Plano Estratégico de Sistemas de Informação (PESI)

Relatório Síntese

Índice

1. Sumário Executivo

De acordo com a intenção da PSP em melhorar a eficiência dos seus sistemas de informação, permitindo uma maior satisfação das suas unidades, através da inserção de novas tecnologias ou o aperfeiçoamento das existentes, dos processos e das respetivas aplicações de suporte, foi desenvolvido um Plano Estratégico de Sistemas de Informação (PESI).

O presente documento pretende sumarizar todo o trabalho realizado, composto por quatro fases que se dividem em 8 documentos entregáveis. Cada fase foi elaborada de forma a responder aos objetivos essenciais à definição da estratégia futura de Sistemas de Informação da PSP. Esses objetivos são: a caracterização do modelo atual de TI/SI e a identificação dos atuais constrangimentos na vertente de TI/SI nas dimensões de tecnologia, pessoas e fornecedores (objetivos respondidos nas fases de Diagnóstico e *Benchmarking*), a definição do modelo de TI/SI futuro e respetivas iniciativas associadas (respondido na fase de Definição da Estratégia e Iniciativas SI), a identificação do plano de investimentos associado à implementação do modelo futuro de TI/SI e a definição um *roadmap* sobre as iniciativas a implementar (respondido nas fases de Definição da Estratégia e Iniciativas SI e *Roadmap*).

Na **fase de Diagnóstico**, foi analisada a situação atual dos sistemas de informação da PSP, abordando as dimensões de recursos humanos, processos e tecnologias. Foram identificados vários problemas, como a falta de integração entre os sistemas, a desatualização e fraca cobertura aplicacional, a falta de soluções de comunicação interna e externa, a complexidade e morosidade nos processos, a falta de suporte ao processo de supervisão e a ausência de ferramentas de análise e apoio à decisão, entre outros. Além disso, foram identificados constrangimentos transversais, como a falta de controlo da qualidade dos dados, a falta de padrões e melhores práticas, a falta de atualização de software e hardware, e o subdimensionamento dos recursos humanos.

Durante a **fase de *Benchmarking***, foram analisadas as melhores práticas de governação e modelos, as tecnologias aplicadas à segurança pública e estudos de caso em diferentes cidades ao redor do mundo. Foram destacados modelos de governação como o COBIT, ITIL, Lean IT e ISO 27001, que fornecem diretrizes para uma gestão eficiente e segura dos sistemas de informação. Em relação às tecnologias, foram mencionadas a *Internet of Things* (IoT), Inteligência Artificial (IA), Sistemas de Informação Geográfica (SIG) e *Big Data*, que têm sido aplicadas com sucesso na melhoria da eficiência e eficácia das organizações de segurança pública. A comparação entre o diagnóstico realizado na PSP e as soluções existentes no mercado/setor destacou a falta de um ERP transversal, ferramentas adequadas de gestão documental, infraestruturas de sistemas de informação atualizadas, capacidades de *data analytics e Big Data*, integração de georreferenciação, utilização de tecnologias como *bodycams*, videovigilância e drones, e arquitetura de telecomunicações abrangente e moderna.

Na **fase de Definição da Estratégia e Iniciativas SI**, foi definida a arquitetura funcional de SI futura da PSP, que tem por base o ponto único de acesso aos serviços pelos cidadãos, empresas e entidades. De seguida foram determinados os princípios orientadores para a criação da proposta de eixos de atuação e respetivas iniciativas.

As iniciativas propostas abrangem várias áreas, desde a modernização dos sistemas de informação até a melhoria dos processos de trabalho e a adoção de tecnologias inovadoras. A implementação dessas iniciativas visa a transformação digital da PSP, aprimorando sua eficiência operacional, a qualidade dos serviços prestados e a colaboração com outras entidades. A estratégia é dividida em cinco eixos principais:

1. **Digital**, que visa a transformação digital da PSP, incluindo a revisão dos conteúdos de informação pública, a criação de um Balcão Único *Online* para acesso aos serviços da PSP, a melhoria da qualidade de dados, a emissão de cartões digitais para colaboradores e a implementação de um sistema de gestão documental;
2. **Auto-Serviço**, que tem como objetivo disponibilizar serviços de auto atendimento para os colaboradores e seus familiares, incluindo o desenvolvimento de uma aplicação móvel (App PSP), a implementação de um sistema de gestão acadêmica, a evolução da intranet da PSP e a implementação de um sistema integrado de gestão (ERP) para recursos humanos, finanças e património;

3. **Cooperação**, que busca melhorar a colaboração da PSP com outras entidades e instituições, incluindo a implementação de uma extranet para facilitar o partilha de informações, o aprimoramento da gestão de ocorrências e fiscalizações, a implementação de uma solução de relacionamento com clientes (CRM) e a melhoria da gestão de meios e planeamento operacional;
4. **Infraestruturas**, que visa aprimorar a arquitetura tecnológica e as comunicações da PSP, incluindo a expansão do armazenamento de dados, a melhoria dos ativos e serviços de alojamento, a implementação de políticas de gestão de acessos e identidades, e a adoção de uma política *Bring Your Own Device* (BYOD); e, por fim,
5. **Eficácia**, que tem como objetivo melhorar a governação do Departamento de Sistemas de Informação e Comunicações (DSIC), revisar o modelo de custeio da implementação do Plano Estratégico de Sistemas de Informação (PESI), aprimorar as práticas de segurança de SI e conformidade, e melhorar o controlo e comunicação de acordos de nível de serviço (SLAs).

Estas iniciativas foram avaliadas de acordo com o seu impacto e a sua urgência, e foram definidos níveis de prioridade consoante a sua classificação, onde na **fase de *Roadmap*** são apresentadas num cronograma de implementação de 01.2024 a 12.2027 (4 anos), demonstrando o esforço financeiro anual (sendo que o valor total varia entre €15,7M e €17,7M), as durações estimadas de cada iniciativa e respetivo início da cada uma e, incluindo as *quick wins* associadas.

Na fase de *Roadmap* são também abordadas as questões sobre o recrutamento e a formação de colaboradores, onde foi feita uma contextualização da situação atual através de um questionário elaborado aos colaboradores do Departamento de Sistemas de Informação e Comunicações (DSIC). Neste capítulo, destaca-se a necessidade de contratar recursos internos e externos, considerando a confidencialidade e sensibilidade das funções desempenhadas. É sugerido o desenvolvimento e capacitação dos recursos internos, bem como a busca de recursos externos no mercado. É também apresentada uma sugestão de dimensionamento do DSIC.

Por fim, são definidos os fatores críticos de sucesso para o projeto, visando garantir sua implementação bem-sucedida.

2. Diagnóstico

2.1. Abordagem Metodológica

O trabalho em questão aborda a análise da situação dos sistemas de informação da Polícia de Segurança Pública (PSP) em Portugal, identificando os principais problemas e lacunas existentes. A abordagem metodológica utilizada incluiu análise documental, **28 entrevistas** com os interlocutores das unidades orgânicas, estabelecimentos de ensino e a unidade especial polícia, e questionários aos colaboradores. A análise da situação atual foi direcionada a três dimensões:

- **Recursos humanos**: Os aspetos de natureza organizacional da área de TI, nomeadamente no que concerne à sua caracterização orgânica e funcional, e respetivos perfis, são essenciais para assegurar uma resposta adequada às tarefas a desempenhar.
- **Processos**: Os processos devem assegurar a execução das tarefas adequadas como resposta às necessidades do negócio, devidamente suportados nas ferramentas tecnológicas.
- **Tecnologias**: As tecnologias são o principal objeto da atividade da área de TI e as principais ferramentas de suporte aos processos de TI e processos de negócio.

2.2. Arquitetura Funcional SI

A arquitetura atual assenta num conjunto alargado e disperso de sistemas para suporte a processos transversais, não integrados e com fraca cobertura aplicacional. A utilização de ferramentas *Microsoft Office* é muito intensiva, resultando na necessidade de articulação manual entre sistemas.

Os sistemas foram divididos em Sistemas *Core* (fundamentais) e Sistemas de Suporte (secundários), tendo sido feita uma apreciação e análises mais focalizadas a cada uma das dimensões.

O SEI, por exemplo, que é considerado o "grande sistema da PSP", possui diversos módulos associados, mas uma fraca capacidade de integração com os restantes sistemas, resultando em duplicação de procedimentos que poderiam ser integrados, sendo a sua atualização de forma manual, o que não garante que a informação é fidedigna e está isenta de erros. O SEI, tendo em conta as suas limitações, dá resposta às necessidades da PSP, mas poderia haver uma maior desmaterialização e eficiência na realização de determinados processos. Em termos de ligação com sistemas externos, o SEI apresenta algumas ligações via *web service*, como por exemplo SISOne4All - pessoas, veículos, armas e documentos, CITIUS, INCM – ofícios, cartões e licenças SIGAE, ANSR – acidentes, BEAV's, etc., mas ainda há a necessidade de maior integração com sistemas externos.

O SIGAE, por sua vez, necessita de maior integração com os sistemas SerOnline, RIDAP e SIREC e ainda com outros sistemas externos necessários para garantir a eficácia e eficiência dos processos relacionados com armas e, quando implementado, explosivos.

Existe ainda uma maior necessidade de integração dos processos e sistemas de pagamento, principalmente entre o SIREC e o SIGAE, e ainda com diversos sistemas externos utilizados pelo Departamento de Gestão Financeira, ou então entre o GIRe/SEI (para questões de remunerados).

A fraca integração entre os sistemas faz com que haja a recolha repetida e redundância de informação e duplicação de "esforços". Existem muitos sistemas dentro da mesma UO que não comunicam entre si, sendo que muita informação ainda se encontra em ficheiros de *MS Excel* e *MS Access*.

