por último, os "Exercícios de Cibersegurança". No gráfico da Figura 5, notamos que existe uma prevalência de unidades de registo na subcategoria "Resposta a Incidentes Críticos", que, a nosso ver, revela que os entrevistados, de forma geral, possuem uma opinião formada sobre este tipo de ação, desencadeada pela PSP, quando ocorre um incidente deste género. Por outro lado, existe uma fraca frequência de opiniões na subcategoria "Exercícios de Cibersegurança", o que demonstra que as iniciativas nesta área, na instituição, são residuais.

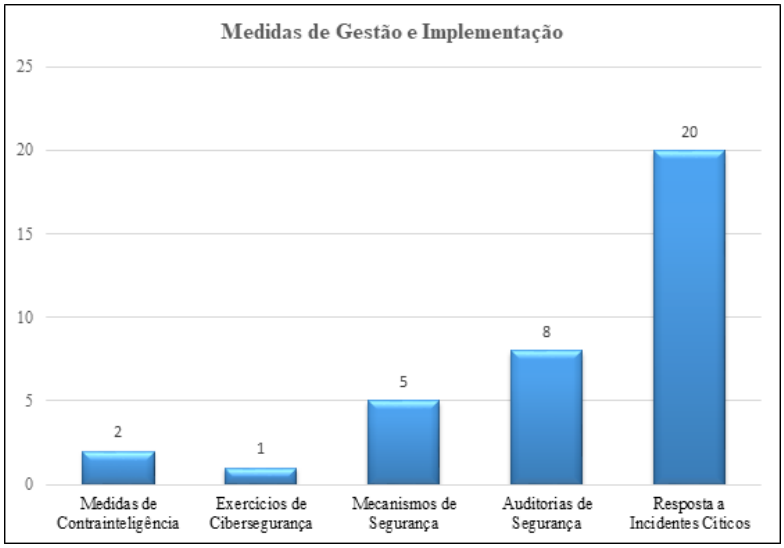


Figura 5- Distribuição das unidades de registo da categoria "Medidas de Gestão e Implementação".

- Resposta a Incidentes Críticos

Abordamos a questão da resposta a incidentes críticos no SEI. Como já vimos anteriormente, a ocorrência de incidentes críticos relaciona-se com quaisquer eventos de

segurança que afetem o normal funcionamento dos sistemas de informação. Esta resposta exige, normalmente, algum planeamento e preparação. Parte da solução passa por traçar um plano de contingência. Este plano de contingência contém uma sequência de ações a desenvolver para recuperar o funcionamento dos sistemas no mais curto prazo possível. Outra medida recomendável é a constituição de uma equipa de resposta a incidentes críticos. Vejamos como a PSP prepara esta resposta aos incidentes críticos no SEI. Para começar, foram indicadas como principais incidentes no SEI, as falhas dos servidores que originam a lentidão do sistema ou a sua completa inoperacionalidade (cfr. u.r.'s 104 e 134). Conseguiu-se apurar a existência de um plano de contingência para responder aos incidentes críticos no SEI. Este plano consiste no recurso a formulários de peças de expediente, que se encontram disponíveis no portal interno da PSP. Esta solução visa responder às necessidades operacionais de *front office* da PSP, no caso de inoperabilidade do SEI. Logo que o funcionamento do sistema seja restabelecido, as peças de expediente são vertidas no SEI, garantindo-se, desta forma, a consistência dos dados. (cfr. u.r.'s 49, 50 e 63). Apenas uma evidência nos aponta a existência de três servidores, na Direção Nacional, que permitirão a redundância dos dados e permitirão a continuidade da operação, caso um deles entre em rutura (cfr. u.r. 135). Apurou-se também que o processo de resolução do incidente se encontra bastante centralizado no Departamento de Sistemas de Informação e Comunicações da Direção Nacional da PSP. Os Núcleos de Sistemas de Informação e Comunicações, das unidades orgânicas da PSP, têm uma intervenção bastante limitada neste processo, limitando-se, na maior parte dos casos, a reportar o incidente ao DSIC, podendo colaborar pontualmente na resolução do incidente (cfr. u.r.'s 82, 105, 106, 138, 139, 141 e 142). Ainda neste contexto, é feita menção ao COSI, que faz o tratamento de incidentes ocorridos na RNSI. A ocorrência destes incidentes é notificada à PSP em relatórios mensais, o que também não nos parece razoável, dada a rapidez com que este tipo de ameaça se propaga. Destaque, ainda, para a proposta de se implementar, na PSP, uma equipa de resposta a incidentes críticos. Esta proposta não terá ido avante, o que, numa organização com a dimensão e as caraterísticas da PSP, nos parece, no mínimo, preocupante. (cfr. u.r.'s 40 e 44). Perante as evidências, parece-nos que este tipo de resposta se encontra algo incipiente, carecendo ainda de algum investimento humano e tecnológico. (cfr. u.r. 52).

- Auditorias de Segurança

As auditorias de segurança são procedimentos de inspeção que permitem verificar se as políticas de segurança se encontram devidamente aplicadas. Permitem também detetar

vulnerabilidades, com vista à adoção de medidas corretivas. Da análise das respostas apresentadas, no âmbito do nosso estudo, não existem evidências da existência de um plano de auditorias periódicas ou inopinadas, transversal à instituição (cfr. u.r. 103). Contudo, ao nível local e no domínio da infraestrutura, são desenvolvidas várias ações de auditoria técnica (cfr. u.r.'s 131, 132 e 133). Apesar de ser considerada importante e recomendada ao nível das organizações, consideramos que esta prática não está estruturada e consolidada de forma transversal na PSP, apresentando-se ainda numa fase incipiente (cfr. u.r.'s 171,189 e 191).

- Mecanismos de Segurança

Os mecanismos de segurança são as ferramentas que permitem operacionalizar as políticas de segurança. Julgou-se de grande importância perceber os mecanismos de segurança empregues pela PSP na manutenção da segurança do SEI. Desde logo, pudemos constatar, na nossa análise, várias referências a mecanismos de controlo e acesso ao SEI, designadamente, na atribuição de perfis que restringem o acesso a determinados tipos de informação (cfr. u.r. 124). Foi sugerida a implementação de sistemas auxiliares ou de dispositivos de segurança que permitam controlar com mais aperto a informação que entra e sai da organização (cfr. 182, 188 e 192). Contudo, não são evidentes quaisquer sinais da existência destes dispositivos na proteção do SEI, sendo-nos possível afirmar a sua inexistência. Também foi evidenciada a possibilidade de as aplicações informáticas gerarem eventos de negócio, que permitem aferir o histórico das operações (cfr. u.r. 184). Neste domínio, cabe-nos acrescentar que o SEI permite o registo das operações dos utilizadores, cujo histórico pode ser consultado em sede de auditoria, no âmbito inspetivo, disciplinar ou judicial (cfr. u.r. 83). Dada a escassez de evidências apresentadas, não podemos concluir pela existência de um leque de mecanismos de segurança do SEI, podendo esta circunstância advir de algum desconhecimento desta área na instituição.

- Medidas de Contrainteligência

Uma das medidas que assume especial relevância na proteção dos ativos das organizações policiais é a contrainteligência. Para Fernandes (2014), estas medidas visam identificar, analisar e avaliar os riscos que impendem sobre as atividades policiais, tendo por fim garantir os ativos (humanos, infraestruturas, sistemas de informação e comunicações, etc). A importância deste tipo de medidas numa instituição policial é ainda mais acentuada devido à possibilidade de comprometimento da missão. Como seria expectável, incidiremos a nossa análise em evidências de medidas de contrainteligência adotadas em relação ao ativo

tecnológico da PSP em estudo, o SEI. Neste domínio, não foram assinaladas quaisquer evidências concretas que nos permitissem afirmar a existência de medidas deste género em curso na PSP (cfr. u.r. 31). No entanto, a falta de evidências destas medidas não nos deixa concluir pela sua inexistência, atendendo o caráter altamente reservado desta atividade no seio da PSP (cfr. u.r. 32). Nesta perspetiva cabe-nos aqui recrutar o conceito de segurança pela ocultação (Security by Obscurity), em que o princípio base subjacente é que "se ninguém souber como a segurança é aplicada então ninguém poderá subvertê-la de forma objetiva" (Zúquete, 2014, p.18).

- Exercícios de Cibersegurança

Os exercícios de cibersegurança servem para testar a capacidade de resposta a ciberataques. Este tipo de exercício constitui uma excelente oportunidade para serem adquiridos treino, experiência e *know-how*, no contexto da segurança dos sistemas de informação. Alguns desses exercícios são organizados por organismos nacionais (e.g Forças Armadas, CNCS), ou por organismos internacionais (ENISA – CyberEurope). Permitem aquilatar o grau de adestramento do efetivo que integra os serviços de segurança informática da instituição. No nosso estudo, há referência à participação de elementos da PSP em vários exercícios de cibersegurança, não só nos exercícios militares anuais, mas também nos exercícios já desenvolvidos pelo Centro Nacional de Cibersegurança (cfr. u.r. 43). Esta evidência revela que esta prática não é totalmente estranha à instituição, o que desde logo se assinala como positivo. Contudo, não é feita qualquer referência a iniciativas no seio da instituição, o que poderia constituir uma boa prática, na medida em que permitiria acentuar o treino nesta área e traria também a oportunidade de a instituição testar a segurança dos seus sistemas de informação, com vista à adoção de ações corretivas.

5.4. Pessoas

Outro dos grandes eixos de intervenção, que decidimos abordar no contexto do presente estudo, prende-se com aspetos de segurança do SEI, associados às pessoas que interagem com este sistema. São, assim, focados os seguintes aspetos: "Ação Disciplinar"; "Formação e Sensibilização dos Recursos Humanos em Cibersegurança"; "Responsáveis pela Segurança"; "Desenvolvedores do SEI". No gráfico da Figura 6, destaca-se uma forte incidência de opinião sobre a subcategoria da "Ação Disciplinar", refletindo a ação que a instituição desenvolve neste domínio sobre as pessoas que violam aspetos de segurança do SEI. Em contraste, são feitas apenas duas referências à subcategoria "Desenvolvedores do

SEI", o que revela a ausência de pessoas da instituição envolvidas no desenvolvimento do SEI.

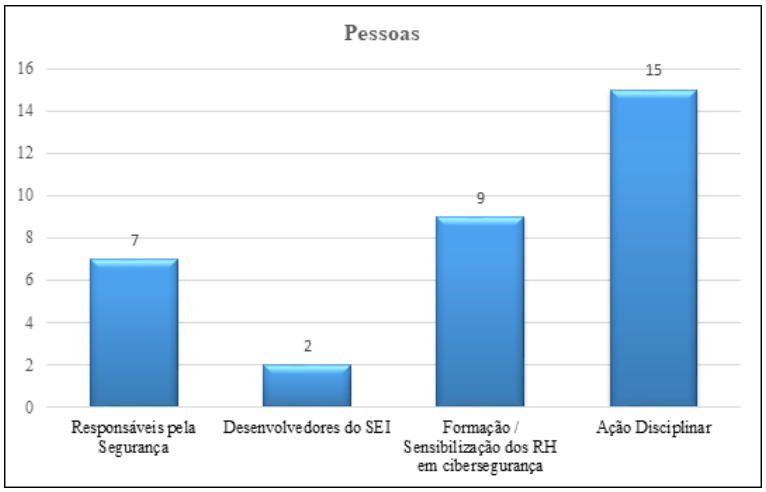


Figura 6 - Distribuição das unidades de registo da categoria "Pessoas".

- Ação Disciplinar

Uma dimensão que quisemos abordar neste estudo tem que ver com a reação desencadeada pela instituição, quando em presença de comportamentos indevidos, por parte dos colaboradores, que coloquem em causa a segurança dos sistemas de informação da PSP. Neste sentido, são apresentadas evidências de que, na esfera de ação das aplicações ,informáticas da PSP, o sistema de informação sobre o qual tem havido maior incidência de utilização abusiva é o SEI (cfr. u.r.143). Esta utilização abusiva consubstancia-se pelas seguintes práticas: consulta e divulgação de informação a terceiros; consulta não inteiramente explicada e esclarecida e consulta com intenção dolosa de obter ganhos ou qualquer benefício dessa transmissão ilícita de informação (cfr. u.r.'s 144 e 145). Estes comportamentos constituem, em nossa opinião, uma violação grosseira dos deveres profissionais, éticos e deontológicos, atacando, assim, o princípio da necessidade de conhecer, o dever de sigilo profissional, previsto no art.º 12.º do Regulamento Disciplinar da PSP (RDPSP)[26] e, em alguns casos, integram matéria de índole criminal. Neste ponto, é registada alguma falta de consciencialização sobre a responsabilidade que impende sobre a informação contida no SEI, bem como na manutenção das credenciais que dão acesso a este sistema. Desta forma, a tónica é colocada na responsabilização de quem adote comportamentos contrários ao estabelecido (cfr. u.r.'s 147, 153 e 154). O dispositivo legal, as recomendações e as sanções dão resposta a quem viole a segurança da informação contida

[26] Lei n.º 7/90, de 20 de Fevereiro.

no SEI (cfr. u.r. 151). Assim, quando alguma situação de violação da segurança da informação do SEI chega ao conhecimento dos serviços de disciplina da instituição, seja por via interna ou por via externa, é instruído o correspondente processo disciplinar, sendo realizadas as diligências necessárias à descoberta dos factos, sustentando-se esta investigação, na maior parte das vezes, em prova documental e testemunhal (cfr. ur's 155, 157, 158, 159, 160 e 161). Esta tramitação não invalida que seja dado conhecimento às autoridades judiciais, sempre que se verifique estar na presença de factos que possam constituir matéria criminal. No que respeita à parte disciplinar, as consequências consistem em sanções de natureza disciplinar, variando em função da acentuação da censura do comportamento, abrangendo normalmente desde penas de multa a suspensão de serviço.