Ainda, a fraca cobertura aplicacional, fruto da desatualização aplicacional, faz com que grande parte das soluções estejam já tecnologicamente desadequadas.

2.3. Constrangimentos

Os principais constrangimentos identificados foram divididos em constrangimentos nos macroprocessos da atividade da PSP e em constrangimentos transversais a todas as áreas.

A. Macroprocessos

1. **Desatualização e fraca cobertura aplicacional**: Muitas soluções existentes na PSP estão desatualizadas e não atendem às necessidades atuais. Algumas soluções propostas em planos anteriores ainda não foram implementadas. Existem várias áreas que carecem de soluções atualizadas, como gestão de património, gestão de contratos, gestão financeira, gestão de stocks, gestão acadêmica, gestão de recursos humanos, entre outras. Algumas unidades orgânicas da PSP ainda não possuem suporte aplicacional adequado para as suas atividades.

2. **Falta de transversalidade e atualização das soluções desenvolvidas**: As soluções implementadas foram personalizadas para cada unidade orgânica, o que resultou em falta de cobertura aplicacional abrangente. Sugere-se a consideração da implementação de soluções mais genéricas e parametrizáveis que atendam a 80% das necessidades das unidades orgânicas. Também é recomendada a utilização de metodologias ágeis para disponibilizar soluções de forma iterativa e incremental.

3. **Falta de soluções de comunicação interna**: Existem lacunas nas soluções de comunicação interna da PSP. A informação confidencial e classificada não possui uma solução segura para partilha adequada. Além disso, há falta de suporte aplicacional para a publicação e consulta de ordens de serviço e comunicações internas dirigidas a unidades orgânicas, comandos e esquadras. A falta de integração entre sistemas e a dependência de ferramentas como o *MS Excel* e o *MS Access* também dificultam a comunicação e partilha de informações.

4. **Falta de soluções de comunicação com o exterior**: Os sistemas internos da PSP não estão integrados com as soluções de comunicação com o exterior. Não há utilização de fontes mestre fidedignas de informação, resultando em processos manuais de validação de documentos. A comunicação com o público é feita principalmente por e-mail, e falta a disponibilização de estatísticas e informações públicas. Também há falta de acesso a informações específicas para utilizadores externos credenciados.

5. **Complexidade e morosidade no processo de licenciamento e verificação**: Os processos de licenciamento e verificação da PSP são burocráticos e demorados. A falta de integração entre os sistemas e a dependência de documentos físicos resultam em processos demorados e propensos a erros. A autenticidade dos documentos é verificada manualmente, e há a necessidade de deslocamento físico para validação de alguns documentos.

6. **Fraco suporte ao processo de supervisão**: A aplicação SEI não suporta o planeamento de supervisão, auditorias e follow-up de não conformidades e planos de ação corretiva. A informação relacionada encontra-se dispersa.

7. **Estatísticas não automáticas e pouco fidedignas**: As estatísticas atuais são obtidas manualmente, sem automação nem acesso em tempo real. São necessárias melhorias na qualidade dos dados, removendo duplicações e validando informações. Além disso, é preciso desenvolver formas de obtenção de estatísticas mais detalhadas e cruzadas, e fornecer informações atualizadas para o público externo. São necessárias ferramentas e formação em *Data Mining* e *Business Intelligence* para melhorar a monitorização e tomada de decisões.

B. Constrangimentos transversais

8. **Falta de controlo da qualidade dos dados**: Ausência de processos que assegurem a qualidade dos dados, destacando a necessidade de fontes seguras e validações robustas.

9. **Criação de Histórico**: Ausência de processos para transferência de informações não relevantes para o histórico.

10. **Manutenção do Histórico de Entidades**: Falta de processos para manter o histórico de entidades quando há alterações de designação, morada ou fusões/extinções.

11. **Inexistência de prazos de conservação de arquivo**: Necessidade de implementar processos de criação e remoção de registos, respeitando prazos de conservação.

12. **Falta de conformidade com o RGPD**: Necessidade de implementar processos em conformidade com o Regulamento Geral de Proteção de Dados, incluindo direitos de acesso, retificação, apagamento, entre outros.

13. **Otimização de processos de negócio**: Necessidade de otimizar os processos de negócio, eliminando tarefas duplicadas e sem valor agregado, e estabelecendo ferramentas de registo e avaliação de prazos de realização.

14. **Fraca desmaterialização**: Baixa automatização e uso de processos manuais, incluindo o uso excessivo de papel, e-mail, correio e serviços de estafetas. Sugere-se a automação do registo de notas e a desmaterialização da publicação de ordens de serviço.

15. **Conversão de arquivo físico em arquivo digital**: Necessidade de converter arquivos físicos em formato digital, especialmente em casos de arquivos financeiros e microfilmagens.

16. **Inexistente suporte tecnológico**: Falta de ferramentas de *workflow*, BPM (*Business Process Management*) e Gestão Documental para suportar a tramitação digital de processos e acesso ao arquivo documental. É necessário respeitar normas e requisitos da Administração Pública.

17. **Inexistente monitorização dos processos**: Ausência de informações de gestão e apoio à decisão sobre atividades realizadas e estado dos processos. Falta de processos para recolha e disponibilização de métricas, criação de resumos de informações e painéis de controlo.

18. **Inexistência de ferramentas de análise e apoio à decisão**: Necessidade de ferramentas de *Data* Mining e *Business Intelligence* para extrair informações de dados resumidos e operacionais.

19. **Inexistência de ferramentas de análise sobre informação aberta**: Necessidade de ferramentas de *Open-source Intelligence* (OSINT) para recolha e análise de informações públicas relacionadas à prevenção e investigação criminal.

20. **Fraca usabilidade**: Dificuldade de utilização de sistemas, exigindo tarefas específicas de pouco valor agregado e falta de adaptação a diferentes dispositivos.

21. **Sistemas não responsivos**: Aplicações *web* que não se ajustam ao tamanho e formato dos dispositivos utilizados, resultando em desperdício de espaço na tela.

22. **Falta de acesso aplicacional móvel**: Limitações no acesso remoto a aplicações e necessidade de dispositivos móveis e acesso móvel no terreno.

23. **Inexistência de gestão centralizada e flexível de perfis de utilizadores**: Falta de uma gestão flexível de perfis de utilizadores que permita restringir o acesso à informação e funcionalidades, acompanhando mudanças organizacionais.

24. **Fraca utilização de assinatura digital profissional**: Uso limitado de assinaturas digitais profissionais, considerando a confidencialidade e autenticidade da informação.

25. **Georreferenciação ainda muito limitada**: Necessidade de um inventário georreferenciado de imóveis, equipamentos e existências, além de mecanismos para registo e consulta integrada de georreferenciação em tempo real.

26. **Desalinhamento face a melhores práticas**: Processos de TI desalinhados das melhores práticas, como COBIT, ITIL e ISO 27001.

27. **Não aplicação de standards organizacionais**: Falta de aplicação de padrões para desenvolvimento, documentação e integração de aplicações.

28. **Falta de atualização de *software* e *hardware***: Ausência de atualização do parque de *hardware* e *software* de base.

29. **Falta de automatização de atualização de *software***: Falta de automação na atualização remota do *software* aplicacional.

30. **Inexistência de plano de continuidade de negócio**: Falta de um plano para garantir a continuidade dos serviços em caso de ameaças às TI.

31. **Subdimensionamento dos recursos humanos**: Número insuficiente de funcionários em relação ao volume de tarefas, falta de competências técnicas adequadas e dependência excessiva de fornecedores.

3. Benchmarking

3.1. Melhores práticas de Governação e modelos

A governação em sistemas de informação refere-se à implementação de processos, políticas e procedimentos para uma gestão eficiente e segura dos SI nas organizações. O objetivo principal é garantir que os SI suportem os objetivos estratégicos da organização, promovendo transparência, responsabilização e conformidade regulamentar. A governação pode ajudar as organizações a melhorar a eficácia, eficiência e agilidade, resultando em melhores decisões e redução de custos. Além disso, a governação contribui para a segurança e conformidade, apoiando o cumprimento de leis e regulamentos, como o RGPD.

Os modelos de governação proporcionam uma estrutura e diretrizes claras para a tomada de decisões, implementação de políticas e gestão eficaz. Alguns dos principais objetivos da governação em SI incluem:

- **Alinhamento estratégico**: Garantir que a estratégia dos SI esteja alinhada com a estratégia de negócios, por meio de modelos de arquitetura corporativa e gestão de portfólio.
- **Entrega de valor**: Articular a tomada de decisão em relação aos investimentos para entregar o máximo valor, considerando benefícios e riscos aceitáveis.
- **Gestão de risco**: Identificar, avaliar, mitigar, comunicar e monitorizar os riscos relacionados aos SI, em um contexto empresarial cada vez mais digital e interconectado.
- **Gestão de recursos**: Gerir e alocar recursos adequados para executar as atividades necessárias, incluindo investimentos em pessoal e infraestrutura.
- **Análise de desempenho**: Avaliar a implementação da estratégia, execução de projetos e alocação de recursos para direcionar ações de SI e otimizar a estratégia da área de tecnologia.

A governação em SI busca melhorar a gestão e maximizar o valor dos sistemas de informação, considerando a estratégia organizacional, a segurança dos dados e o cumprimento das regulamentações.

Figura 1 - Principais vertentes da Governação

Modelos:

- **COBIT**: *Framework* de governação de TI que visa gerar processos eficazes e gestão efetiva das rotinas de tecnologia da informação. Enfatiza fatores de desempenho, área de foco e comunicação.
- **ITIL**: *Framework* de boas práticas de gestão de serviços de TI que abrange princípios, governação, cadeia de valor de serviço, práticas e melhoria contínua.
- ***Lean* IT**: Modelo que combina o pensamento *Lean* e o sistema *Toyota* de produção na área de SI, com o objetivo de aumentar a produtividade e otimizar o uso dos recursos. Baseia-se na especificação do valor, identificação do fluxo de valor, garantia do fluxo contínuo e busca pela melhoria contínua.
- **ISO 27001**: Fornece diretrizes para a definição de um Sistema de Gestão de Segurança da Informação, abrangendo aspetos técnicos, boas práticas de negócio, políticas de processamento de informação, formação de colaboradores e planos de contingência. Os princípios da ISO 27001 incluem o contexto da organização, o âmbito do SGSI, a liderança, o planeamento, o suporte, a operação, a avaliação de desempenho e a melhoria. O objetivo é garantir a segurança da informação e minimizar riscos, com atenção à documentação adequada e correção de problemas identificados

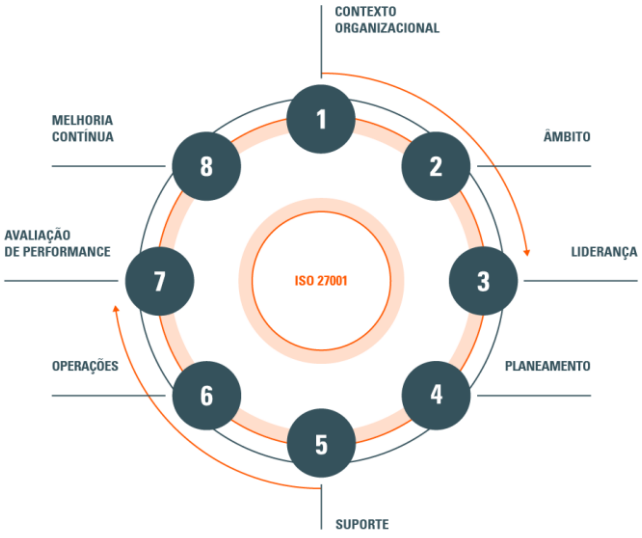

Figura 2- Diretrizes ISO 27001

3.2. Tecnologias aplicadas à Segurança Pública

A. Tecnologias

As tecnologias aplicadas à segurança pública têm desempenhado um papel fundamental na melhoria da eficiência e eficácia das organizações responsáveis pela segurança da população. Algumas das tecnologias mais relevantes incluem a ***Internet of Things* (IoT), Inteligência Artificial (IA), Sistemas de Informação Geográfica (SIG) e *Big Data***.

A **IoT** permite a obtenção e integração de dados em tempo real a partir de várias fontes, como dispositivos móveis, sistemas de intrusão, reconhecimento facial, câmaras de segurança com análise de vídeo, leitura de placas de veículos, drones, entre outros. A integração desses dados possibilita o acesso e compartilhamento de informações importantes para a segurança pública.

A **IA** identifica padrões, tendências e anomalias em tempo real, fornecendo uma maior consciência situacional e apoio na tomada de decisões. Além disso, a IA permite otimizar processos, sugerir ações e automatizar tarefas redundantes, proporcionando maior agilidade e precisão nas respostas às emergências. O *Machine Learning* é uma técnica que permite processar e analisar grandes volumes de dados em tempo real, baseando-se na experiência dos usuários dos sistemas e retroalimentando as regras e fluxos de trabalho da IA.

Os **SIG** são sistemas informáticos/geográficos que permitem localizar objetos em um mapa e geri-los de acordo com características similares. Eles são amplamente utilizados na gestão do território, planeamento urbano, estudos de transformação do território, proteção civil, cartografia temática, estatística, estudo do patrimônio cultural/ambiental/construído, entre outras aplicações. Os SIG permitem um planeamento preciso do território e das intervenções a serem realizadas.

O ***Big Data*** é uma abordagem tecnológica que permite aceder e processar dados de diversas fontes e formatos não estruturados, permitindo a correlação entre dados para identificação de *insights*. No contexto da segurança pública, o *Big Data* é utilizado para estudar o comportamento de criminosos, identificar horários e locais de maior ocorrência de crimes, além de auxiliar no policiamento preditivo.

B. Case Studies

No caso de São Paulo, Brasil, o **sistema DETECTA** utiliza *Big Data* para reunir e analisar informações em tempo real, otimizando a segurança pública. O sistema integra dados de diversas fontes, como registos de ocorrências e relatórios de pessoas desaparecidas, para oferecer uma visão abrangente da situação.

Em Londres, Reino Unido, o **sistema *Crush*** utiliza algoritmos de *Big Data* para mapear localidades com base em registos de crimes passados e informações sobre o clima. Isso permite que a polícia desloque os agentes de forma mais eficiente e realize policiamento preditivo.

Em Nova York, EUA, **o *Domain Awareness System* (DAS)** é uma rede de câmaras, sensores, bancos de dados e infraestrutura relacionada que fornece informações e análises aos policiais para garantir a segurança pública. No entanto, o DAS também levanta preocupações relacionadas à privacidade e aos falsos-positivos.

Na Cidade do México, o **uso de drones** pela polícia resultou em uma queda de 10% na taxa de criminalidade. Os drones ajudam na deteção e detenção de suspeitos, além de fornecerem evidências cruciais em futuros processos judiciais.

Em Dublin, Irlanda, estão sendo implementadas tecnologias como **câmaras corporais, reconhecimento automático de placas de veículos e CCTV de terceiros para auxiliar as forças policiais**. A utilização de *bodycams* tem sido discutida como uma medida para reduzir a letalidade policial e proteger os agentes.

No Brasil, tanto em Santa Catarina quanto em São Paulo, ***bodycams*** - câmaras de segurança são incorporadas aos uniformes policiais, resultando numa redução significativa de confrontos e resistência às abordagens policiais.

Em Hamburgo, Alemanha, foi desenvolvida uma **plataforma baseada em Sistemas de Informação Geográfica** para aprimorar as operações de segurança durante a cúpula do G20 em 2017. A plataforma integra várias fontes de dados e fornece informações em tempo real para apoiar as operações diárias da polícia.

Estes estudos de caso destacam como a aplicação de tecnologias como *Big Data*, Inteligência Artificial, *Internet of Things* e Sistemas de Informação Geográfica pode melhorar a eficiência e a eficácia das organizações responsáveis pela segurança pública. No entanto, também são mencionadas preocupações relacionadas à privacidade e aos possíveis falsos-positivos.

3.3. Análise Comparativa – Fase de Diagnóstico vs Fase de *Benchmarking*

Vertente	PSP – levantamento (fase de diagnóstico)	Soluções existentes no Mercado/Sector
ERP	Não existe um ERP transversal que tenha uma abrangência interdepartamental, com informação unificada e integração com outros sistemas (internos ou externos). Encontram-se em falta soluções ou versões atualizadas de gestão de património, de stocks, financeira, de contratos, de recursos humanos, entre outras, e os sistemas que existem não estão integrados entre si. Ex.: GIRe (Gestão Integrada de Recursos) e SIREC (Sistema Integrado de Receitas).	A implementação de um ERP consolida os dados entre departamentos e integra várias áreas de negócio, como recursos humanos, financeira e logística, tornando os processos estandardizados e permitindo a transversalidade dos mesmos. De forma geral, as entidades congéneres optam pela utilização de soluções desenvolvidas presentes no mercado, como o **SAP** (polícia da Irlanda do Norte, p.e.), o **Oracle** (Met Police e polícia de Merseyside, p.e.), **Quidgest** (solução portuguesa direcionada ao sector público).
Gestão Documental	Não existem ferramentas fidedignas de Gestão Documental para suporte à tramitação eletrónica dos processos, partilha de documentos e o acesso simples e imediato ao arquivo documental. A solução atual (GESDOC) é muito limitativa no que diz respeito ao upload (500kb), não apresenta integração com os restantes sistemas, é pouco *user-friendly* e não tem possibilidade de edição e controlo de versões.	Um sistema de Gestão Documental permite à PSP uma organização e extração de documentos simplificadas através de pesquisas globais, aumentando a produtividade e reduzindo o desperdício de tempo. Existem no mercado várias ferramentas de gestão de conteúdos, como o **FileDoc, Smart Docs, SimpleFlow, Quidgest, OpenText**, entre outras.
Infraestruturas SI	Os equipamentos da PSP apresentam uma idade avançada e a capacidade de armazenamento de dados está desatualizada relativamente às necessidades atuais da PSP. A infraestrutura do *Data Center* tem diversas debilidades (falta de dispositivos contra incêndios e sistemas de refrigeração adequados). Os equipamentos já não têm capacidade de resposta às necessidades de desempenho e de alta disponibilidade, e a integridade dos sistemas e/ou dos dados pode ser comprometida por um incidente. Não existe um site alternativo para continuidade por motivos de falha, falta ou desastre.	A refrigeração e o sistema anti-incêndio são duas das mais importantes boas práticas na manutenção de um D*ata Center*. Um fator bastante importante na gestão de *Data Centers* é também a criação de caminhos alternativos em caso de falhas nos servidores ou outro tipo de *down time*. Fabricantes reconhecidos com soluções ajustadas como a **Rittal, Schneider, Cisco, IBM**, entre outras. Recursos humanos qualificados para tarefas operacionais e de manutenção dos *data centers* é igualmente uma necessidade para o sucesso destas infraestruturas.