- Formação/Sensibilização dos RH em Cibersegurança

Um dos aspetos mais relevantes para a gestão da segurança dos sistemas de informação nas organizações está relacionado com a Formação e a Sensibilização do RH na área de cibersegurança. Neste contexto, foram colocadas diversas questões aos entrevistados, no sentido de se perceber em que medida é ministrada formação, nesta área, na instituição.

Neste sentido, foi referida uma formação, ministrada no âmbito do Curso de Formação de Oficiais de Polícia, no ISCPSI (cfr. u.r. 32). Considera-se esta formação um bom ponto de partida, atendendo às funções de comando ou chefia que os alunos deste curso irão desempenhar na instituição. No que respeita ao restante dispositivo, foi consistente a ideia de que não é conhecida qualquer outra formação ou plano de formação autónomos, neste domínio na PSP (cfr. u.r.'s 33, 39, 101 e 129). De resto, esta constatação foi confirmada com a análise do plano de formação do Departamento de Formação da Direção Nacional da PSP. O que existe nesta área é ministrado no âmbito de formações SEI e outras similares, bem como nos contactos com as SSIC das Divisões (cfr. u.r.'s 102 e 148). Face à ausência de formação autónoma e especializada nesta área, foi passada a mensagem da pertinência da implementação de um processo de formação contínuo, nesta área, na instituição (cfr. u.r.'s 78 e 191).

- Responsáveis pela Segurança

No que diz respeito à responsabilidade pela segurança dos sistemas de informação da PSP, em geral e do SEI, em particular, é apontada desde logo uma entidade externa à PSP – o Centro de Operações de Segurança Informática (COSI) (cfr. u.r. 30), ou seja, o serviço responsável pela segurança tecnológica da RNSI do MAI, que é, como já vimos, a infraestrutura em que se insere o SEI. Ao nível da PSP, são apontados como principais

responsáveis, a nível orgânico, o DN/DSIC e o DN/DIP (cfr. u.r. 88). São ainda identificadas as divisões e os núcleos do DSIC, de acordo com o despacho das unidades flexíveis da PSP (cfr. u.r. 38). Parece-nos consentâneo que toda a estrutura policial tem responsabilidades de segurança do sistema (cfr. u.r. 87). Foi destacada ainda, a figura do Elemento de Ligação Informática (ELI), regulada na NEP N.º DN/GINFOR/99/01, de 22 de Agosto de 2003. Os ELI's são nomeados em cada subunidade, por Divisão, e, entre outras funções que desempenham, têm a incumbência de verificar periodicamente a correta atribuição dos perfis existentes no seu serviço (cfr u.r. 127). De forma genérica, foram indicados nas respostas dos entrevistados, alguns dos principais intervenientes na segurança dos sistemas de informação na PSP. Contudo, podemos reforçar e complementar as respostas dadas, recorrendo a diversos normativos, que a seguir se expõem. A Portaria n.º 383/2008, de 29 de Maio, no art.º 9, explana as competências do DSIC, no âmbito da gestão da segurança dos Sistemas de Informação da PSP. Também o Despacho n.º 19935/200, de 17 de julho, que define as unidades orgânicas flexíveis da Direção Nacional da Polícia de Segurança Pública (PSP), cria no artigo 1, al) h, integradas no DSIC, duas Divisões com incumbências no âmbito dos Sistemas de Informação da PSP, a Divisão de Gestão e Segurança de Infraestruturas Tecnológicas (DGSIT) e a Divisão de Serviços e Sistemas de Informação (DSSI). Aquele despacho destaca também a responsabilidade que impende sobre a Divisão de Segurança e Gestão da Informação, a qual se encontra integrada no Departamento de Informações Policiais. A esta Divisão compete desenvolver várias atividades confluentes com a segurança da informação nos sistemas de informação da PSP, nomeadamente, realizar as adequadas averiguações de segurança, em caso de quebra ou comprometimento de segurança da informação, nos termos da lei em vigor, e o exercício de funções de gestão e coordenação permanente, bem como de apoio relativamente ao módulo do sistema de informações policiais. A NEP nº DN/ASDDN/GEP/03/01, de 24 de janeiro de 2011, define os princípios e as regras de utilização, exploração e gestão do SEI. Nesta norma, são apresentadas várias entidades que consideramos relevantes na manutenção da segurança do SEI. Em primeiro lugar, realçamos a Equipa Única do SEI (EUSEI), responsável pela coordenação central das atividades do SEI. Esta equipa é assessorada tecnicamente pelo Gabinete de Sistemas de Informação (GSI). Outra figura ali referida é o Oficial de Ligação SEI (OLSEI), o responsável local pelas atividades do SEI. Encontra-se nomeado um OLSEI em todas as unidades, estabelecimentos de ensino e departamentos da Direção Nacional da PSP. Naquela NEP, é também contemplado um serviço de *Helpdesk* SEI. Este serviço é um

ponto de apoio aos utilizadores SEI, na vertente policial e na vertente técnica, estruturando-se em dois níveis: o local e o nacional.

- Desenvolvedores do SEI

Ainda no vetor das pessoas, ganham especial destaque as pessoas ou os serviços que, de uma forma ou de outra, estão ligados ao desenvolvimento do SEI. Neste âmbito, foi pouco expressiva a quantidade de testemunhos que abonassem em torno desta questão. Neste domínio, as evidências apontam para uma preocupação com as competências técnicas das pessoas que desenvolvem este tipo de aplicação. É referido que estas pessoas devem dar algumas garantias de capacidade e de qualidade técnica (cfr. u.r.'s 181 e 187), opiniões com as quais não podemos deixar de concordar. No caso em estudo, o SEI foi concebido e desenvolvido pela empresa Accenture, uma empresa de consultadoria de gestão, tecnologias de informação e *outsourcing*, oficialmente reconhecida nesta área, o que, à partida, confere as garantias necessárias de compromisso para o desenvolvimento da aplicação. Salientam-se, ainda, para o desenvolvimento do SEI, as pessoas e os serviços pertencentes à PSP, que, de forma mais direta, estiveram ligados à sua conceção, desenvolvimento e exploração, pelo que aqui se faz, mais uma vez, alusão à NEP nº DN/ASDDN/GEP/03/01, de 24 de janeiro de 2011. Destaca-se ali a Equipa Única do SEI que assume especial preponderância na gestão e no suporte ao desenvolvimento do SEI. Embora a existência desta equipa esteja ali prevista, durante o presente estudo, não detetamos evidências concretas da sua existência. A Divisão de Serviços e Sistemas de Informação, do DSIC, também assume especial relevo no desenvolvimento aplicacional na instituição, realçando-se, entre outras competências, a gestão de serviços de desenvolvimento de *software* em regime de *outsourcing* no âmbito dos Sistemas de Informação. Pelo exposto até ao momento, verifica-se que o desenvolvimento do SEI vem sendo realizado em regime de *outsourcing*, sob orientação e coordenação da PSP. Neste ponto, admitimos que possam ser levantadas questões em torno do desenvolvimento aplicacional da instituição, em regime de contrato de prestação de serviços (*outsourcing*), dado que este regime suscita algumas reservas, devido à natureza da instituição e ao tipo de matérias que nela são tratadas.

5.5. Importância do SEI na PSP

Abordamos aqui a categoria "Importância do SEI na PSP", verificando a dispersão de unidades de registo que se enquadram nas respetivas subcategorias. Constata-se, no gráfico da Figura 7, uma dispersão homogénea de valores com ligeiras oscilações. A subcategoria mais mencionada trata-se de "Contributo do SEI para a PSP", com uma

frequência absoluta de 9 ocorrências, valor que reflete a centralidade do sistema nas diversas atividades da PSP. Por outro lado, a subcategoria menos invocada foi a "Tipologia de Informação do SEI", com uma frequência absoluta de 5 unidades de registo. Na nossa opinião, este valor pode apontar para uma falta de conhecimento absoluto da abrangência dos tipos de informação que o SEI comporta. Analisemos, de seguida, os elementos identificados em cada subcategoria.

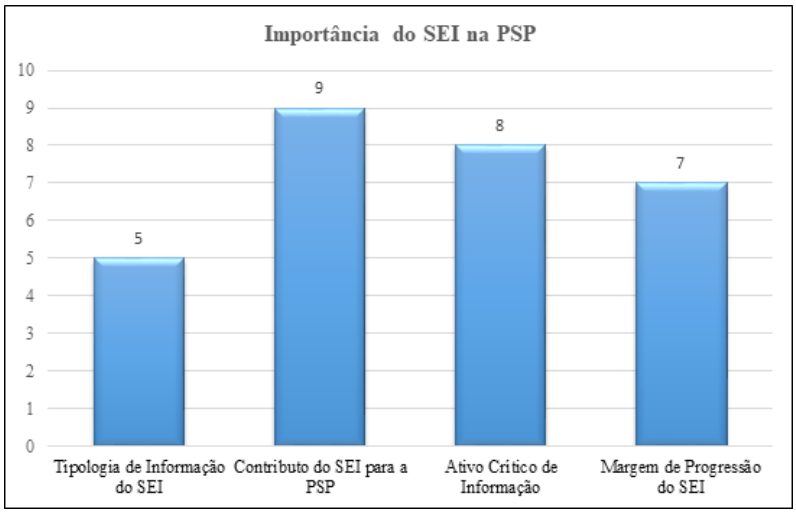


Figura 7 - Distribuição das unidades de registo da categoria "Importância do SEI na PSP".

- Contributo do SEI para a PSP

Logo numa primeira impressão, diríamos que um dos maiores contributos do SEI na prossecução das atividades da PSP é "permitir a centralização da informação e a sua análise." (cfr. u.r. 5). A necessidade de centralização da informação foi um dos aspetos que esteve subjacente à conceção e implementação deste sistema. Com efeito, este objetivo foi alcançado na medida em que "O SEI alimenta, em termos comparativos, mais de metade da informação que se partilha entre os Órgãos de Polícia Criminal (OPC's), designadamente, através da PIIC" (cfr. u.r. 2). No que respeita à análise da informação, podemos referir que este sistema constitui uma ferramenta importantíssima, visto que é uma fonte, por excelência, de informação de diferentes tipos, a que os analistas podem recorrer, na fase de pesquisa, para produzir produtos de informação ou de inteligência, servindo de apoio à decisão de comando operacional e de âmbito operacional (cfr. u.r. 8). Neste sentido, o SEI não deve ser encarado como uma mera ferramenta de elaboração de expediente, dado que também "constitui um importante repositório de informação, imprescindível ao desenvolvimento normal e eficaz da missão da PSP" (cfr. u.r. 57). O SEI é, ainda, uma importante ferramenta de gestão de meios humanos e materiais (cfr. u.r. 58), podendo-se

referir, a título de exemplo, o recurso feito pelo Centro de Comando e Controlo (CCC), na gestão de meios disponíveis para responder às ocorrências, no SEI – Gestor de Incidentes (cfr. u.r. 136). Sintetizando, considera-se que os maiores contributos do SEI para a atividade desenvolvida pela PSP passam pela GESTÃO - a gestão de informação e a gestão de meios (humanos e materiais).

- Ativo Crítico de Informação

Até aqui, vimos o tipo de informação que o SEI comporta, bem como o importante contributo que este sistema de informação dá, nas diversas atividades desenvolvidas pela instituição. Neste mesmo alinhamento, procuraremos evidenciar a criticidade desta infraestrutura de informação para a PSP. Desde logo, podemos referir o papel extremamente relevante que este sistema assume no contexto do SIIC, pelo volume de informação criminal partilhada através da PIIC. Na u.r. 3, é referido o facto de a PSP ter muito mais informação do que os outros atores que integram a PIIC. Salienta-se que a troca de informação criminal entre forças e serviços de segurança é extremamente importante no âmbito da cooperação policial na esfera da ação penal. Daí que "o SEI se apresente como um ativo crítico, não só para a PSP, mas também para os outros Órgãos de Polícia Criminal e para o Ministério Público (MP) (cfr. u.r. 4) ". É neste sentido que o SEI se apresenta como um repositório de informação sem precedentes ao nível das polícias. Na u.r. 27, é igualmente mencionado, a propósito da concretização de ciberataques, que o ativo intangível mais precioso que a PSP pode ver afetado é efetivamente a informação do SEI. No mesmo sentido se aponta, na u.r. 54, ao ser afirmado que o SEI tem um enorme potencial para ser explorado por indivíduos e/ou organizações, reportando-se à informação nele contida. Muitos elementos cruciais da atividade da PSP encontram-se registados em plataformas digitais, especialmente no SEI, como é referido na u.r. 149. Por tudo quanto foi até aqui dito, sustentado em testemunhos dos entrevistados, corrobora-se a ideia de que o SEI é um importante ativo crítico de informação na PSP, pelo recurso intensivo que lhe é feito e pelo efeito aglutinador que assume no vasto leque de informação que advém das diversas atividades desenvolvidas na instituição.

- Margem de Progressão do SEI

A importância do SEI, para a PSP, pode ainda ser expressa através da identificação das suas eventuais formas de evolução, com vista à otimização e à rentabilização da sua utilização. Neste sentido, deve-se considerar que o processo de gestão da segurança dos sistemas de informação, por ser um processo proactivo e evolutivo, identifica

vulnerabilidades do sistema, visando a sua supressão, através do desenvolvimento sustentado do sistema. Desta forma, constata-se que algumas funcionalidades do sistema ficam aquém do desejável, tanto em termos de produtividade como de segurança, pelo que serão apontadas algumas sugestões de desenvolvimento. Desde logo, sobressaem as limitações do uso da informação (cfr. u.r. 6), uma vez que o conhecimento produzido neste sistema poderia ser rentabilizado através da análise de informação. Esta limitação do sistema poderia ser ultrapassada com a aplicação de "motores de pesquisa e análise prospetiva, que hoje em dia são banais nas grandes organizações"(cfr. u.r. 7). Outra questão que robusteceria o SEI passaria pela sua credenciação, através da ANS, para que pudesse comportar matérias classificadas. Apesar de existirem evidências de que tal processo terá sido iniciado, até ao momento, não se concretizou, sendo relativamente fácil de o implementar (cfr. u.r. 19). Outra possibilidade de desenvolvimento a contribuir para o reforço da segurança do SEI passaria por melhorar o sistema na restrição de visualização e impressão de peças de expediente, ideia recrutada da u.r. 29. Neste estudo, são ainda apontadas possíveis melhorias no desenvolvimento e na difusão de módulos, como o da Investigação Criminal, das Informações Policiais e o da Organização de Operações Policiais. (cfr. u.r. 79). No que concerne à inserção de dados no SEI, também se nota que há algo a melhorar. "Quer isto dizer que deve existir uma preocupação permanente e contínua para que todos os utilizadores coloquem a informação de forma correta, íntegra, sem erros ou duplicações, optando sempre pela atualização e melhoramento da informação já existente" (cfr. u.r. 80), sendo esta uma preocupação sentida na instituição, que tem como resposta o controlo dos dados em sede de qualidade. Em termos de promoção da versatilidade do sistema, há a referir a possibilidade de evolução para uso em dispositivos móveis, o que representaria uma mais-valia para o serviço operacional (cfr. u.r. 111).