Vertente	PSP – levantamento (fase de diagnóstico)	Soluções existentes no Mercado/Sector
Data Analytics e Big Data	Atualmente na PSP não existem ferramentas e nem formação em *Data Mining* e *Business Intelligence* para monitorização. A PSP também não possui nenhuma área/departamento de análise de dados para que possa ser implementado um policiamento preditivo, de forma a identificar tendências para a prevenção e para apoiar a tomada de decisão. Melhorias em *dashboards* – ex: sala de comando e controlo.	A *Data Analytics* na segurança pública é utilizada não só no controlo e monitorização dos processos e operações, mas é também utilizada pelas maiores polícias do mundo como a NYPD ou a Met Police para o policiamento preditivo. Outras utilizações mais operacionais são a construção de perfis criminais e para a análise de provas que contenham dados, como nos casos de fraudes fiscais e cibercrime, através de *data mining* e *Big Data*. Fabricantes de soluções específicas: **NICE, TIBCO, SAS Institute**.
Georreferenciação (SIG)	O módulo de gestão de meios PSP e georreferenciação necessita de atualização e que seja integrado com o sistema SIRESP e também que realize a gestão dos recursos policiais X gestão de incidentes, com uma representação gráfica do terreno e integração com sistemas de vídeo público e privado. Não existem mecanismos de consulta integrada em tempo real.	Existem soluções para o setor de segurança pública que permitem que o ciclo de vida da ocorrência seja completo, a integração entre a área operacional e administrativa/processual - ex: **OnCall Hexagon, ArcGIS Pro ESRI, Telycan**. Estas soluções têm também integrações com soluções de *Data Analytics* no policiamento preditivo, como no caso da identificação de *hot spots*, por exemplo. A polícia de Hamburgo é um exemplo da utilização destas tecnologias.
IoT - *Bodycams*, Videovigilância e Drones	Foi lançado o concurso público de aquisição da plataforma de gestão de informação proveniente de *bodycams* e de sistemas de videovigilância municipais, sendo que depois da aquisição será lançado o concurso para a aquisição das *bodycams*. A PSP possui drones, utilizados para a monitorização de grandes eventos, por exemplo, mas falta incorporar a sua utilização para mapeamento de terrenos e controlo de massas, integrando com um Sistema Integrado de Georreferenciação.	Existem inúmeros casos de polícias mundiais que recorrem a métodos de videovigilância. Nos exemplos dados no capítulo anterior, verifica-se o caso de São Paulo e Nova Iorque que recorrem a redes de câmaras, utilizando *Big Data* para o cruzamento de informação. Exemplos: **Dahua, FLIR, Hikvision, Bosch, Avigilon, Axis**. No caso da Irlanda, a Garda Síochana tem um projeto de lei para a utilização de CCTV de terceiros. Para além disso, têm também um projeto de lei para a utilização de *bodycams.* Algumas polícias de cidades brasileiras utilizam também as *bodycams*, que refletiu numa queda do número de confrontos e casos de resistência policial. Fabricantes de *bodycams* para forças de segurança: **Argus, Axon, Motorola**. Por fim, observa-se o caso da Cidade do México que utiliza drones para monitorizar a cidade, com resultados bastante positivos. Fabricantes de drones específicos para forças de segurança: **Brinc Drones, DJI, Autel Robotics**.

3.4. Arquitetura de telecomunicações

A topologia da rede atual da PSP é a apresentada na imagem abaixo.

- A rede de comunicações WAN assenta na RNSI para a comunicação de dados entre todos os sites da PSP.
- A rede RNSI assegura, de base, todas as caraterísticas de desempenho adequado, escalabilidade e segurança.
- As redes locais (LAN) ligam-se entre si através da rede RNSI, e são exclusivamente cabladas (isto é, não existem acessos WiFi). Estão disponíveis acessos através de algumas placas de dados das operadoras de telecomunicações que ligam também à rede através da RNSI.

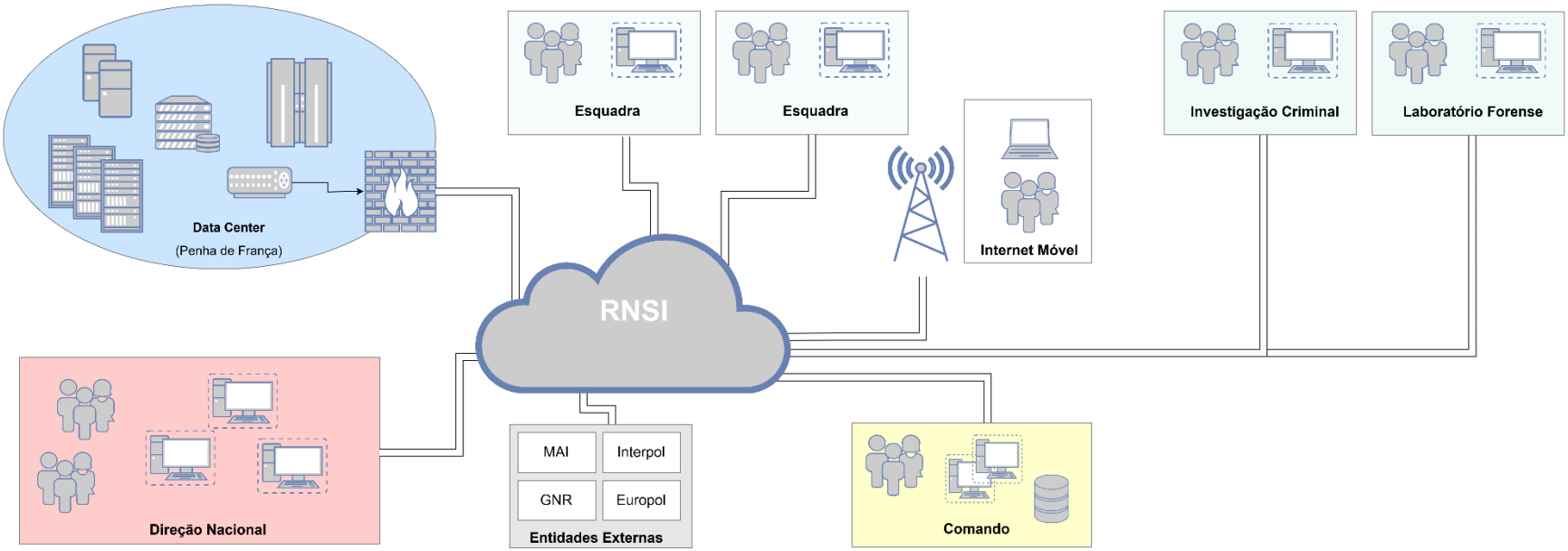

Figura 3 - Diagrama da rede atual da PSP

Nota: Diagrama construído com base na interpretação da equipa de consultoria das interações com as diversas áreas relevantes e de alguns inputs fornecidos pela PSP

O estado atual da infraestrutura de redes da PSP permite retirar as seguintes conclusões:

Rede de dados: A Gestão de praticamente toda a rede de dados WAN é assegurada pela RNSI. A rede de voz sobre dados encontra-se em desenvolvimento e assenta igualmente sobre a rede da RNSI. Os contratos de voz e dados são geridos pelo MAI (contrato da rede estruturada é assegurado pela RNSI e gerido pela PSP. As redes LAN nos diversos locais são geridas pela própria PSP.

Servidores departamentais: Os equipamentos apresentam uma idade avançada (com algumas exceções), pelo que a tecnologia carece de atualização. Por esse motivo não existem capacidades de tolerância a falhas de forma abrangente. Os servidores interligam com o armazenamento por intermédio de equipamentos de comunicação assentes em tecnologia de *Switch.*

Segurança da informação: A segurança da informação é assegurada com base em diversas tecnologias de controlo (à intrusão; SPAM; etc) que estão assentes em diversos equipamentos, com sistemas e gestão próprios. No entanto, não existe integração entre as diversas tecnologias, nem uma lógica de visão única (tipo *dashboard* de controlo) das várias dimensões de segurança. Os upgrades, *patches* e *updates* às diversas aplicações são assegurados, mas sempre dependente da disponibilidade da equipa.

Salvaguarda da informação: Existem políticas de *backups* de dados em vigor, embora haja limitações no procedimento relacionadas com a capacidade e antiguidade dos equipamentos utilizados, não sendo realizados backups para fora do *Data Center*. As políticas de catalogação e salvaguarda dos arquivos de backup devem ser atualizadas. A política de antivírus é adequada às necessidades.

Armazenamento de dados: A capacidade de armazenamento de dados (*storage*) da PSP encontra-se desatualizada face às suas necessidades atuais de geração de dados. Além da geração de dados, deverão ser consideradas as necessidades associadas a gestão e armazenamento de dados.

Resistência a falhas: Existem diversos pontos de falha, designadamente balanceador de tráfego que está em modo *standalone* devido à avaria do equipamento de redundância. Não existe redundância para disponibilização do mesmo serviço aplicacional (*clustering*) em nenhuma das aplicações.

Data Center: A infraestrutura do *data center* tem diversas debilidades (p.e. segurança dos acessos físicos, eliminação de incêndios, refrigeração). Os equipamentos já não têm capacidade de resposta às necessidades de desempenho e de alta disponibilidade, e a integridade dos sistemas e/ou dos dados pode ser comprometida por um incidente, ainda de não seja de gravidade elevada. Não existe um site alternativo para continuidade por motivos de falha, falta ou desastre.

4. Definição da Estratégia de Iniciativas SI

4.1. Arquitetura Funcional

A arquitetura futura permitirá um ponto único de acesso aos serviços pelos cidadãos e empresas. E outro ponto único de acesso ao Office PSP: atendimento presencial, *frontoffice* PSP e *backoffice* PSP. A complexidade, a origem dos serviços e a diversidade de aplicações e sistemas ficará escondida ao utilizador.

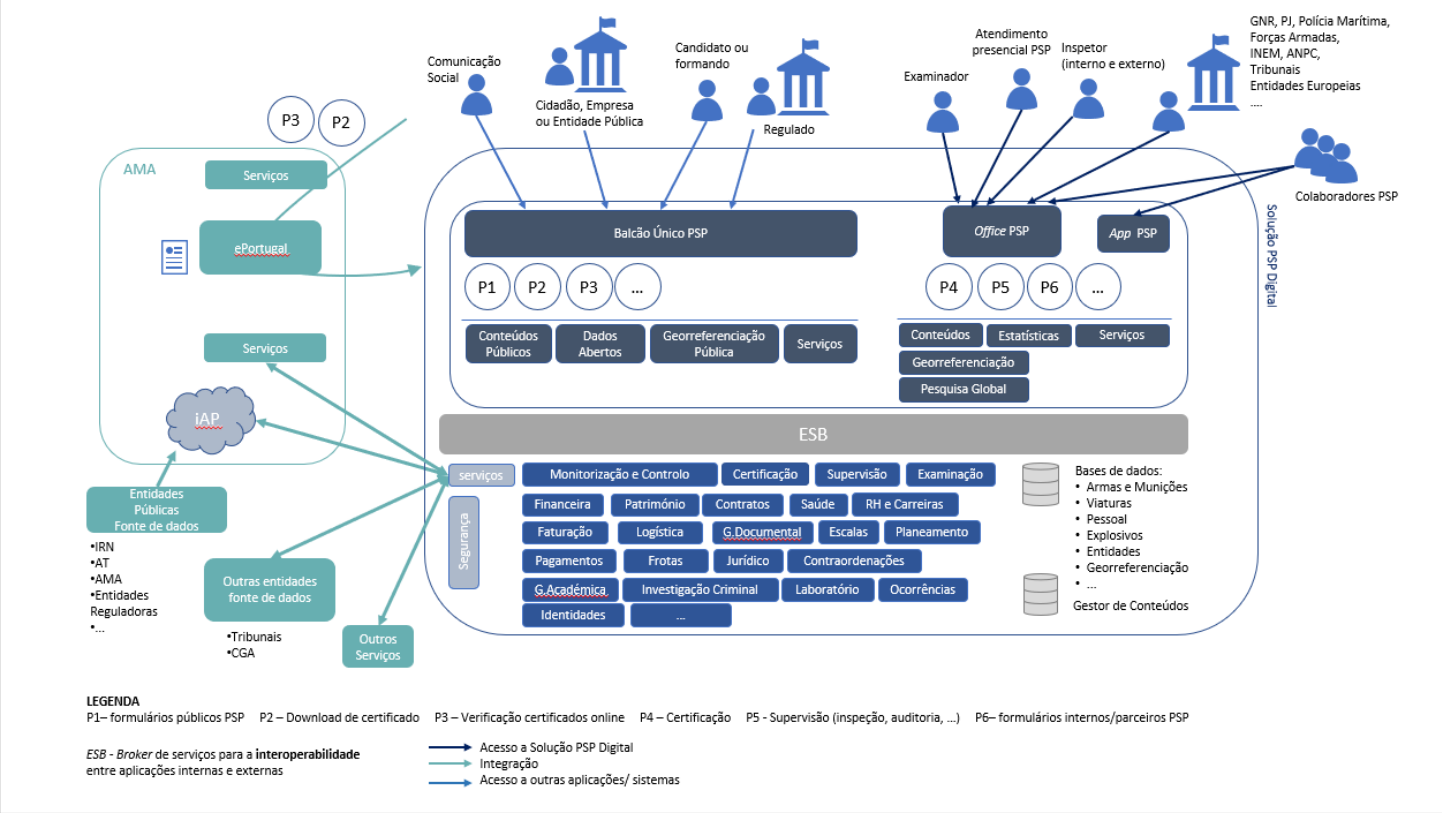

Figura 4 - Arquitetura funcional futura

4.2. Princípios Orientadores

Estes foram os princípios que nos guiaram na proposta de iniciativas.

A. Interoperabilidade

Para a PSP responder de forma integrada e atempada ao volume de pedidos/ documentação que lhe chega, será necessário ter um *backbone* interoperável, desde a entrada do pedido (com recolha de dados mestre) até à sua resposta, integrando todos os intervenientes no processo. A documentação deverá ser registada e desmaterializada num sistema de gestão documental.

Adicionalmente, a informação (certificação, licença) produzida num processo deverá poder ser processável, verificável e partilhável, de forma automática, com outros processos. Deverá também ter período de validade e ser cancelável e atualizável com efeitos imediatos. Este fluxo de informação, permitirá a alimentação de *dashboards* de informação de negócio e de monitorização, possibilitando não só a decisão informada como o controlo dos processos.

B. Abrangência e Flexibilidade

Por forma a responder de forma abrangente aos múltiplos processos da PSP, e acompanhando tempestivamente as alterações legais e mudanças de requisitos do negócio, recomenda-se a utilização de soluções genéricas end-to-end, parametrizáveis, com fluxo de trabalho flexível ou não definido, e a automação da triagem e reencaminhamento. Sugerimos a aquisição de pacotes de software para o âmbito padrão e a implementação do restante âmbito no modelo Agile Híbrido.

Neste modelo, após um planeamento estratégico de alto nível (PESI) (*waterfall*), é utilizado o SCRUM para o desenvolvimento de cada iniciativa. Cada iniciativa é disponibilizada de forma iterativa e incremental, sendo a MVP (*Minimum Viable Product)*, a primeira versão funcional, sobre a qual se pode recolher feedback. A vantagem desta abordagem é trazer valor ao negócio quanto antes (entrega de funcionalidades) e a capacidade de ajuste (prioridades, âmbito, prazos) face ao feedback e alterações no ambiente.

C. Autonomia

A disponibilização de soluções padrão, intuitivas e simples, de pedido de serviços PSP possibilitará a sua utilização por qualquer utilizador externo ou interno. Neste âmbito sugerimos:

- A disponibilização de informação pública e interna (estatísticas, georreferenciação, …) – neutralizando o esforço de produção, agregação e comunicação de informação, a pedido, para o interior e exterior.
- A disponibilização de soluções de auto-serviço (app colaborador, pedido de meios, registo de ocorrência, pedido de serviço / reclamação no Balcão Único).
- Sempre que possível, a aprovação e controlo automáticos (plafonamento, alertas), aliviando a supervisão.

D. Mobile-Ready

Com as devidas medidas de segurança, os equipamentos pessoais podem ser utilizados como complemento aos equipamentos institucionais *(Bring Your Own Device (BYOD)).* Sugerimos soluções acessíveis a todos e em mobilidade, *mobile-ready* (foco no essencial e na melhor experiência de utilizador em dispositivos móveis), simples, intuitivas e respeitando também padrões de acessibilidade e de usabilidade.

E. Sustentabilidade

Em complemento ao orçamento de estado, sugere-se o desenvolvimento de medidas de rentabilização (monetização): que reduzam a utilização de recursos e o custo operacional (pela simplificação dos processos e sua digitalização); que possibilitem o maior controlo da receita; que melhorem as condições de trabalho dos colaboradores (melhores SI, formação, progressão na carreira, flexibilidade de turnos; cuidados de saúde, alojamento, remuneração,…),e que aumentem a receita (maior serviço prestado, novos serviços,…). A maior autonomia no investimento permitirá a consistência e a continuidade da estratégia planeada.

4.3. Iniciativas

A. Eixo 1: + Digital

Iniciativas	Âmbito	Objetivos
1.1. Revisão dos conteúdos de informação Pública (Internet)	• Disponibilizar *dashboards* de informação pública da PSP atualizada relativa a: atividade, recursos, receita e despesa. • Disponibilizar georreferenciação pública PSP: esquadras, número de ocorrências por zona geográfica, outra. Esta informação poderá ser visualizada em conjunto com informação pública de outras entidades (GNR, SEF, ANEPC, ANSR, …)	• Permitir o acesso a informação pública PSP atualizada evitando a receção e o tratamento de pedidos por e-mail e a estatística a pedido. • O utilizador externo poderá, de forma autónoma, filtrar, analisar e extrair a informação em *dashboards*. • Partilhar informação pública georreferenciada em conjunto com outras entidades (GNR, SEF, ANEPC, ANSR, …) • Partilhar informação e conteúdos públicos, organizada e pesquisável.
1.2. Balcão Único Online PSP	• Conversão do portal externo PSP num ponto único de acesso externo, por cidadãos, entidades e parceiros, aos serviços PSP. O Balcão Único Online será *web first*, com autenticação Nacional e Europeia, com Atributos de Funcionário. • Integrar os sistemas da PSP com os sistemas de entidades externas, de forma a poder recolher, de forma consentida pelo requerente, dados mestre fidedignos. Auditoria de acessos, consultas, edições, remoções, atualizações. O ponto reencaminhará o utilizador para os diferentes formulários e aplicações de acesso externo, sem necessidade de nova autenticação.	• Atualizar tecnologicamente o acesso web e aumentar a segurança na autenticação e segmentação por perfis internos e externos. • Garantir conformidade com normas de acessibilidade e usabilidade. • Integrar os sistemas da PSP com os sistemas de entidades externas, de forma a poder recolher, de forma consentida pelo requerente, dados mestre fidedignos. • Registo auditável de acessos, consultas, edições, remoções e atualizações.