- Tipologia de Informação do SEI

No sentido de percebermos a importância do SEI na instituição, torna-se relevante identificar o tipo de informação que nele é depositada. Sabemos que este sistema de informação foi concebido e implementado em 2004, perante um quadro de grande exigência para a PSP, que comportava a segurança de um evento de grande dimensão, como o foi, no caso, o Euro 2004. Concomitantemente, este sistema foi concebido para responder às necessidades sentidas pela instituição de possuir um sistema de informação centralizado e integra, que agilizasse a gestão da informação da PSP. O SEI, desde a sua implementação até à atualidade, foi evoluindo, vindo a assimilar novas funcionalidades, decorrentes da

missão da PSP. Neste sentido, apurou-se que o SEI se apresenta como "um relevante repositório de informação policial de cariz sensível" (cfr. u.r. 53). Nele são armazenadas e depositadas várias matérias, "principalmente de cariz criminal, contraordenacional e cível (ex. as participações de acidentes) " (cfr. u.r. 65). Para além desta informação, "são ali depositadas diversas informações policiais, tais como, identificações de pessoas, dados pessoais, fotografias e moradas" (cfr. u.r. 66). Parte integrante do SEI é, também, o módulo de pedidos externos, através do qual são introduzidos no sistema "informações e pedidos de diligências, oriundos de entidades externas, tais como, tribunais e outras forças de segurança" (cfr. u.r. 67). No SEI, "ficam também armazenadas matérias relacionadas com a gestão de meios humanos (escalas, excessos) e com a gestão de meios materiais (acionamento de meios, meios disponíveis, ocorrências) " (cfr. u.r. 68). Pelo que foi até aqui demonstrado, o tipo de informação que o SEI comporta resulta de um vasto leque de atividades desenvolvidas pela PSP, a nível logístico, administrativo e operacional, informação essa que apresenta um cariz sensível, peculiar e de alguma reserva, merecendo especial atenção e sensibilidade, dada a sua importância na PSP. Vejamos de seguida o contributo do SEI para as atividades desenvolvidas na Instituição.

Conclusão

A segurança dos ativos informacionais, no meio digital, assume nos dias de hoje uma importância incontornável na sociedade da informação. O acesso e a partilha de informação através de novos meios tecnológicos, vulgo, Tecnologias de Informação e Comunicação, tornaram-se um paradigma sobre o qual assentam os processos de gestão informacional da sociedade contemporânea. Esta realidade encontra-se presente à escala mundial, muito devido à rede tecnológica global - a internet -, marco tecnológico que revolucionou o paradigma do acesso e da partilha da informação, constituindo-se como uma verdadeira autoestrada digital.

Mas, se é certo que esta teia tecnológica fomenta a aproximação dos povos e das economias, trazendo consigo inúmeros benefícios, não devemos ignorar que a mesma gera igualmente uma dependência excessiva das infraestruturas críticas de informação, pelo valor intangível das matérias que estas comportam. Repare-se que neste meio virtual emergem diversos perigos que se propagam a uma velocidade vertiginosa. Desde logo, pela ocorrência de diversos incidentes, de origem natural ou decorrentes da ação humana, inadvertida ou intencional. Neste último caso, assiste-se mesmo à migração de determinados fenómenos criminais, comuns na realidade física, para a realidade virtual, dando origem ao conceito de cibercriminalidade. A constatação desses perigos suscitou na sociedade, em geral, uma consciência coletiva de que algo havia a fazer neste domínio. Foram assim emergindo diversos organismos, estatais e privados, que se debruçaram sobre as questões da segurança no meio digital, dando corpo ao que hoje se designa por cibersegurança.

No presente trabalho, ganhamos consciência da dinâmica que borbulha em torno desta problemática, através da constatação das diversas manifestações, de âmbito jurídico e normativo, das quais extraímos vários subsídios para a construção dos alicerces da presente investigação. Constatou-se, por exemplo, que, a nível Europeu, foram tidas diversas iniciativas políticas e legislativas, com vista à preservação da segurança no meio virtual e à diminuição dos efeitos colaterais da sua violação. Destacam-se, neste sentido, a adoção das seguintes medidas: a Estratégia Europeia para a Cibersegurança, a Convenção sobre a Cibercriminalidade do Conselho da Europa, a Diretiva 91/250/CEE do Conselho, que garante a proteção jurídica dos programas de computador; a Diretiva 2013/40/EU do Parlamento Europeu, de 12 de agosto, que tem por objetivo a aproximação do direito penal dos Estados-Membros no domínio dos ataques contra Sistemas de Informação; a Diretiva (EU) 2016/1148 do Parlamento Europeu, de 06 de julho, que adota medidas adequadas a

garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia, obrigando os Estados-Membros a adotarem uma estratégia nacional de segurança das redes e dos Sistemas de Informação; o Regulamento Geral de Proteção de Dados[27], que reforça a proteção jurídica dos direitos dos titulares dos dados, exigindo ainda a adoção de novas regras e procedimentos do ponto de vista tecnológico, neste domínio. Também a nível nacional, é patente essa preocupação, que, no encalço das passadas da União Europeia, adotou, ao nível político-estratégico, várias iniciativas legislativas, como as que a seguir se destacam: Estratégia Nacional de Segurança no Ciberespaço[28], que visa aprofundar a segurança das redes de informação, por forma a garantir uma utilização livre, segura e eficiente do ciberespaço, por parte de cidadãos, empresas e entidades públicas e privadas; Regulamento Geral de Proteção de Dados,[29] que define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança de redes e Sistemas de Informação relativos a dados pessoais; a Lei do Cibercrime[30], que proporciona o enquadramento legal dos crimes praticados no âmbito da informática, entre muitas outras.

Quisemos enriquecer o nosso estudo, complementando-o com a abordagem de normas técnicas de organizações internacionais oficialmente reconhecidas, que se debruçam sobre a temática da segurança nos Sistemas de Informação. Destacamos, assim, no painel normativo, três normas que consideramos as mais ajustadas ao contexto do presente trabalho de investigação, ou seja, a norma BS ISO/IEC 17799:2005 – Tecnologias de Informação - Técnicas de Segurança – Código de Prática Para a Gestão da Segurança da Informação; a norma BS ISO/IEC 27001:2005 Sistema de Gestão de Segurança da Informação – Requisitos; e a norma BS 7799-3:2006 – Diretrizes para a Gestão do Risco da Segurança da Informação.

Ao longo do percurso investigatório que fomos traçando, pretendeu-se assimilar os aspetos que se apresentavam com maior pregnância e transversalidade na gestão da segurança dos Sistemas de Informação das organizações contemporâneas. Neste sentido, identificámos cinco aspetos que iam mantendo uma certa consistência nas abordagens realizadas, ou seja, as políticas de segurança, os mecanismos de segurança, os recursos humanos, as auditorias e a resposta aos incidentes críticos. Na posse destas diretrizes, considerámos estar em condições de avançar com a análise da segurança dos Sistemas de

[27] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril.
[28] Resolução de Conselho de Ministros n.º 36/2015, de 12 de junho.
[29] Resolução do Conselho de Ministros n.º 41/2018, de 28 de março.
[30] Lei 109/2009, de 15 de setembro.

Informação na PSP. O passo seguinte consistiu em mergulhar na instituição (PSP) e perceber em que medida estes aspetos eram considerados na gestão da segurança dos Sistemas de Informação da PSP, tendo sempre em linha de vista os objetivos específicos delineados no contexto do presente trabalho. Chegados aqui, optámos por desenvolver um método de investigação exploratório, que consistiu no levantamento das normas internas existentes e na recolha de testemunhos e de entrevistas a especialistas externos e a responsáveis pela gestão da segurança dos Sistemas de Informação na instituição, chegando-se às seguintes conclusões:

Cabe-nos desde logo referir que, de acordo com a Portaria n.º 383/2008, de 29 de maio, a responsabilidade pela Gestão da Segurança dos Sistemas de Informação da PSP se encontra acometida, centralmente, ao Departamento de Sistemas de Informação e Comunicações (DSIC), numa vertente mais tecnológica, e ao Departamento de Informações Policiais (DIP), numa vertente de segurança da informação, ao nível de credenciação e de auditoria dos acessos à informação do SEI. Localmente, ou seja, ao nível das Unidades, são os Núcleos de Sistemas de Informações e Comunicações que atuam sob orientação do DSIC e os Núcleos de Informações Policiais que atuam, por sua vez, sob orientação do DIP. Queremos também realçar que nas unidades, subunidades e serviços da PSP se encontram nomeados os ELI's (Elementos de Ligação Informática),[31] os responsáveis de apoio de 1.ª linha dos utilizadores do Sistemas de Informação da PSP. No que respeita ao apoio ao serviço do SEI, relevam ainda o Serviço de *Helpdesk* SEI[32], local e nacional, e os Oficiais de Ligação SEI (OLSEI)[33], estes últimos adstritos localmente às unidades, estabelecimentos de ensino e a cada um dos departamentos da Direção Nacional da PSP.

Focando agora as medidas de segurança implementadas para proteção do SEI, conseguiu-se identificar algumas que, de forma direta ou indireta, prosseguem esse desiderato. Nomeamos, em primeiro lugar, a existência de diversas normas internas que constituem uma manta de retalhos daquilo que se auspicia ser uma política de segurança de informação na organização. Nota-se uma preocupação generalizada com esta problemática na instituição, no entanto, é tratada de forma algo difusa, não sendo fácil encontrar um fio condutor que aborde, de forma sistémica, todas as vertentes deste assunto na instituição. A criação de políticas de segurança únicas e transversais às organizações é recomendada e, neste aspeto, consideramos que existe algo a repensar na instituição. Outra medida de

[31] Conforme o previsto na NEP n.º DN/GINFOR/99/01, de 22 de agosto de 2003 da DN/PSP.
[32] Conforme NEP n.º DN/ASDDN/GEP/03/01, de 01 de fevereiro de 2011 da DN/PSP.
[33] Idem.

segurança identificada passa pela credenciação dos utilizadores do SEI, através da atribuição de perfis diferenciados em função do princípio da necessidade de conhecer. A atribuição dos perfis obedece a um processo de credenciação, que pode ser feito localmente, no caso de perfis mais genéricos, e centralmente, nos perfis restritos, que são mais específicos. Neste ponto, foram notadas algumas fragilidades, designadamente no processo de descredenciação, reportados aos casos de alteração de situação do efetivo (Faltas/Férias/Transferências/Aposentação, etc.). Cabe-nos aqui invocar a interoperabilidade que o SEI estabelece com o GIVERH (Sistema de Gestão Integrada de Vencimentos e Recursos Humanos), a qual poderia ser rentabilizada, no sentido de adequar o estado do perfil do utilizador à sua situação efetiva. Várias outras medidas de segurança foram identificadas no funcionamento do próprio SEI, tais como: o processo de autenticação; a exigência da justificação de consultas às peças de expediente; a inativação de sessões ao fim de 15 minutos; a advertência de responsabilização Disciplinar/Penal pela utilização abusiva da informação; o registo do histórico de ações nos processos policiais, entre outras. Outra medida de segurança indicada como boa prática é a realização de auditorias de segurança. Neste ponto, temos a referir que foram identificadas algumas iniciativas, na perspetiva tecnológica e na perspetiva dos acessos à informação. Não foi, contudo, identificado um plano consistente e transversal à instituição, que promova a realização de auditorias periódicas ou inopinadas à segurança dos Sistemas de Informação da PSP, algo que consideramos fundamental na deteção de vulnerabilidades para se desencadearem as correspondentes ações corretivas. No que respeita à formação dos recursos humanos, em matéria de segurança dos Sistemas de Informação, constata-se que não existe um plano de ação de formação ou de sensibilização especialmente direcionado para este fim, facto que não contribui para a criação e consolidação de uma cultura de cibersegurança na organização, o que também pode ser apontado como uma vulnerabilidade. Por fim, trazemos à colação uma das medidas identificadas no âmbito da preservação do SEI, que se prende com a ação desenvolvida pela instituição, quando em presença da violação da segurança dos seus ativos informacionais. Antes de mais, convém referir que o SEI tem sido alvo de utilização abusiva por parte de alguns utilizadores da organização. Muitos destes utilizadores encontram-se devidamente credenciados e usam essa condição para aceder indevidamente à informação do SEI, violando, desta forma, o princípio da necessidade de conhecer, e, em alguns casos, o dever profissional de sigilo, dependendo do destino que dão a essa informação. Quando essas situações são detetadas por parte da instituição, é desencadeada a correspondente ação criminal e/ou disciplinar. Neste aspeto, nota-se que apesar dos esforços desenvolvidos, existe

ainda alguma falta de consciencialização do efetivo em matéria de reserva e de sigilo da informação contida no SEI. Ressalva-se que esta situação é potenciada pelas fragilidades de conceção do sistema, que permitem a visualização, a gravação e a impressão de peças de expediente, referentes aos processos policiais ali existentes.