1.3. Melhoria da Qualidade de Dados	• Integrar os sistemas da PSP com os sistemas de entidades externas, para validação, limpeza e correção dos dados nos sistemas da PSP, por sua confrontação com os dados mestre fidedignos. • Aliviar e aumentar a eficiência das bases de dados operacionais, transferindo a informação antiga para histórico e criando informação resumo. Atender a prazos de conservação de arquivo digital. • Revisão dos sistemas da PSP para atender aos requisitos RGPD Europeus e Nacionais, nomeadamente: tratamento equitativo e lícito; limitação da finalidade; minimização dos dados e do seu prazo de conservação.	• Consulta de informação em dados mestre para limpeza e correção de dados existentes por: remoção ou junção de duplicados e semelhantes. • Implementação de processos ETL para a criação de informação estatística e resumo sobre: pessoa, entidade, objeto, localização. • Implementação de processos de transferência para histórico. • Implementação de processos RGPD, nomeadamente: a. Direitos ao acesso; Retificação; Apagamento; Limitação do tratamento; Portabilidade (à sua transferência para outra plataforma ou extração); b. SIS (Sistema de Informação Schengen); *VIS (Visa Information System)* e acordo *TFTP (Terrorist Finance Tracking System).*
1.4. Cartão Digital PSP	• Emissão de cartões eletrónicos digitais, 3 em 1, de colaborador PSP (polícia ou civil), de assistência à doença (colaborador e familiar) e de atributos de funcionário. • Atestando a sua autenticidade, integridade, validade e entidade emissora a nível Nacional e Europeu. E permitindo a atualização imediata de atributos de funcionário, utilizados para autenticação e autorização (atender ao seu perfil) e para a assinatura digital, a cada promoção, colocação ou alteração de funções. Verificação de licenças eletrónicas digitais.	• Desmaterializar a emissão de cartões PSP, cartão de assistência à doença de colaboradores e familiares e de gestão de perfis e acessos consoante a colocação ou funções. • Facilitar o acesso a utilizadores externos à PSP. • Desmaterializar e automatizar o processo de verificação da validade, autenticidade e integridade de um cartão e de um acesso. Poder cancelar, revogar, suspender, prolongar, renovar a validade ou atualizar o âmbito de uma autorização, a qualquer momento e com efeitos imediatos. • Oferecer portabilidade de acessos a nível europeu.
1.5. Gestão Documental	Permitir a existência de um identificador único para cada documento. Da mesma forma, o documento será arquivado, pelas áreas, em formato digital o que permitirá reduzir o espaço físico alocado a este objetivo e uma maior facilidade no acesso aos documentos, tanto pela área que elaborou o mesmo como pelas restantes áreas. De forma a garantir a confidencialidade dos documentos.	• Realizar a gestão de toda a informação em circulação de forma transversal – desde o registo ao armazenamento e à consulta bem como o controlo dos prazos de resposta. • Utilização de documentos eletrónicos ao invés de documentos físicos, desmaterializando os processos da PSP

1.6. Nova solução de licenciamentos	• Emissão de licenças, certificados e autorizações com certificados eletrónicos digitais, atestando a sua autenticidade, integridade, validade e entidade emissora a nível Nacional e Europeu. • Verificação de licenças eletrónicas digitais. • Integração com gestão documental no arquivo de documentos submetidos/ gerados.	• Desmaterializar a emissão de licenças, certificados e aprovações da responsabilidade da PSP. • Desmaterializar e automatizar o processo de verificação da validade, autenticidade e integridade de uma licença. O serviço passa a ser disponível a qualquer cidadão ou entidade com acesso ao serviço de verificação no site ou app do autenticação.Gov. • Poder cancelar, revogar, suspender, prolongar, renovar a validade ou atualizar o âmbito de uma licença, a qualquer momento e com efeitos imediatos. • Oferecer portabilidade de licenças a nível europeu.

B. Eixo 2: + Auto-Serviço

Iniciativas	Âmbito	Objetivos
2.1. Evolução da Intranet PSP	• Disponibilizar *dashboards* de informação interna privada da PSP atualizada relativa a: atividade, recursos, receita e despesa. • Disponibilizar georreferenciação: esquadras, número de ocorrências por zona geográfica, outra. • Definir e implementar um modelo de classificação de informação que permita a proteção de partilhada de informação sensível e confidencial.	• Permitir o acesso a informação atualizada e correta interna da PSP, em *dashboards* e relatórios, evitando a receção e o tratamento de pedidos por e-mail e a estatística a pedido. • Partilhar informação georreferenciada em conjunto com outras entidades (GNR, SEF, ANEPC, ANSR, …). • Operacionalizar as instruções para a segurança nacional, salvaguarda e defesa das matérias classificadas do Gabinete Nacional de Segurança no âmbito de Classificação de Informação em função do grau de confidencialidade (Muito Secreto, Secreto, Confidencial, Reservado). Criação de mecanismos de segurança (implementação de controlos de segurança e encriptação) que permitam a partilha de informação sensível e confidencial de forma segura utilizando meios digitais. Alinhar com requisitos legais e assegurar o correto acesso à informação. Assegurar a proteção de dados não estruturados (ex: documentos e emails). • Criação de mecanismos de geração e de disseminação segregada de informação.
2.2. App PSP (colaborador e familiar)	Disponibilização de App, para dispositivo móvel, para as seguintes funcionalidades: • serviço com viatura e consumo de combustível. (ESPAP) • pedido de ajudas de Investimento. • reembolso de despesas de saúde • pedido/ transferência logístico. • candidaturas a: concursos, colocações, formações, pré-aposentação, alojamento, bolsas de estudo, serviço externo remunerado; agendamento de ato médico, férias, ausências, escalas (acerto). • Aquisição de refeição em messe e bar.	• Disponibilizar um aplicativo móvel para Android e iOS, para auto-serviço. Mecanismos de plafonamento com autorização automática ou de alerta para aprovação manual. Verificação (auditoria interna) por amostragem. • Integração com gestão documental • Validação automática das faturas com AT. • Alimentação de *dashboards* e de relatórios (ex: relatório mensal de consumo de frota ESPAP; confrontação com fatura de cartões de combustível).

2.3. ERP RH, Financeiro e Patrimonial	• Facilitar e sincronizar informação entre sistemas internos PSP. • Gestão eficaz de património, bens e serviços. • Preparação de orçamentos, faturação, tesouraria, reconciliação bancária e contabilidade. Geração de mapas oficiais de reporte. • Capacidade de planeamento e gestão de todas as iniciativas/operações e recursos, com integração total com os módulos de RH, Financeiro e Patrimonial.	• Facilitar o processo de envio e receção de informação estruturada entre sistemas da PSP. • Permitir a gestão financeira autónoma de cada unidade orgânica e em simultâneo facilitar a sua consolidação, através de diversos mecanismos de automação e ajuda ao utilizador. • A integração de todos os processos num único sistema permite a simplificação do ciclo de aprovisionamento e a eliminação de Investimentos de gestão. Gerir de forma eficiente a aquisição de bens e serviços; • Gerir de forma eficiente a aquisição de bens e serviços, acompanhando todas as etapas do processo aquisitivo, desde a proposta de aquisição, consulta de fornecedores, receção de propostas e receção de bens e serviços. Simplificar o ciclo de aprovisionamento e eliminar Investimentos de gestão.
2.4. Implementação de Gestão Académica	• Gestão integrada da vida académica do colaborador interno ou externo, desde a sua candidatura e processo de triagem; passando pela sua formação, examinação e certificação; até ao planeamento de formação de atualização ou de renovação de certificação ao longo da sua vida ativa. Disponibilização de solução de examinação *proctored online*, com capacidade de agendamento e de parametrização de exames e de lotes de questões. • Emissão de certificados digitais (fidedignos, autênticos, verificáveis, partilháveis, atualizáveis e revogáveis).	• Disponibilizar uma solução de gestão académica (LMS – *Learning Management System*) ao Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI) • Detetar necessidades e competências e assim influenciar o desempenho dos colaboradores e os resultados da organização.

C. Eixo 3: + Cooperação

Iniciativas	Âmbito	Objetivos
3.1. Implementação da Extranet PSP	• Criação de um novo ponto de acesso web a Extranet PSP, *web first*, com autenticação Nacional e Europeia, com Atributos de Funcionário. • Integrar os sistemas da PSP com os sistemas de entidades externas, de forma a poder recolher, de forma consentida pelo requerente, dados mestre fidedignos. • Auditoria de acessos, consultas, edições, remoções, atualizações. • O ponto reencaminhará o utilizador para as diferentes aplicações, sem necessidade de nova autenticação.	• Atualizar tecnologicamente o acesso *web* e aumentar a segurança na autenticação e segmentação por perfis internos e externos. • Integrar os sistemas da PSP com os sistemas de entidades externas, de forma a poder recolher, de forma consentida pelo requerente, dados mestre fidedignos. • Instrumentar a aplicação atual com vista ao registo auditável de acessos, consultas, edições, remoções e atualizações.
3.2. Ação de Fiscalização/ Contraordenação	• Utilização do novo *backoffice* PSP, *web first*, para agilização do registo de auditorias iniciais e de ações de fiscalização, incluindo a comunicação com utilizadores externos (regulados, parceiros de fiscalização e entidades reguladoras). Registo e acompanhamento de contraordenações. Integração com gestão documental no arquivo de documentos submetidos/ gerados. • Parametrização de *checklists* e de respostas a não conformidades por tipo de licença. Planeamento e monitorização de ciclos de auditoria e fiscalização. • *Dashboards* de monitorização de ciclos de supervisão e de estatísticas de fiscalização por tipo, unidade orgânica, entidade/ objeto, localização, receita e período de análise.	• Suporte aplicacional *web first* às deslocações no âmbito de auditorias e fiscalizações. Capacitar os inspetores a preencher *checklists* e a registar não conformidades no terreno. Integração com gestão documental. • Disponibilizar *web service* ou acesso a utilizador: consulta da *checklist* de fiscalização, registo de plano de ações corretivas, envio de documentação ou de evidências de correções efetuadas. • Preenchimento automático de formulário de contraordenação por cada entidade competente, com base nos registos e relatório de fiscalização. Se entidade competente não for a PSP, envio da contraordenação por *web service*. Suporte ao acompanhamento da contraordenação. • Disponibilizar *dashboards* de monitorização de ciclos de supervisão e de estatísticas de fiscalização por tipo, unidade orgânica, entidade/ objeto, localização, receita e período de análise.