Em termos de Incidentes Críticos no SEI, foram assinaladas falhas nos servidores da aplicação, as quais originam lentidão da operação ou mesmo indisponibilidade do sistema. Embora sejam situações pontuais, com pouca expressividade temporal, quando ocorrem, são bastante notadas pelo efetivo, dado que grande parte das atividades da instituição tem respaldo no SEI. Refira-se que uma da medidas tomadas pelas organizações, para responder adequadamente aos incidentes críticos nos Sistemas de Informação, passa pela criação de um plano de contingência. O plano de contingência que identificámos na PSP, para responder aos incidentes críticos no SEI, consiste em recorrer a formulários, disponíveis no portal da intranet da PSP, para elaboração de peças de expediente, em caso de indisponibilidade de serviço do sistema. Estas peças de expediente são vertidas no SEI, numa fase posterior, quando o mesmo regressar à sua operação normal. Na nossa perspetiva, este plano de contingência não é suficientemente abrangente, na medida em que responde apenas às necessidades de resposta *front office* da PSP. Desta forma, falta ainda tocar no problema de fundo a que os planos de contingência devem responder, que consiste na resposta ao incidente do ponto de vista tecnológico. Significa isto que se pretende, do plano de contingência, uma sequência de ações a desenvolver, para que se restabeleça a operação do sistema, com a maior brevidade possível (*Disaster Recovery*), isto na perspetiva de garantir a continuidade do serviço (*Business Continuity*). Neste contexto, é importante desenvolver competências, através de exercícios simulados, constatando-se que a PSP tem participado em alguns exercícios de cibersegurança, a nível nacional e internacional. Também se notou a ausência de uma equipa CSIRT na PSP. A criação desta equipa já foi proposta, mas não se veio a concretizar. A integração em redes de serviços CSIRT também é recomendável, na medida em que a dinâmica ali estabelecida proporciona a aquisição de *know-how* externo para o seio da instituição.

Acresce, ainda, que, ao longo do presente estudo, foi notória a ausência de um Sistema de Gestão de Segurança de Informação devidamente implementado e consolidado na instituição, de forma a prosseguir a segurança da informação nas vertentes das pessoas, dos processos e das tecnologias, algo fortemente recomendado nas organizações e cuja implementação é imposta na Política de Segurança da Informação do MAI, para os serviços previstos no Decreto-Lei n.º 203/2006, de 27 de Outubro, dos quais a PSP é parte integrante.

Por último, ressalta do presente estudo que a PSP, em termos tecnológicos, se encontra bastante dependente de entidades externas, pois, no que respeita ao desenvolvimento do SEI, o mesmo é realizado pela empresa Accenture. Por outro lado, a segurança deste mesmo sistema, em termos de infraestrutura, também está dependente da COSI da SGMAI, algo que merece reflexão, dadas as limitações e a perda de autonomia da instituição nestas áreas.

Uma das principais limitações para a realização do presente trabalho foi a dificuldade em encontrar pessoas pertencentes à instituição que se predispusessem a colaborar no estudo. Foi ainda sentida dificuldade em angariar a colaboração de organismos externos, cuja atividade conflui com a segurança dos Sistemas de Informação da PSP, como é o caso da RNSI e do COSI, circunstância que constituiu naturalmente uma limitação à investigação. Notou-se, ainda, alguma reserva no tratamento desta temática, visto que este estudo, em última análise, para além da segurança do SEI, pode apontar algumas fragilidades dos serviços envolvidos, algo que, na nossa opinião, não deve ser encarado como um ponto negativo, mas antes como uma oportunidade para identificar as dificuldades e estimular o processo de mudança. O facto de se tratar de uma área hermética, ainda pouco abordada na instituição, constituiu, também, uma limitação.

Concluído o trabalho de investigação, consideramos ter alcançado os objetivos a que nos propusemos inicialmente. No entanto, pensamos que, neste âmbito das tecnologias de informação, e mais propriamente na vertente da segurança dos ativos críticos de informação, existe ainda um longo caminho a percorrer, considerando o recurso intensivo que a PSP faz das tecnologias de informação. Seria interessante fazer um estudo sobre o nível de literacia digital do efetivo, de forma a termos consciência das necessidades de formação nesta área. Outro estudo que poderia ser viável tem que ver com a caraterização do parque informático da PSP, no sentido de se perceber o nível de adequação e de operacionalidade destes equipamentos.

Finalmente, sugerimos a criação de uma linha de investigação de cibersegurança no Instituto Superior de Ciências Policiais e Segurança Interna, em articulação direta com os serviços responsáveis pela manutenção e segurança dos Sistemas de Informação da PSP, visto que a preservação destes sistemas é fundamental para a prossecução das atividades da Instituição.

Lista de Referências

Bibliografia

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). Sage: London.

Accenture / PSP. (2002). Plano Estratégico de Sistemas de Informação. Lisboa: Accenture / Polícia de Segurança Pública.

Accenture / PSP. (2004). Formação EURO 2004 – Guia do Formando. Lisboa: Accenture / Polícia de Segurança Pública.

Accenture / PSP. (2009). Estudo SEI +. Estudo de Utilização e Evolução do SEI. Sistema Estratégico de Formação, Gestão e Controlo Operacional da PSP. Lisboa: Accenture / Polícia de Segurança Pública.

Alter, S. (1999). *A general, yet useful theory of information systems*. Communications of the AIS, 13:1-68.

Bardin, L. (2008). Análise de Conteúdo (4ª ed.).Lisboa: Edições 70.

Cassaro, A. (2011). *Sistemas de informações para tomada de decisões. 4 ed*. São Paulo: Cengage Learning.

Dhillon, G., & Backhous, J. (2000). *Information systems security management in the new millenium*. Communications of the ACM.

Domingues, E. (2015). *Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo.* (tese de mestrado) Lisboa: ISCPSI

Flick, U. (2005). *Métodos qualitativos na investigação científica*. Lisboa: Monitor.

Flick, U., Netz, S., Silveira, T. (2004*). Uma introdução à pesquisa qualitativa*. *2.Ed*. Porto Alegre: Bookman.

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

Gaivéo, J. (2008). *As pessoas nos sistemas de gestão da segurança da informação* (tese de doutoramento). Lisboa, Portugal.

Ghiglione, R., Matalon, B. (2001). *O inquérito: teoria e prática*. Lisboa (Oeiras): Celta Editora, Ld.ª

Khauaja, D. M. R.; Campomar, M. C. (2007). *O sistema de informações no planejamento de marketing: em busca de vantagem competitiva*. Revista de Gestão da tecnologia e sistemas de informação. São Paulo, v. 4, n. 1, p. 23-46, jan./abr. 2007.

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology (2nd ed.*).Thousand Oaks, CA: Sage Publications.

Laudon, K. & Laudon, J. (2012). *Management Information Systems: Managing the Digital Firm, 12th Ed., Upper Saddle River*. New Jersey: Pearson Education Inc.

Lemos, J. (2011). *Sistemas de Informação e Qualidade de Dados: O caso do Sistema Estratégico de Informação, Gestão e Controlo Operacional da Polícia de Segurança Pública*. Lisboa: ISCPSI.

Mamede, H.S. (2014). *Segurança Informática nas Organizações*. Lisboa: FCA – Editora Informática, Ld.ª.

MSI (1997). *Livro Verde para a Sociedade da Informação em Portugal. Missão para a Sociedade da Informação*. Ministério da Ciência e da Tecnologia.

Neves, Artur Castro (2006). *Políticas Públicas e Reformas na Sociedade da Informação.* Porto: Edições Afrontamento.

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

Pinto, C., Rodrigues, J., Santos, A., Melo, L Moreira, M. & Rodrigues R. (2009). *Fundamentos de Gestão.* Lisboa: Editorial Presença.

PSP (2011). *Plano Estratégico de Sistemas de Informação*. Relatório Síntese Revisão de Maio de 2011.

Quivy, R., & Campenhoudt, L. (1998). *Manual de investigação em ciências sociais* (2ª ed.). (J. Marques, M. Mendes, & M. Carvalho, Trads.). Lisboa: Gradiva.

Quivy, R., & Campenhoudt, L. (2005). *Manual de investigação em ciências sociais* (4ª ed.). (J. Marques, M. Mendes, & M. Carvalho, Trads.). Lisboa: Gradiva.

Rascão, J. (2004). *Sistemas de Informação para as organizações: A Informação chave para a Tomada de Decisão*. Lisboa: Edições Sílabo.

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

Sousa, Sérgio (2009). *Tecnologias de Informação. O que são? Para que Servem?* Lisboa: FCA – Editora de Informática, Lda.

Stewart, M. (2009). *Managing Information Risk: A Director's Guide*. Cambridgeshire: IT Governance Publishing.

Toffler, Alvin (1981). T*he Third Wave*. London: Pan Books Ltd.

Tralhão, S. (2008). *Políticas de Segurança dos Sistemas de Informação – Forma e Fundo.* Bragança: IPB – ESTG.

Vacca, John R. (2014). *Managing Information Security – Second Edition*. USA: Syngress.

Zúquete, A (2014). *Segurança em Redes Informáticas. 4.ª Edição Aumentada*. Lisboa: FCA – Editora Informática.

Documentos Oficiais dos Órgãos da União Europeia (UE)

Conselho da Europa (2001). Convenção sobre o Cibercrime.

Diretiva 91/250/CEE do Conselho, de 14 de Maio de 1991, relativa à proteção jurídica dos programas de computador.

Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho.

Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2008, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

JOIN (2013) 1 final (Estratégia da União Europeia para a Cibersegurança: um espaço aberto, seguro e protegido).

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).

Legislação

Lei n.º 7/90, de 20 de Fevereiro – *Diário da República*, 1.ª Série, n.º 43, 670-684. Assembleia da República. (Regulamento Disciplinar da Polícia de Segurança Pública).

Lei n.º 67/98, de 26 de outubro - *Diário da República*, 1.ª Série, n.º 247, 5536-5546. Assembleia da República. (Lei da Proteção de Dados Pessoais).

Lei nº 5/2004, de 10 de Fevereiro – *Diário da República*, 1.ª Serie, n.º 34, 788 – 82, Assembleia da República. (Lei das Comunicações Eletrónicas).

Lei nº 41/2004, de 18 de Agosto – *Diário da República*, 1.ª Série, n.º 194, 5241-5245. Assembleia da República. (Lei da Proteção da Privacidade no Sector das Comunicações Eletrónicas).

Lei n.º 53/2007, de 31 de Agosto – *Diário da República*, 1.ª Série, n.º 168, 6065-6074. Assembleia da República. (Lei Orgânica da PSP).

Lei n.º 32/2008, de 17 de julho. *Diário da República*, 1.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*, 1.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*, 1.º Série, n.º 155, 4031-4037. Assembleia da República. (Regime Jurídico da Segurança no Ciberespaço).

Decreto-Lei nº 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, 1.º Suplemento, n.º 178, 4990-(2) a 4990-(11). Ministério da Ciência e da Tecnologia. (Regime jurídico dos documentos eletrónicos e da assinatura digital).

Decreto-Lei n.º 203/2006, 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*, 1.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*, 1.ª Série, n.º 204, 9054-9086. Ministério da Administração Interna. (Estatuto do Pessoal Policial da Polícia de Segurança Pública).

Decreto Regulamentar n.º5/95, de 31 de janeiro – *Diário da República*, Série I-B, n.º 26, 582-584. Ministério da Administração Interna. (Base da Dados Pessoais da Polícia de Segurança Pública).

A Resolução de Conselho de Ministros n.º 50/88, de 8 de setembro – *Diário da República*, 1.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*, 1.ª Série, 1.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*, 1.ª Série, n.º 179, 6354-6378. Assembleia da República. (Aprova a Convenção sobre o Cibercrime).

Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho – *Diário da República*, 1.ª Série, n.º 113, 3738-3742. Presidência do Conselho de Ministros. (Aprova a Estratégia Nacional de Segurança do Ciberespaço).

Resolução do Conselho de Ministros n.º 41/2018, de 28 março – *Diário da República*, 1.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).

Portaria n.º 383/2008, de 29 de Maio – *Diário da República*, 1.ª Série, n.º 103, 3015-3020. Ministérios das Finanças e da Administração Pública e da Administração Interna. (Estrutura nuclear da Direcção Nacional da Polícia de Segurança Pública).

Despacho n.º 19935/2008, de 17 de julho – *Diário da República*, 2.ª Série, n.º 144, 33398. Direção Nacional da Polícia de Segurança Pública – Ministério da Administração Interna. (Unidades orgânicas flexíveis da unidade Direcção Nacional da PSP).

Normas e Documentação Interna da PSP

Despacho n.º 20/GDN/2009, de 14 de dezembro (Unidades territoriais da Polícia de Segurança Publica (PSP): Organização e competências).

Norma de Execução Permanente n.º DN/GINFOR/99/01, de 22 de agosto de 2003 (ELI – Elementos de Ligação Informática)

Norma de Execução Permanente n.º DN/ASDDN/GEP/03/01, de 1 de fevereiro de 2011 (Sistema Estratégico de Informação (SEI)).

Regulamento da Formação do Sistema Estratégico de Informação (SEI) de 01 de Fevereiro de 2011.

Código de Procedimento n.º 02/DIP/2018, de 10 de julho. (Bases de dados do DIP – Atribuição de Perfis)

Visão Global de Operacionalização da Estratégia para as TIC na PSP 2013-2016.

Portefólio de Formação Policial 2018 (DF/DNPSP).

Norma de Execução Permanente N° CMD/NINFOR/01/06, de 31 de janeiro de 2006, do COMETPOR (uso, administração e segurança das estruturas Informáticas).

Manual de Procedimentos do COMETPOR. Versão 4.0. (2015).

Manual de Qualidade do COMETPOR Versão 1.0 (2015).

Webgrafia

http://www.apdsi.pt/

http://www.cert.pt/

http://www.cncs.gov.pt/cert-pt/

http://www.enisa.europa.eu/

http://www.gns.gov.pt/

http://www.gns.gov.pt/new-ciberseguranca.aspx

http://www.pgdlisboa.pt/

https://bestpractical.com/

https://dre.pt/

https://intranet.mai.pt/Pages/Mai_Politica1.aspx

https://tic.gov.pt/documents/2018/CTIC_TIC2020_PS-MAI.pdf

https://www.27001.pt/index.html

https://www.accenture.com/us-en

https://www.apcergroup.com/pt/certificacao/pesquisa-de-normas/187/iso-iec-27001

https://www.bsigroup.com/

https://www.cepol.europa.eu/pt

https://www.csirt.rnsi.mai.gov.pt/

https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

https://www.facebook.com

https://www.fbi.gov/investigate/cyber

https://www.iec.ch/

https://www.iso.org/home.html

https://www.iso.org/isoiec-27001-information-security.html

https://www.iso.org/standard/39612.html

https://www.redecsirt.pt/

https://www.sans.org/

https://www.sans.org/media/score/checklists/ISO-17799-2005.pdf

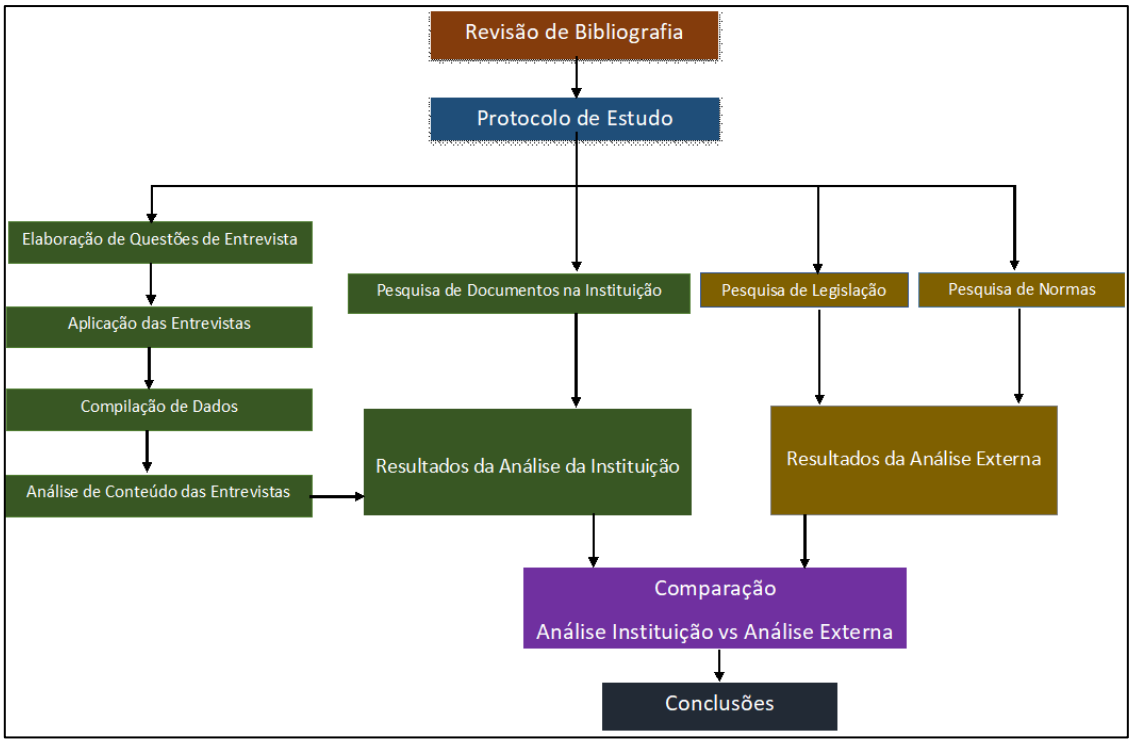
http://www.seg-social.pt/documents/10152/15483073/Politica_seguranca_informacao_II.pdf

https://www.sg.mai.gov.pt/Paginas/default.aspx

https://www.youtube.com/

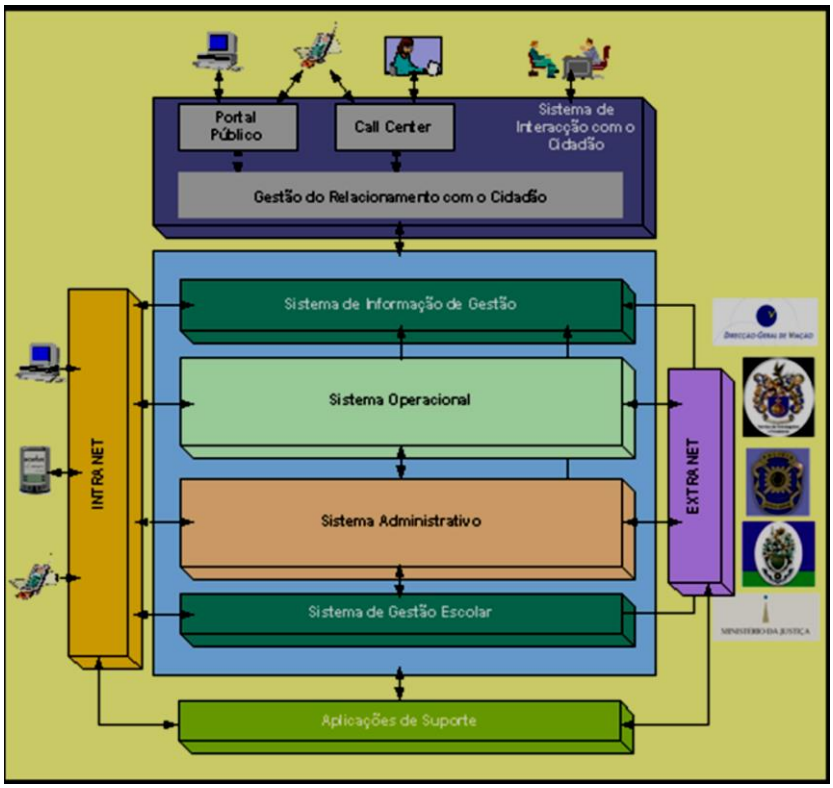
Documentação Anexa

Anexo I – Método de Investigação



Fonte: Elaborado pelo autor.

Anexo II – Modelo Concetual Proposto no Plano Estratégico de Sistemas de Informação da PSP (PESI)

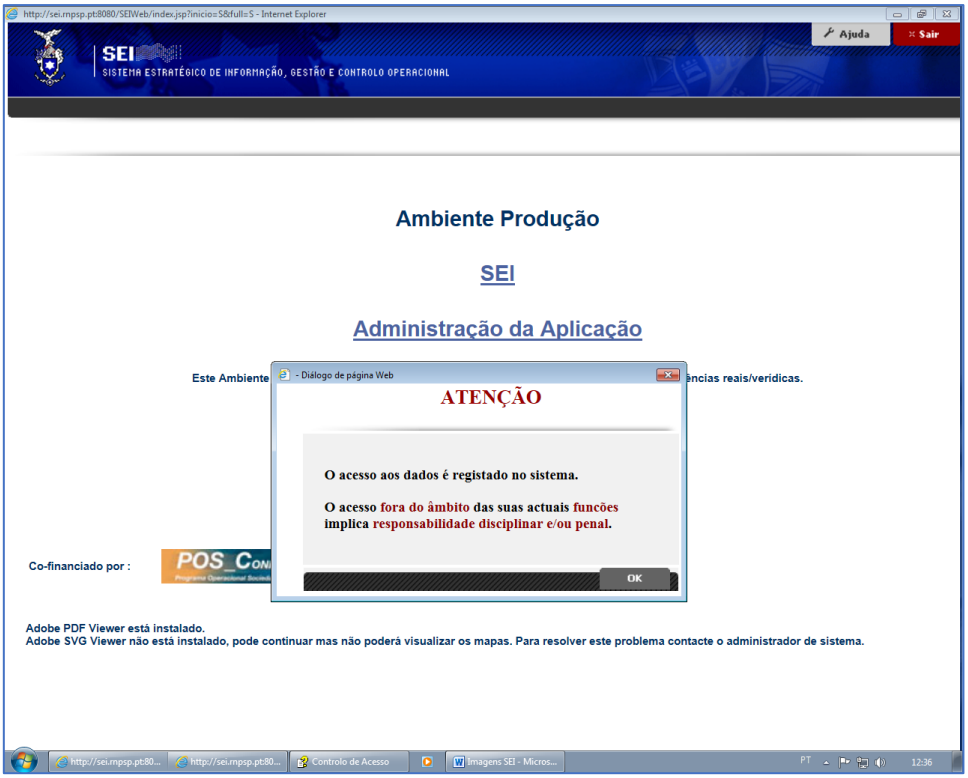


Fonte: Accenture/PSP, 2002, Página 355.

Fonte: PSP – Apresentação do SEI (Em 30 de Novembro de 2011).

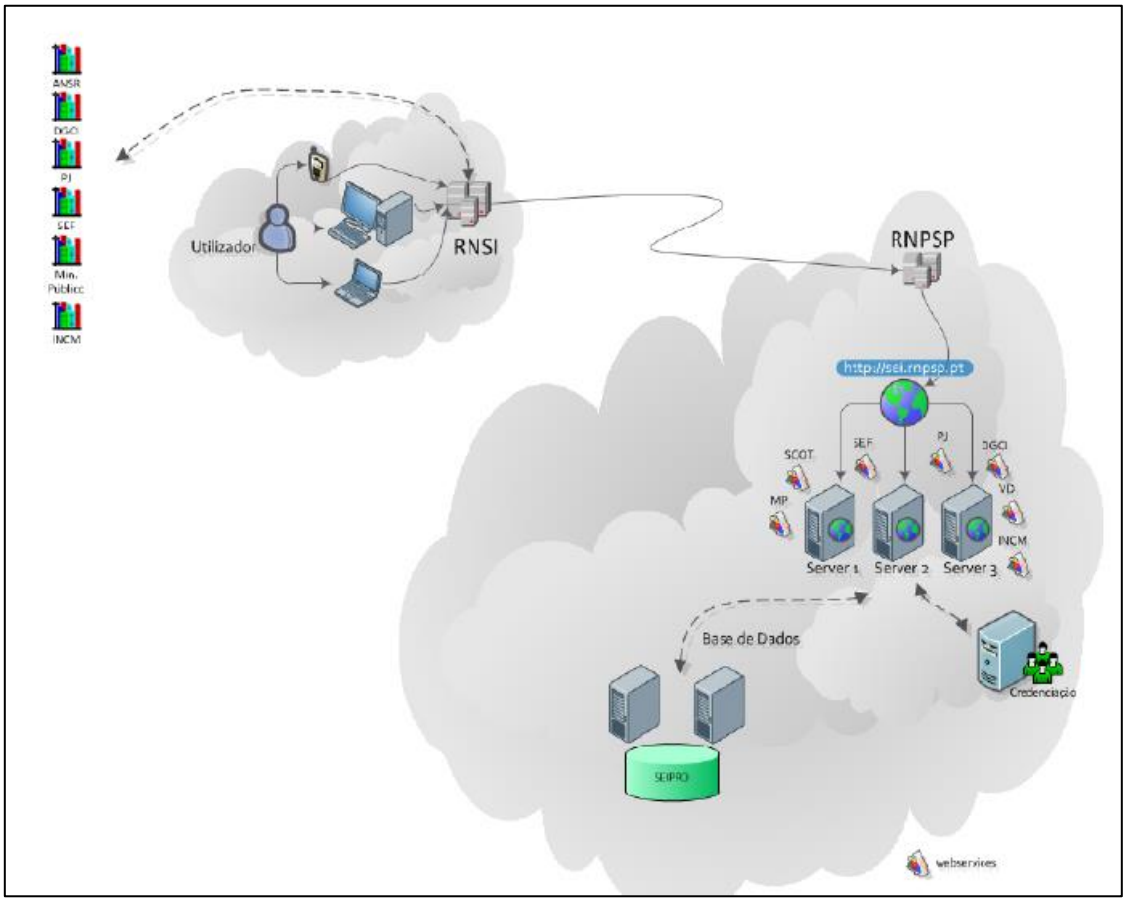
Anexo III – Interface do Sistema Estratégico de Informação, Gestão e Controlo Operacional

Fonte: Print screen da interface do SEI no browser Internet Explorer.



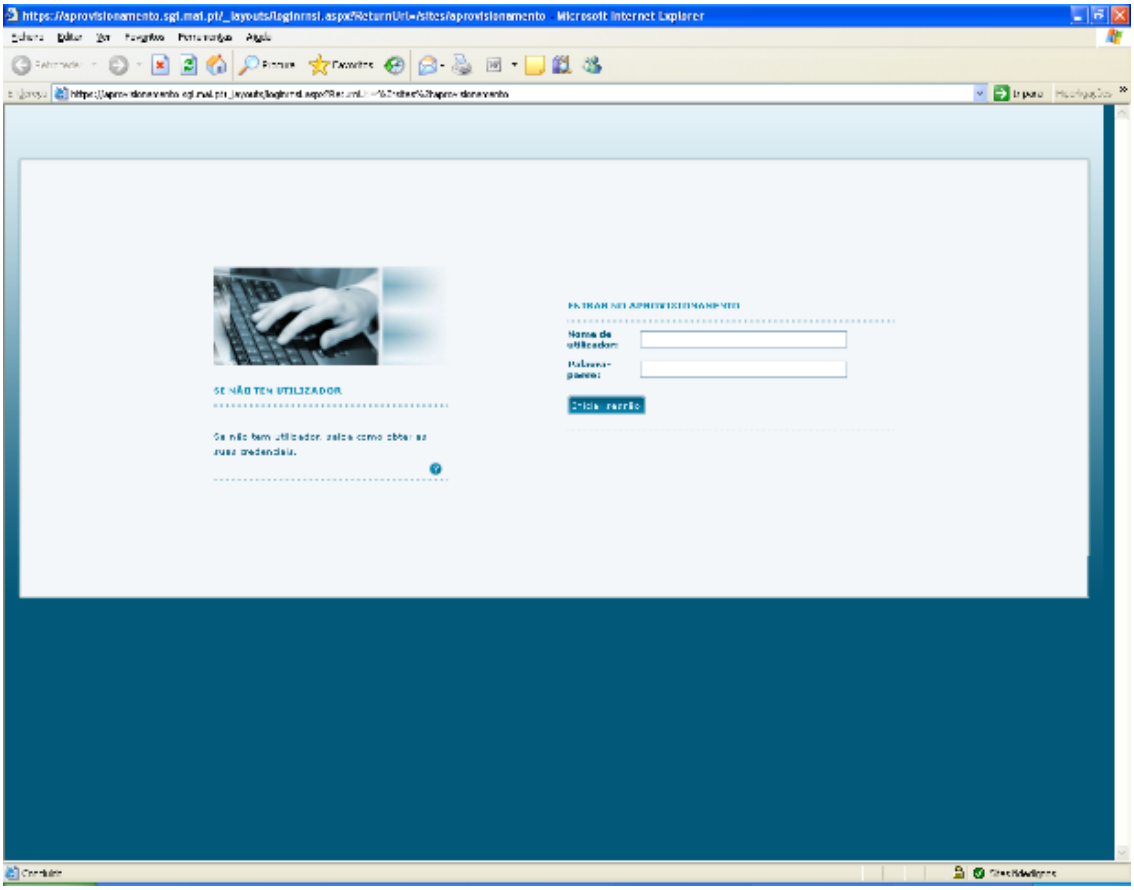
Fonte: Print screen da interface do SEI no browser Internet Explorer.