3.3. Nova solução de gestão de ocorrências	• Integrar os sistemas da PSP com os sistemas do MAI e MJ, de forma a poder enviar/ receber informação de forma estruturada e atualizada, para a sincronização de informação entre sistemas. • *No novo backoffice* PSP, registo (*web first*) de ocorrências no terreno, em formulário e relatório genéricos e flexíveis (com campos parametrizáveis e pesquisáveis) e acompanhando tempestivamente alterações legislativas. Integração com gestão documental. • Alimentação de *dashboard* de ocorrências, por tipo, unidade orgânica e período de análise.	• Criação de *web services* de integração de sistemas PSP com sistemas do MAI e MJ, facilitando o processo de envio e receção de informação estruturada e a atualização do estado dos processos. • Disponibilizar no novo *backoffice* PSP, a funcionalidade de registo de ocorrência. • Integração com gestão documental para arquivo digital de documentos associados. • Disponibilizar um *dashboard* de estatísticas de ocorrências por tipo, estado, unidade orgânica e período de análise.
3.4. Nova solução de Gestão Meios e Planeamento	• Fornecer capacidades superiores de gestão de incidentes/ocorrências no ponto de atendimento de segurança pública (PSAP), sala de controlo de emergência, estação, unidade ou em qualquer lugar onde os operacionais precisem de ir. • Garantir uma resposta segura, eficiente e eficaz, ligando os operacionais no terreno às salas de controlo e aos supervisores para uma consciencialização, comunicação e coordenação das operações.	• Os intervenientes podem tomar medidas seguras e eficazes e manter as salas de controlo informadas do seu estado e localização, independentemente do local onde se encontrem. • Proporcionar uma melhor experiência de utilização, tomada de decisão mais informada, fluxos de trabalho mais simples e uma maior consciência situacional, sem sobrecarregar o operador. ✓ Atendimento de Chamadas e Criação de Incidentes/Ocorrências ✓ Recomendação e Despacho de Meios ✓ Mobilidade
3.5. Implementação de solução CRM com pesquisa global	• Integrar os sistemas da PSP com os sistemas de entidades externas, de forma a poder obter uma Visão 360º ou pesquisa global integrada e relacionada sobre um objeto ou entidade. • Capacidade de criação de relacionamentos entre entidades e objetos. • Capacidade de mapear esses relacionamentos através de uma solução de CRM.	• Criação de *web services* de consulta de informação em entidades externas sobre entidades, objetos e suas relações. • Criação de equivalências entre os tipos de objetos de distintas entidades. • Criação de interface de pesquisa global integrada em múltiplos sistemas internos e externos, com capacidade de segmentação/ segregação da informação por utilizador e perfis/entidades a que está associado.

D. Eixo 4: + Infraestruturas

Iniciativas	Âmbito	Objetivos
4.1. Desenvolvimento da Arquitetura tecnológica e comunicações	• Implementação de uma política adequada de armazenamento de dados, ultrapassando as atuais limitações verificadas, devido às faltas de espaço nos suportes, o que faz com que o sistema operacional se encontre em "*Near Real Time*". • Ainda, para a salvaguarda da informação, é necessária a implementação de uma política adequada de salvaguarda de dados (*backup e restore*).	• Garantir espaço para o armazenamento dos dados da PSP, de forma eficaz e eficiente, sem que haja limitações de espaço ou velocidade de resposta na recuperação, atingindo ou aproximando o sistema operacional de resposta em "*Real Time*". • Garantir que todos os dados relevantes sejam armazenados num local seguro, para recuperação adequada e em tempo útil, em caso de falha ou de corrupção de dados.
4.2. Melhoria dos ativos e serviços de alojamento	• Aquisição de novos servidores para responder às necessidades atuais e futuras da PSP. • Definição da arquitetura de SI, COM e dados e mecanismos de interoperabilidade. • Instalação de redes WiFi nas esquadras e nas escolas EPP e ISCPSI.	• Adquirir novo servidores para servir as necessidades departamentais, dotando a PSP com uma arquitetura tecnológica moderna que responda aos desafios de atualização resultantes da evolução dos sistemas e que permita otimizar os recursos. • Disponibilizar acessos WiFi a computadores autorizados nas esquadras, e nas escolas, assegurando todos os mecanismos de segurança necessários à sua boa operacionalização e funcionamento.
4.3. Melhoria Gestão de Acessos e de Identidades	• Implementar um processo de Gestão de Identidades e Acessos (IAM) para os sistemas e ferramentas geridos pela PSP.	• Restringir acessos indevidos a informação; • Definir níveis de permissão de acesso distintos de acordo com o perfil do utilizador; • Melhorar a segurança da informação; • Automatizar o processo de gestão de acessos e permissões; • Monitorizar os acessos; • Melhorar o processo de concessão, revisão e revogação de acessos.

4.4. Implementação de política Bring Your Own Device (BYOD)	• Implementar uma política de BYOD (*Bring Your Own Device*) que permita aos trabalhadores da PSP utilizar os seus próprios dispositivos de forma segura para a realização de atividades profissionais. • Implementação de mecanismos de segurança que diminuam o risco de utilização (*Multi-Factor Authentication (MFA), Mobile Device Management (MDM),* Encriptação).	• Aumento da flexibilidade do acesso a ferramentas corporativas fora das instalações da PSP; • Reduzir a necessidade da utilização de dispositivos corporativos para acesso a informação profissional; • Reduzir investimentos de aquisição de equipamento; • Eliminar a utilização de ferramentas não corporativas/alternativas para o uso profissional; • Aumentar a produtividade.
4.5. Implementação solução de observabilidade	• Definir um sistema de monitorização e controlo e, ainda a definição de sistemas de redundância, *backups*, entre outros. • Permitir o controlo de versões, com repositório para artefactos, código e configurações. • Ainda, é importante a gestão de configurações e instalações, de modo a garantir a emissão de certificados, redundância e segregação aplicacional, o aumento de desempenho e escalabilidade, etc.	• Melhoria na monitorização de negócio e alarmística (*dashboards, logs*, alertas). • Implementar infraestrutura para e criar testes automáticos. • Utilização de ferramentas de controlo de segurança e qualidade de código. • Definir automatismos para escalar as aplicações: horizontalmente (mais máquinas/*containers* iguais); verticalmente (aumentar recursos de máquina/*container* (memória, armazenamento, ...) • Garantir a continuidade do negócio.

E. Eixo 5: + Eficácia

Iniciativas	Âmbito	Objetivos
5.1. Novo Modelo de Governação DSIC	• Aprovar e implementar a proposta para a nova estrutura organizacional para o DSIC. Contratação de RH para o quadro, ou da prestação de serviços em continuidade, para preenchimento das necessidades funcionais decorrentes da implementação da nova estrutura organizacional. • Criação de um Gabinete de Gestão de Projetos, com recursos qualificados. • Criação de uma equipa de Governação, Standards e Qualidade da Informática, com pessoal qualificado e de uma equipa de Segurança Informática, com pessoal qualificado.	Aprovar e implementar o novo modelo organizacional para o DSIC tendo em vista: • Clarificação das atribuições de cada área e aumento da especialização, em linha com as tendências de mercado • Prestação de serviços orientada para o cliente interno e externo, melhoria da qualidade do serviço prestado e aumento da agilidade na resposta às necessidades • Criação de uma área para prevenção e proteção contra todo o tipo de risco aos ativos de TI, seja Físico ou Digital, através da implementação de controlos físicos, administrativos e técnicos.
5.2. Revisão do modelo de custeio da implementação do PESI	• Criação de um modelo de sustentabilidade que promova a adoção, de soluções digitais – menos onerosas (em esforço e meios), por cidadãos, empresas e parceiros e que reparta o seu Investimento pelos beneficiários (rentabilização).	• Aumento da eficácia e eficiência da utilização dos sistemas de informação na PSP, de modo sustentável e contínuo; • Rentabilização das novas soluções digitais.
5.3. Melhoria das Práticas de Segurança SI e Compliance	• Definir e implementar todos os principais *frameworks* e melhores práticas para assegurar o sucesso da gestão e execução dos serviços prestados pelo DSIC.	• Assegurar a identificação e adoção de *frameworks* e melhores práticas de gestão e execução de serviços de informática, tais como: Implementação ágil/SCRUM; Cobit; ITIL; ISO 27001, Lean IT. • Controlo de Qualidade: ✓ Segregar ambientes aplicacionais (produção, qualidade, testes, desenvolvimento); ✓ *Canary Releases* – entrega a utilizadores restritos; ✓ Melhorar o envolvimento dos *stakeholders* no levantamento de requisitos

5.4. Melhoria do Controlo e comunicação de SLAs	• Implementação de processos e mecanismos de monitorização e controlo dos níveis de serviço definidos (SLAs).	• Definição e cumprimento de níveis de serviço (SLAs); • Garantia de maior envolvimento dos recursos na concretização dos objetivos da PSP;

4.4. Priorização das iniciativas

A priorização das iniciativas identificadas é essencial para a construção do *roadmap.* Deste modo, foram classificadas as iniciativas de acordo com cinco critérios: os benefícios que traz para a organização, a abrangência que os resultados terão na PSP, a satisfação que trará aos colaboradores, o impacto das melhorias no cliente externo, e facilidade de operacionalização da iniciativa. Cada critério foi avaliado consoante o seu impacto e o grau de urgência. Estas iniciativas foram distribuídas pelo período de quatro anos de acordo com a sua classificação, sendo que as iniciativas com uma classificação entre 25 e 30 pontos foram colocadas no 1º ano; as iniciativas com classificação entre 20 e 24, no 2º ano; as iniciativas com pontuação entre 15 e 19 inseriram-se no 3º ano; e, por fim, as restantes foram alocadas ao 4º ano.