Anexo IV – Esquema da Integração do SEI na RNSI



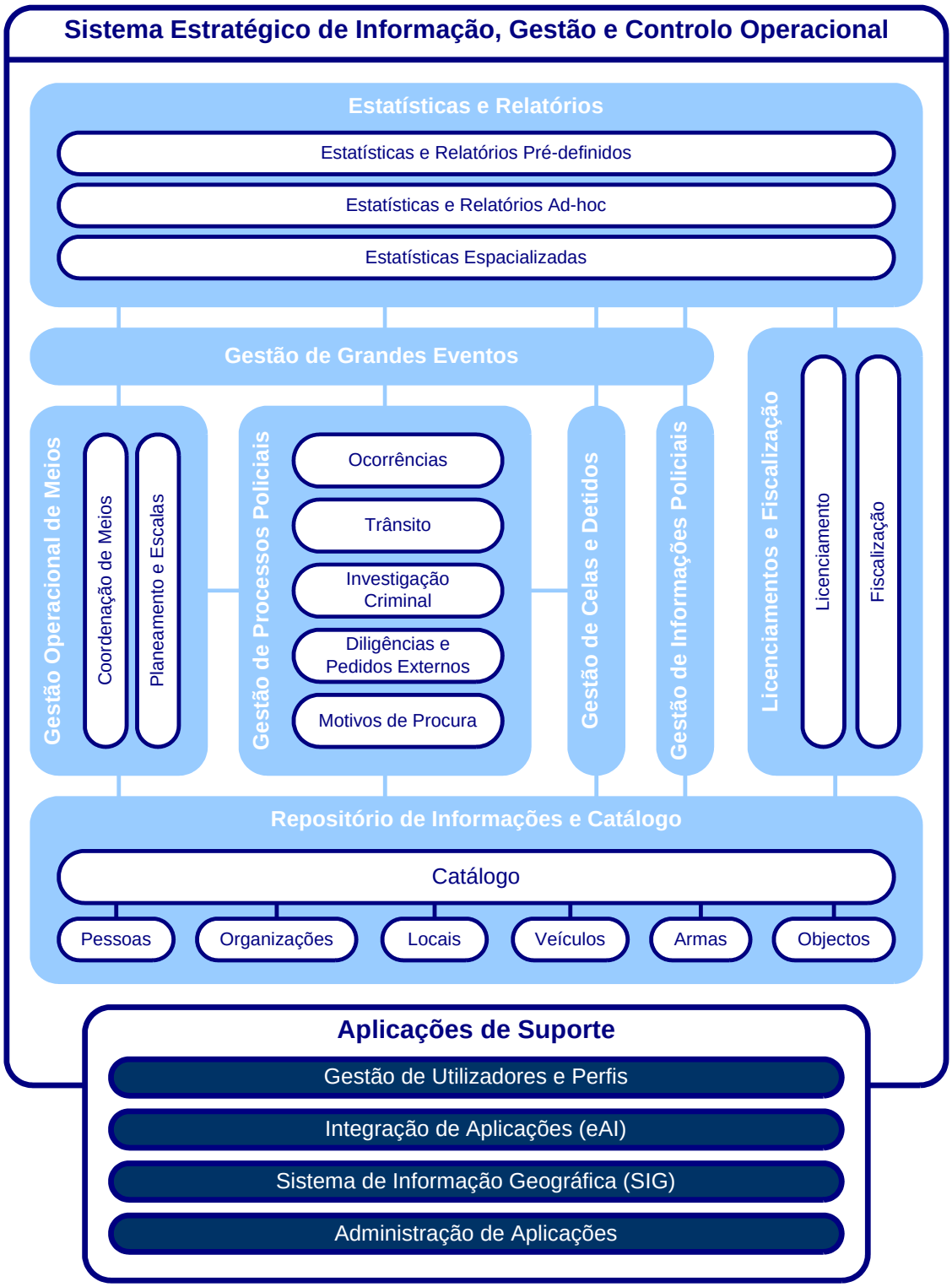
Fonte: Lemos, J., 2011, página 89.

Anexo V – Interface do Sistema de Gestão de Identidades da RNSI (SGI)



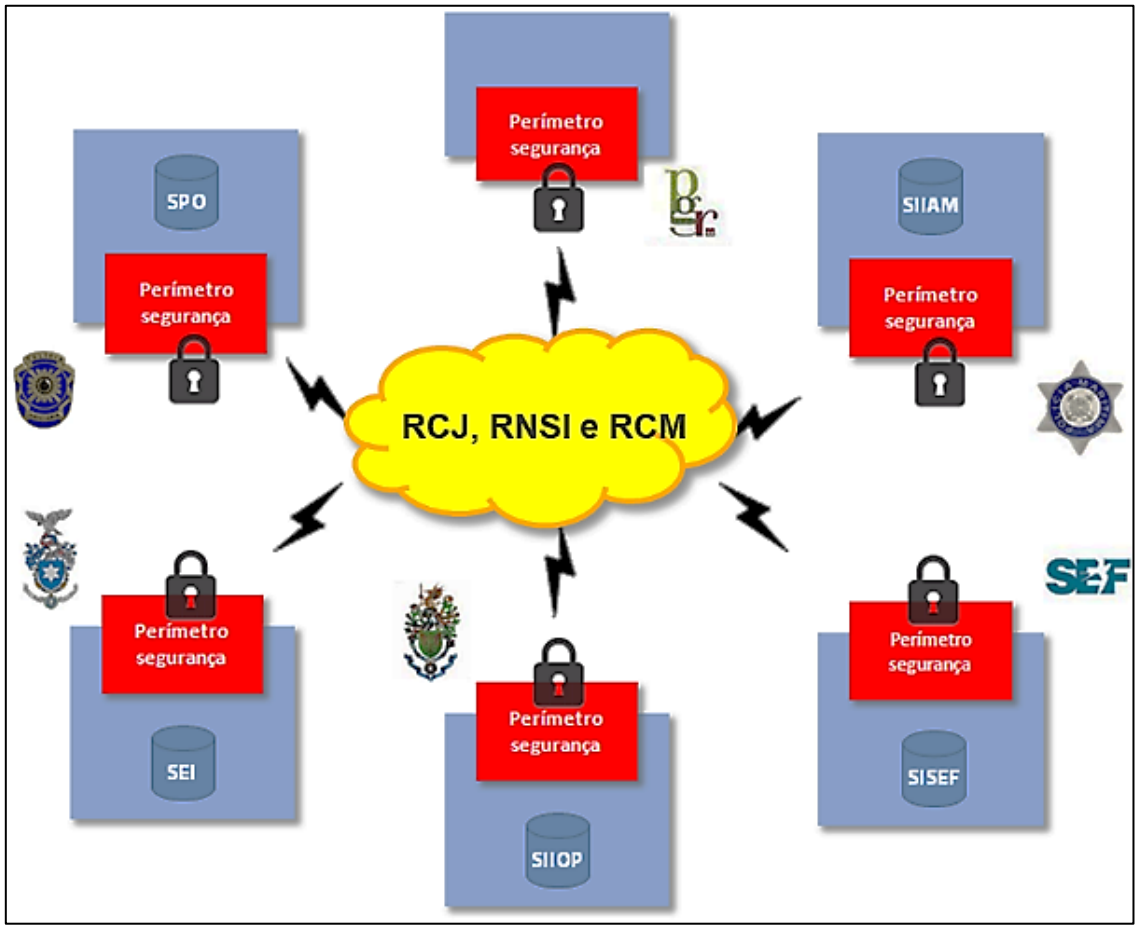
Fonte: Print screen da interface do SGI no browser Internet Explorer.

Anexo VI – Módulos Aplicacionais do SEI



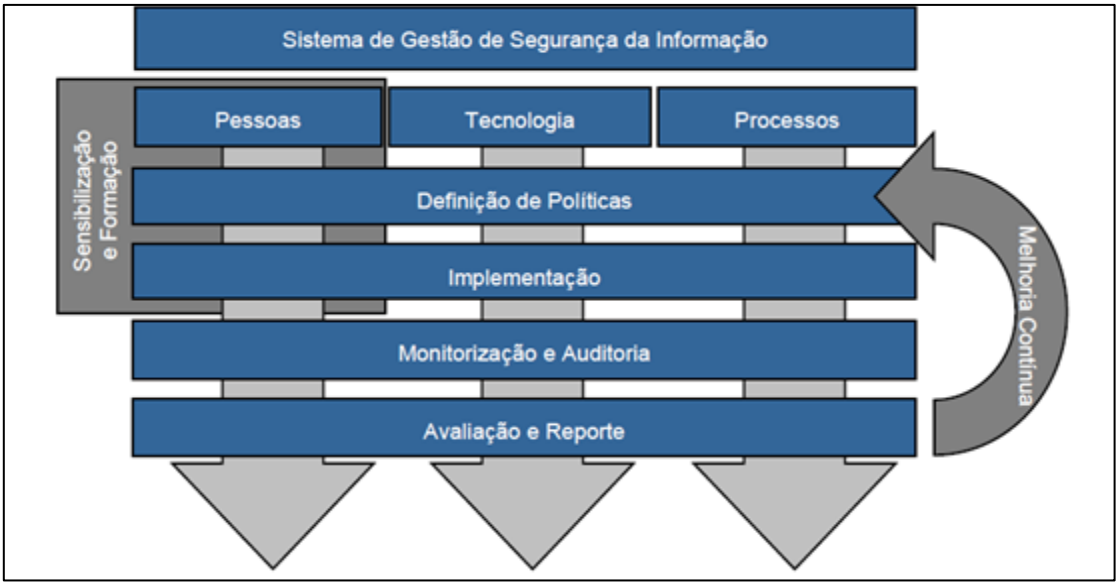
Fonte: Accenture/PSP, 2004, Página SEI 8.

Anexo VII - Modelo Concetual da PIIC



Fonte: PIIC - "Apresentação do resultado do desenvolvimento da PIIC- ISCPSI". (Em 26 de março de 2013)

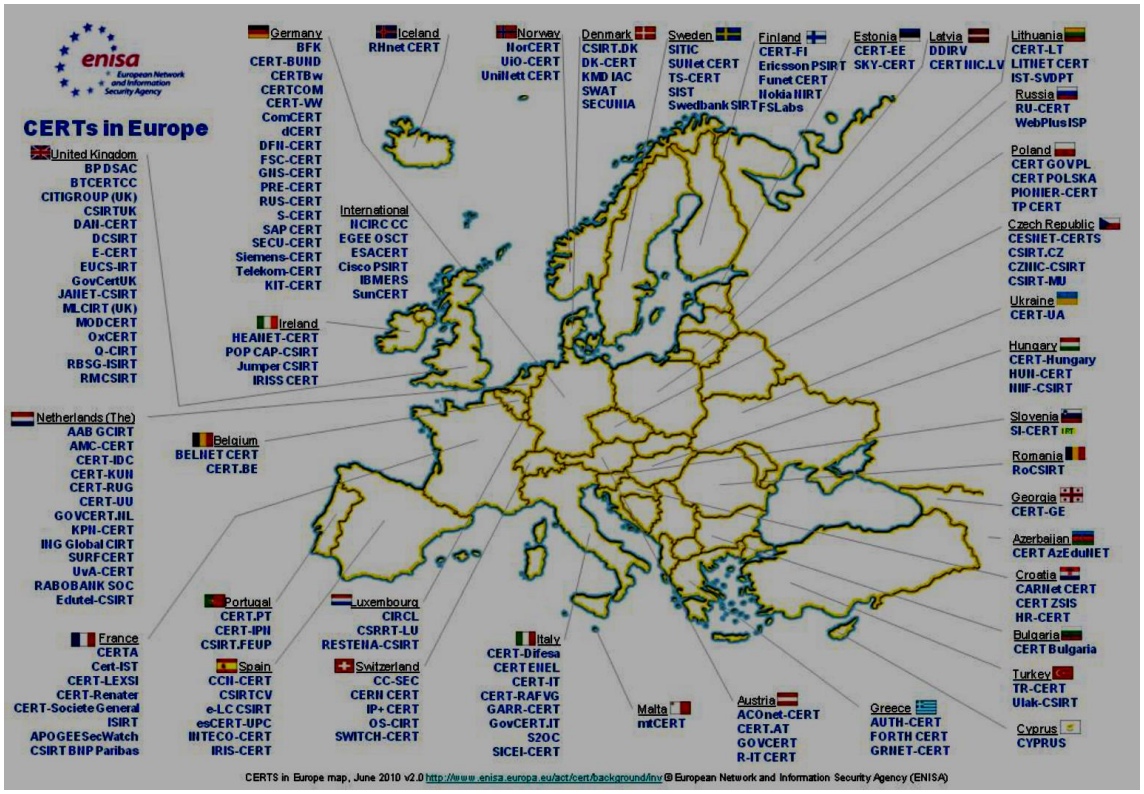
Anexo VIII – Sistema de Gestão de Segurança da Informação (SGSI)



Fonte: II I.P., 2017, página 7. [34]
(Adaptado de *Information Security Framework - Forrester Research, Inc.*).

[34] Disponível em:
<http://www.seg-social.pt/documents/10152/15483073/Politica_seguranca_informacao_II.pdf>
Acesso em Dezembro de 2018.

Anexo IX - Rede CERT na Europa



Fonte: ENISA - Página Web da Enisa[35]

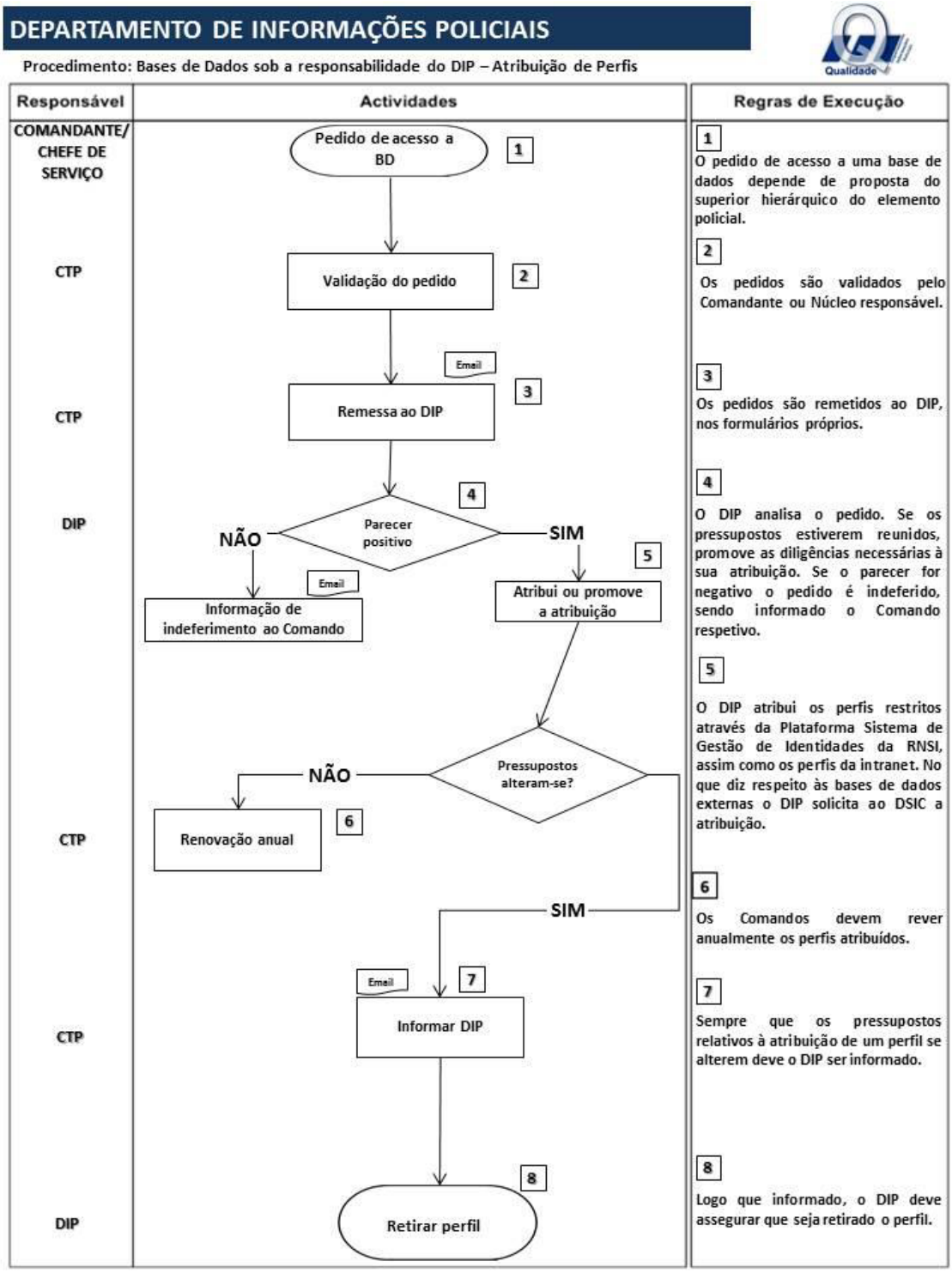
[35] Disponível em: <https://www.enisa.europa.eu/news/enisa-news/copy_of_new-from-enisa-2013-updated-map-inventory-of-europe2019s-201cdigital-fire-brigades201d-with-173-computer-emergency-response-teams-listed> Acesso em Janeiro de 2019.

Anexo X - Tabelas de Perfis do SEI

Perfis Restritos (de atribuição Central)	***Perfis Gerais (de atribuição Local)***
C9-Gestor_Grande_Evento_Nacional	B1-Policia_Base
C10-Gestor_Acumulacao_Despacho	B2-Supervisor_Operacional-Graduado_Servico
I1-Director_Informacoes_DN	B3-Escalador
I2-Analista_Informacoes	B4-Gestor_Pedido_Externo
I4-Credenciador_Elementos_Policiais	B5-Elemento_Registo_Pedidos_Externos
I5-Ver_Fonte_Informacoes	B6-Gestor_Queixa_Electronica
I6-Receber_Aviso_Inactivacao_Informacoes	B7-Registo_Viaturas_Entidade_Externa
I7-Navegar_Catalogo_Restrito	B8-Pesquisa_Rapida_Viaturas
I8-SICOP_Entidades_Externas	B9-Pesquisa_Rapida_Pessoas
I9-Supervisor_Informacao_Oculta	C1-Comandante_Comando-Div-Sec
O1-Director_DEPOP_DN	C2-Oficial_Servico_Comando
O2-Elemento_Operacoes_DN	C3-Oficial_Servico_Div-Sec
A1-Administrador_SEI	C4-Comandante_Esquadra
A2-Coordenador_Informacao_RI	C5-Aprovador_Processo_Crime
A3-Gestor_Unidades_Policiais	C6-Aprovador_Processo_CO
A4-Gestor_Tabelas_Gerais	C7-Aprovador_Processo_Diverso
A5-Gerir_Tabelas_Infraccoes	C8-Aprovador_Pedido_Externo
A6-Gestor_Codigos_DAE	D1-Gestor_Celas_Detidos
	D2-Elemento_Registo_Inspeccoes
	M1-Operador_Incidente
	M2-Supervisor_Incidente
	O5-Oficial_Operacoes
	V1-Investigador
	V2-Gestor_Investigacao
	T0-Transito_Base
	T1-Comandante_Divisao-Seccao_Transito
	T2-Comandante_Esquadra_Transito
	T3-Gestor_Processo_CO_Transito
	T4-Gestor_Acidentes_Transito
	T5-Gestor_Parques
	T7-Aprovador_Processo_CO_Transito
	T8-Aprovador_Acidentes_Transito
	T10-Gestor_Pedido_Emissao_Certidao_Acidente
	Perfis Restritos (de atribuição Central)
	C9-Gestor_Grande_Evento_Nacional
	C10-Gestor_Acumulacao_Despacho
	I1-Director_Informacoes_DN
	I2-Analista_Informacoes
	I4-Credenciador_Elementos_Policiais
	I5-Ver_Fonte_Informacoes
	I6-Receber_Aviso_Inactivacao_Informacoes
	I7-Navegar_Catalogo_Restrito
	I8-SICOP_Entidades_Externas
	I9-Supervisor_Informacao_Oculta
	O1-Director_DEPOP_DN
	O2-Elemento_Operacoes_DN
	A1-Administrador_SEI
	A2-Coordenador_Informacao_RI
	A3-Gestor_Unidades_Policiais
	A4-Gestor_Tabelas_Gerais
	A5-Gerir_Tabelas_Infraccoes
	A6-Gestor_Codigos_DAE

Fonte: PSP - 'PSP_SEI_PERFIS_Versão 2011-04-13'

Anexo XI - Fluxograma de Atribuição de Perfis



Fonte: PSP - Código de Procedimento n.º 02/DIP/2018, de 10 de julho (Anexo A).

Apêndices

Apêndice A - Entrevista a Oficial da PSP (Funções de Comando Operacional)

A presente entrevista insere-se no âmbito da dissertação de mestrado para obtenção do grau de mestre do Curso de Mestrado Integrado em Ciências Policiais (CMICP), ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório desta dissertação é "A Segurança dos Sistemas de Informação da Polícia de Segurança Pública (PSP): O Sistema Estratégico de Informação (SEI)", sendo orientador da mesma, o Senhor Superintendente Sérgio Felgueiras.

Pretende-se com esta dissertação estudar a gestão da segurança dos Sistemas de Informação da PSP e, em concreto, analisar como é que a PSP protege o seu Sistema Estratégico de Informação, evidenciando-se a necessidade de securitização permanente deste sistema face às ameaças e riscos que impendem sobre o mesmo, considerando a importância que este sistema representa no plano das atividades, operacional e administrativa, da PSP.

Local: - - -

Data: - - -

Cargo/Posto: - - -

Guião

1. Considera que o SEI é um ativo crítico de informação para a PSP?
2. Quais entende serem os maiores contributos do SEI para as várias atividades desenvolvidas pela PSP?
3. Que aspetos de segurança de informação foram tidos em consideração na conceção do SEI e, nas sucessivas alterações que foram realizas neste sistema?
4. Considera que a disponibilidade, a integridade e a confidencialidade da informação são suficientemente acauteladas no SEI?
5. Quais são as principais ameaças e riscos que atualmente impendem sobre os Sistemas de Informação da PSP em geral, e sobre o SEI em particular?
6. Na sua opinião, quais são as maiores vulnerabilidades que o SEI apresenta para a segurança da informação?
7. Que medidas de contrainteligência são tomadas pela PSP em relação aos seus Sistemas de Informação, de forma genérica, e do SEI em particular?

8. A gestão da segurança da informação nas organizações compreende três vertentes: as Pessoas, os Processos e as Tecnologias. Considera que a PSP abrange estas três vertentes da gestão da segurança de informação no SEI de forma eficaz?
9. A PSP tem algum Sistema de Gestão de Segurança de Informação devidamente implementado e consolidado?
10. Considera que os Sistemas de Informação da PSP podem constituir um alvo elegível para a concretização de ciberataques?
11. Quais seriam os principais impactos causados por uma eventual disrupção no funcionamento do SEI?

Apêndice B - Entrevista a Oficial da PSP (Funções de Chefia - NSIC)

A presente entrevista insere-se no âmbito da dissertação de mestrado para obtenção do grau de mestre do Curso de Mestrado Integrado em Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI). O título provisório desta dissertação é "A Segurança dos Sistemas de Informação da Polícia de Segurança Pública (PSP): O Sistema Estratégico de Informação (SEI)", sendo orientador da mesma, o Senhor Superintendente Sérgio Felgueiras.

Pretende-se, com esta dissertação, estudar a gestão da Segurança dos Sistemas de Informação da PSP e, em concreto, analisar os meios de que a PSP dispõe para proteger o seu Sistema Estratégico de Informação. Evidencia-se, assim, a necessidade de securitização permanente deste sistema, face às ameaças e aos riscos que impendem sobre o mesmo, considerando a importância que este sistema representa no plano das atividades, operacional e administrativa, da PSP.

Local: - - -

Data: - - -

Cargo/Posto: - - -

Guião

Grupo I - Ameaças, Riscos e Vulnerabilidades

1. Quais são as principais ameaças e riscos para o SEI e para as suas infraestruturas tecnológicas?
2. Considera que a interoperabilidade do SEI com outros Sistemas de Informação pode constituir uma vulnerabilidade para a segurança da informação?
3. O acesso ao SEI, através de equipamentos/dispositivos móveis, pode representar uma vulnerabilidade para a segurança da informação?
4. O NSIC do (Comando) identificou algum tipo de vulnerabilidade de segurança que afetasse a normal operação do SEI, designadamente, no que respeita à integridade, disponibilidade e confidencialidade da informação ali contida?
5. De que forma a PSP identifica e mitiga as vulnerabilidades de segurança dos seus Sistemas de Informação, em geral, e do SEI, em particular?

Grupo II - Gestão da Segurança da Informação

6. Na sua opinião, existe na PSP um Sistema de Gestão da Segurança da Informação (SGSI) devidamente consolidado que trate a segurança da informação nas vertentes dos Processos, das Pessoas e das Tecnologias?

7. As políticas de segurança definem um foco de segurança, estabelecendo requisitos adequados a atingir um determinado resultado. Na PSP, que políticas e procedimentos de segurança existem, que visem, de forma direta ou indireta, a proteção do SEI?
8. Os mecanismos de segurança permitem a operacionalização das políticas de segurança. Que mecanismos de segurança foram implementados, pelo NSIC do (Comando), para garantir a proteção do SEI e das suas infraestruturas tecnológicas?
9. A formação e a sensibilização dos recursos humanos constituem pontos-chave na segurança dos Sistemas de Informação. Existe, no (Comando), algum plano de formação/sensibilização que aborde aspetos de segurança da informação em plataformas eletrónicas de informação da PSP, como é o caso do SEI?
10. O NSIC do (Comando) realiza auditorias (programadas / inopinadas) à segurança do SEI ou das suas infraestruturas tecnológicas?
    a. Em caso afirmativo, de que tipo de auditorias se tratam?

Grupo III - Incidentes Críticos

11. Considerando que um incidente é um evento que interrompe o procedimento de normal operação do sistema, gerando um determinado nível de crise, quais são os principais incidentes que têm perturbado o normal funcionamento do SEI, nos vários serviços e subunidades do (Comando)?
12. Que ações são desenvolvidas, pelo NSIC do (Comando), antes, durante e depois (Prevenção, Deteção e Reação) da ocorrência de incidentes de segurança nos Sistemas de Informação da PSP e nas respetivas infraestruturas tecnológicas?
13. A norma ISO / IEC 27001 exige a adoção de um processo de gestão de incidentes, para que os eventos de segurança da informação sejam documentados e relatados através dos canais de gestão adequados, o mais rapidamente possível, exigindo, ainda, a sua comunicação às autoridades competentes. O NSIC documenta e reporta os eventos de segurança nos Sistemas de Informação da PSP e nas respetivas infraestruturas tecnológicas?
    a. Em caso afirmativo, a quem é feito o reporte destes incidentes e qual é a tramitação subsequente deste processo?

Apêndice C - Entrevista a Oficial da PSP - (Funções de Chefia - NIP)

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

O título provisório desta dissertação é "A Segurança dos Sistemas de Informação da Polícia de Segurança Pública (PSP): O Sistema Estratégico de Informação (SEI)", sendo orientador da mesma o Sr. Superintendente, Professor Doutor, Sérgio Felgueiras.

Pretende-se com esta dissertação estudar a gestão da Segurança dos Sistemas de Informação da PSP, e em concreto, analisar como é que a PSP protege o seu Sistema Estratégico de Informação, evidenciando-se também a necessidade de securitização permanente deste sistema face à importância que o mesmo representa no plano das atividades, operacional e administrativa, da PSP.

Local: - - -

Data: - - -

Cargo/Posto: - - -

Guião

1. Considera que o SEI é um ativo crítico de informação da PSP?
2. Quais entende serem os maiores contributos do SEI nas várias atividades desenvolvidas pela PSP?
3. Quais seriam os principais impactos causados por uma eventual disrupção no funcionamento do SEI?
4. Que tipo de matérias são armazenadas e tratadas no SEI?
5. O SEI é uma das ferramentas utilizadas na produção de Inteligência Policial? Em caso afirmativo, em que medida é que tal acontece?
6. Quais são os requisitos que um sistema de Informação deve atender para que possa comportar matéria classificada?
7. Considera que a disponibilidade, a integridade e a confidencialidade da informação é suficientemente acautelada no SEI?
8. Que medidas de contrainteligência são tomadas pela PSP em relação aos seus Sistemas de Informação de forma genérica e, ao SEI em particular?
9. Na sua opinião, quais são as maiores vulnerabilidades que o SEI apresenta para a segurança da informação?

10. Pensa que o SEI apresenta ainda alguma margem de progressão no seu atual estado de desenvolvimento?
    a. Em caso afirmativo, quais os sentidos em que tal poderia vir a ocorrer?
11. Quais considera serem as principais ameaças e riscos que impendem sobre o SEI?
12. A quem são reportados os problemas de funcionamento do SEI?
13. O SEI permite fazer o rastreamento das ações realizadas pelos seus utilizadores no sistema? Em caso afirmativo, quem executa esse rastreio e com que finalidade?
14. A gestão da segurança da informação nas organizações compreende três vertentes: as Pessoas, os Processos e as Tecnologias. Considera que a PSP abrange estas três vertentes da gestão da segurança de informação no SEI de forma eficaz?
    a. Quais são os serviços organicamente responsáveis pela sua operacionalização?

Apêndice D - Entrevista a Técnico Superior da PSP (Funções de Chefia - NDD)

A presente entrevista insere-se no âmbito da dissertação de mestrado para obtenção do grau de mestre do Curso de Mestrado Integrado em Ciências Policiais (CMICP), ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI). O título provisório desta dissertação é "A Segurança dos Sistemas de Informação da Polícia de Segurança Pública (PSP): O Sistema Estratégico de Informação (SEI)", sendo orientador da mesma o Senhor Superintendente Sérgio Felgueiras.

Pretende-se com esta dissertação estudar a gestão da segurança dos Sistemas de Informação da PSP e, em concreto, analisar o modo como a PSP protege o seu Sistema Estratégico de Informação, evidenciando-se a necessidade de securitização permanente deste sistema face às ameaças e riscos que impendem sobre o mesmo, considerando a importância que este sistema representa no plano das atividades, operacional e administrativa, da PSP.

Local: - - -

Data: - - -

Cargo/Posto: - - -

Guião

1. Quais são os Sistemas de Informação (SI) da PSP sobre os quais incide maior número de infrações disciplinares?
2. Que infrações disciplinares são mais frequentes na utilização dos Sistemas de Informação da PSP?
3. O atual quadro legislativo e regulamentar responde adequadamente às necessidades da instrução de processos disciplinaresSSaa11 decorrentes da utilização indevida dos Sistemas Informação da PSP?.
4. Como é que este tipo de infração disciplinar chega ao conhecimento do Núcleo de Deontologia e Disciplina (NDD) e qual a tramitação subsequente?
5. Que meios de prova e de obtenção de prova são admissíveis na instrução de processos disciplinares que envolvam os Sistemas de Informação da PSP?
6. O NDD dispõe de peritos na instrução de processos disciplinares em que sejam visados os Sistemas de Informação da PSP?
7. Quais são as consequências possíveis para um infrator que viole ou utilize abusivamente os Sistemas de Informação da PSP?

Apêndice E - Entrevista a Especialista em Cibersegurança (CNCS)

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

O título provisório desta dissertação é "A Segurança dos Sistemas de Informação da Polícia de Segurança Pública (PSP): O Sistema Estratégico de Informação (SEI)", sendo orientador da mesma, o Senhor Superintendente Sérgio Felgueiras.

Pretende-se com esta dissertação estudar a gestão da segurança dos Sistemas de Informação da PSP e, em concreto, analisar como é que a PSP protege o seu Sistema Estratégico de Informação, evidenciando-se a necessidade de securitização permanente deste sistema face as ameaças e riscos que impendem sobre o mesmo, considerando a importância que este sistema representa no plano das atividades, operacional e administrativa, da PSP.

Local: - - -

Data: - - -

Cargo/Posto: - - -

Guião

1. Como carateriza o estado da cibersegurança em Portugal?
2. Que tipo de ações são desenvolvidas pelo CNCS no panorama da cibersegurança nacional?
3. Quais as principais vulnerabilidades identificadas pelo CNCS no contexto cibersegurança nacional?
4. Na sua opinião, quais considera serem as principais ameaças para a segurança dos Sistemas de Informação de um serviço da administração pública, como é o caso da Polícia de Segurança Pública?
5. Considera que os Sistemas de Informação da PSP podem constituir um alvo elegível para a concretização de ciberataques?
6. Quais as possíveis consequências da concretização de um ciberataque nos Sistemas de Informação da PSP?
7. Quais são os constrangimentos de não existir um Sistema de Gestão de Segurança de Informação numa organização?

8. Na sua opinião, quais considera serem os principais eixos de intervenção na segurança dos Sistemas de Informação de uma organização?
9. Qual considera ser a abordagem mais apropriada para a segurança dos Sistemas de Informação de uma organização? A Pró-ativa ou a reativa?
10. Quais as principais ações a desencadear por parte de uma organização que seja alvo de um ciberataque?
11. Que formas de cooperação se encontram disponíveis por parte desse Centro na promoção da segurança dos Sistemas de Informação da PSP?

Apêndice F - Entrevista a Especialista Cibersegurança (ISEP)

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

O título provisório desta dissertação é "A Segurança dos Sistemas de Informação da Polícia de Segurança Pública (PSP): O Sistema Estratégico de Informação (SEI)", sendo orientador da mesma, o Sr. Superintendente Sérgio Felgueiras.

Pretende-se com esta dissertação estudar a gestão da segurança dos Sistemas de Informação da PSP e, em concreto, analisar como é que a PSP protege o seu Sistema Estratégico de Informação, evidenciando-se a necessidade de securitização permanente deste sistema face as ameaças e riscos que impendem sobre o mesmo, considerando a importância deste sistema no plano das atividades, operacional e administrativa, da PSP.

Local: - - -

Data: - - -

Cargo/Posto: - - -

Guião

Grupo I – Ameaças, Vulnerabilidades e Riscos

1. Quais considera serem, na atualidade, as principais ameaças e riscos para a segurança dos Sistemas de Informação das organizações?
2. Na sua opinião, quais são as principais vulnerabilidades dos Sistemas de Informação das organizações?
    a. Como é que estas vulnerabilidades podem ser detetadas?
3. Considera que os Sistemas de Informação da PSP podem constituir um alvo elegível para a concretização de ciberataques?
4. Quais as possíveis consequências decorrentes da concretização de um ciberataque nos Sistemas de Informação da PSP?

Grupo II – Gestão da Segurança dos SI

5. Quais são as normas de referência para a implementação de um Sistema de Gestão da Segurança dos Sistemas de Informação numa dada organização?
6. Quais são os constrangimentos de não existir um Sistema de Gestão de Segurança de Informação numa dada organização?

7. Quais considera serem os principais eixos de intervenção na gestão da segurança dos Sistemas de Informação de uma organização?
8. O processo de gestão da segurança dos Sistemas de Informação numa organização deve assumir um carater estático ou evolutivo? Porquê?

Grupo III – Pessoas, Políticas, Mecanismos e Auditorias de segurança

9. No seu entender, as políticas de segurança dos Sistemas de Informação devem ser únicas e transversais a toda a organização ou podem ser múltiplas e fragmentadas consoante o fim visado e a estrutura organizacional?
10. Que tipos de mecanismos de segurança são mais eficazes na promoção da segurança dos Sistemas de Informação de uma organização?
11. Qual a importância da realização de auditorias de segurança aos Sistemas de Informação de uma dada organização?
12. Considera que a sensibilização e formação dos recursos humanos em aspetos de segurança dos Sistemas de Informação podem contribuir para o reforço da Segurança da Informação da organização?

Grupo IV – Incidentes Críticos

13. Qual considera ser a postura mais apropriada na manutenção da segurança dos Sistemas de Informação? A pró-ativa ou a reativa?
14. Na sua ótica, qual deve ser a abordagem aos incidentes críticos nos Sistemas de Informação das organizações?

Apêndice G – Termo de Consentimento Informado

Termo de Consentimento Informado

Eu, _____, aceito participar de livre vontade no estudo da autoria de Vítor Elísio Ferreira Cucu (Aspirante a Oficial de Polícia do Instituto Superior de Ciências Policiais e Segurança Interna), orientado pelo Superintendente Sérgio Ricardo Costa Chagas Felgueiras (Professor Associado do Instituto Superior de Ciências Policiais e Segurança Interna), no âmbito da dissertação de Mestrado Integrado em Ciências Policiais.

Foram-me explicados e compreendo os objetivos principais deste estudo e aceito responder a uma entrevista que explora questões sobre a Segurança dos Sistemas de Informação da PSP, e em especial do Sistema Estratégico de Informação.

Compreendo que a minha participação neste estudo é voluntária, podendo desistir a qualquer momento, sem que essa decisão se reflita em qualquer prejuízo para mim.

Ao participar neste trabalho, estou a colaborar para o desenvolvimento da investigação na área de Tecnologia Policial, não sendo, contudo, acordado qualquer benefício direto ou indireto pela minha colaboração.

Entendo, ainda, que toda a informação obtida neste estudo será estritamente confidencial e que a minha identidade nunca será revelada em qualquer relatório ou publicação, ou a qualquer pessoa não relacionada diretamente com este estudo, a menos que eu o autorize por escrito.

Nome_____

Assinatura_____

Data ___/___/___

Apêndice H – Quadro de Categorização

Categoria		Subcategoria		Ocorrências	
				Totais /Subcategorias	Total /Categoria
1	Importância do SEI na PSP	1.1	Tipologia de Informação do SEI	5	29
		1.2	Contributo do SEI para a PSP	9	
		1.3	Ativo Crítico de Informação	8	
		1.4	Margem de Progressão do SEI	7	
2	Necessidade de Proteção do SEI	2.1	Ameaças e Riscos	17	54
		2.2	Sabotagens	0	
		2.3	Ciberataques	3	
		2.4	Vulnerabilidades	23	
		2.5	Impactos das Falhas de Segurança	11	
3	Políticas e Estratégias	3.1	SGSI na PSP	12	52
		3.2	Requisitos de Segurança	12	
		3.3	Políticas de Segurança	21	
		3.4	Cibercultura na Instituição	4	
		3.5	Parcerias	3	
4	Pessoas	4.1	Responsáveis pela Segurança	7	33
		4.2	Desenvolvedores do SEI	2	
		4.3	Formação / Sensibilização dos RH em cibersegurança	9	
		4.4	Ação Disciplinar	15	
5	Medidas de Gestão e Implementação	5.1	Medidas de Contrainteligência	2	36
		5.2	Exercícios de Cibersegurança	1	
		5.3	Mecanismos de Segurança	5	
		5.4	Auditorias de Segurança	8	
		5.5	Resposta a Incidentes Críticos	20	

Fonte: Elaborado pelo autor.

Apêndice I – Manual de Codificação

Entrevistado	Código daUnidade de Registo (u.r.)	Categoria	1. Importância do SEI na PSP			
		Subcategoria	1.1 Tipologia de Informação do SEI	1.2 Contributo do SEI para a PSP.	1.3 Ativo Crítico de Informação	1.4 Margem de Progressão do SEI
		Manual de Codificação	Codificam-se, nesta subcategoria, as informações relativas ao tipo de informação do SEI	Codificam-se, nesta subcategoria, as ideias que permitem compreender o contributo do SEI na atividade da PSP	Codificam-se nesta subcategoria, as ideias relativas à extrema relevância da informação tratada no SEI.	Codificam-se, nesta subcategoria as informações que nos identifiquem possíveis evoluções do SEI
XXXX	1	"Para a PSP e para todo o sistema de investigação criminal nacional."			X	
XXXX	2	"O SEI alimenta, em termos comparativos, mais de metade da informação que se partilha entre os Órgãos de Polícia Criminal (OPC's), designadamente, através da PIIC."		X		
XXXX	3	"Nós temos muito mais volume de informação."			X	
XXXX	4	"Sim, é um ativo crítico, não só para a PSP, mas para os outros Órgãos de Polícia Criminal e para o Ministério Público (MP)."			X	
Total de Unidade de Registo por Subcategoria			**0**	**1**	**3**	**0**
Total de Unidades de Registo por Categoria			**4**			

Fonte: Elaborado pelo autor.