A tabela x reflete os resultados da priorização, assim como a estimativa do investimento e duração de cada uma das iniciativas e a avaliação do panorama atual da PSP em comparação com as iniciativas sugeridas. Nesta avaliação, 1 significa que é inexistente, 2 significa que está obsoleto e 3 significa que algo equivalente está em uso, mas necessita de melhorias/*upgrades* ou substituição de uma nova solução.

Eixo	Iniciativa	*AS-IS*	Total	Prioridade	Investimento	Duração
1. + Digital	1.1. Revisão dos conteúdos de informação Pública (Internet)	3	22	2ª	100k – 150k €	6 a 12 meses
	1.2. Balcão Único *Online* PSP	1	24	2ª	300k – 350k €	10 a 12 meses
	1.3. Melhoria na Qualidade de Dados	1	19	3ª	140k – 180k €	13 a 16 meses
	1.4. Cartão digital PSP	1	18	3ª	40k – 60k €	6 a 9 meses
	1.5. Gestão Documental	2	26	1ª	160k - 200k €	12 a 18 meses
	1.6. Nova solução de Licenciamentos	3	14	4ª	150k - 200k €	9 a 12 meses
2. + Auto-Serviço	2.1. Evolução Intranet PSP	3	25	1ª	260k – 300k €	18 a 24 meses
	2.2. App PSP (colaborador e familiar)	1	22	2ª	110k - 140k €	4 a 6 meses
	2.3. Implementação de ERP (RH, Financeiro e Patrimonial)	3	26	1ª	840k - 990k €	9 a 12 meses
	2.4. Implementação de Gestão Académica	2	17	3ª	40k - 70k €	5 a 8 meses
3. + Cooperação	3.1. Implementação de Extranet	1	19	3ª	60k – 90k €	5 a 7 meses
	3.2. Ação de Fiscalização / Contraordenação	3	14	4ª	280k – 310k €	7 a 9 meses
	3.3. Nova solução de gestão de ocorrências	3	13	4ª	650k – 750k €	9 a 12 meses
	3.4. Nova solução de Gestão Meios e Planeamento	1	25	1ª	5,3M – 5,5M €	9 a 18 meses
	3.5. Implementação de solução CRM com pesquisa global	1	20	2ª	400k – 500k €	9 a 12 meses
4. + Infraestrutura	4.1. Desenvolvimento da Arquitetura tecnológica e comunicações	1	25	1ª	400k – 420k €	4 a 6 meses
	4.2. Melhoria dos ativos e serviços de alojamento	3	18	3ª	4,6M – 5,1M €	18 a 24 meses
	4.3. Melhoria Gestão de Acessos e de Identidades	3	20	2ª	120k - 160k €	6 a 8 meses
	4.4. Implementação de política *Bring Your Own Device* (BYOD)	1	14	4ª	150k – 180k €	6 a 12 meses
	4.5. Implementação solução de observabilidade	1	16	3ª	1,3M – 1,5M €	6 a 8 meses
5. + Eficácia	5.1. Novo Modelo de Governação DSIC	3	25	1ª	60k – 90k €	6 a 9 meses
	5.2. Revisão do modelo de custeio da implementação PESI	1	13	4ª	60k - 75k €	4 a 8 meses
	5.3. Melhoria das Práticas de Segurança SI e *Compliance*	1	20	2ª	180k – 250k €	18 a 24 meses
	5.4. Melhoria do Controlo e comunicação de SLAs	1	26	1ª	35k - 60k €	3 a 5 meses

Tabela 1 - Quadro resumo da priorização das iniciativas

5. Roadmap

5.1. *Quick Wins*

Os *quick wins* são uma questão fundamental para a implementação deste projeto. Os *quick wins* são caracterizados por terem baixa complexidade de implementação e médio/alto potencial de ganhos para o negócio:

Melhoram o desempenho dos processos: Ao serem utilizadas corretamente, os *quick wins* podem aumentar a rentabilidade e produtividade da empresa, pois aceleram a execução de projetos/processos/fluxos e reduzem custos.

Implementação simples: Como o nome sugere, a implementação dos *quick wins* é um processo rápido e simples, isto é, não se trata de um grande projeto. Além disso, pela baixa complexidade, esse tipo de otimização tende a ter boa aceitação entre as equipas envolvidas.

Redução de riscos: Por se tratar de soluções não tão complexas, os *quick wins* geralmente não oferecem riscos elevados ao negócio durante a implementação ou depois dela.

Pontual ou localizado: Os *quick wins* são aplicadas num determinado local do processo. Geralmente, num ponto menor, mas que permite gerar resultado imediato.

Menor custo: Em alguns casos os investimentos necessários para fazer os *quick wins* são até nulos. Portanto, outra característica marcante são os baixos custos.

5.2. *Roadmap* de implementação

Para apoiar a implementação do projeto, é recomendada a utilização de *frameworks* ágeis de gestão de projetos. São sugeridas as seguintes:

- A *framework* Scrum é baseado em pilares e papéis bem definidos, permitindo a participação dos clientes na equipa de desenvolvimento e validação das entregas. Esta *framework* utiliza *sprints* (ciclos de desenvolvimento) para garantir qualidade nas entregas e flexibilidade na mudança de requisitos. Isso reduz os riscos, pois os progressos e atrasos são monitorizados. Os princípios do Scrum incluem transparência, inspeção e adaptação.
- A metodologia *Kanban* é um conjunto de princípios e práticas observados em iniciativas de sucesso em todo o mundo. Este método permite maior agilidade nas organizações, abraçando a mudança constante na gestão do trabalho do conhecimento. O *Kanban* promove a gestão à vista, o desenvolvimento adaptativo e os estágios de trabalho para possibilitar a melhoria contínua.

Estes *frameworks* ágeis fornecem estruturas eficazes para priorização, monitorização e entrega de projetos, permitindo que as organizações se tornem mais colaborativas, unificadas e produtivas num ambiente de mudança constante.

O *Roadmap* geral e o *Roadmap* com as *quick wins* são apresentados na Tabela 2 e na Tabela 3.

Eixo	Iniciativa	Total	Prioridade	2024	2025	2026	2027	Implementação
1. + Digital	1.1. Revisão dos conteúdos de informação Pública (Internet)	22	2ª		100k – 150k €			6 a 12 meses
	1.2. Balcão Único *Online* PSP	24	2ª		300k – 350k €			10 a 12 meses
	1.3. Melhoria na Qualidade de Dados	19	3ª		50k – 70k €	90k – 110k €		13 a 16 meses
	1.4. Cartão digital PSP	18	3ª			40k – 60k €		6 a 9 meses
	1.5. Gestão Documental	26	1ª	160k - 200k €				12 a 18 meses
	1.6. Nova solução de Licenciamentos	14	4ª				150k - 200k €	9 a 12 meses
2. + Auto-Serviço	2.1. Evolução Intranet PSP	25	1ª	260k – 300k €				18 a 24 meses
	2.2. App PSP (colaborador e familiar)	22	2ª		110k - 140k €			4 a 6 meses
	2.3. Implementação de ERP (RH, Financeiro e Patrimonial)	26	1ª	600k - 750k €		120k €	120k €	9 a 12 meses
	2.4. Implementação de Gestão Académica	17	3ª			40k - 70k €		5 a 8 meses
3. + Cooperação	3.1. Implementação de Extranet	19	3ª			60k – 90k €		5 a 7 meses
	3.2. Ação de Fiscalização / Contraordenação	14	4ª			230k – 260k €	50k €	7 a 9 meses
	3.3. Nova solução de gestão de ocorrências	13	4ª				650k – 750k €	9 a 12 meses
	3.4. Nova solução de Gestão Meios e Planeamento	25	1ª	3,4M – 3,6M €	625k €	625k €	625k €	9 a 18 meses
	3.5. Implementação de solução CRM com pesquisa global	20	2ª		400k – 500k €			9 a 12 meses
4. + Infraestrutura	4.1. Desenvolvimento da Arquitetura tecnológica e comunicações	25	1ª	400k – 420k €	*1	*1	*1	4 a 6 meses
	4.2. Melhoria dos ativos e serviços de alojamento	18	3ª			2,3M – 2,6M €	2,3M – 2,6M €	18 a 24 meses
	4.3. Melhoria Gestão de Acessos e de Identidades	20	2ª		120k - 160k €			6 a 8 meses
	4.4. Implementação de política *Bring Your Own Device* (BYOD)	14	4ª				150k – 180k €	6 a 12 meses
	4.5. Implementação solução de observabilidade	16	3ª			1,3M – 1,5M €	*2	6 a 8 meses
5. + Eficácia	5.1. Modelo de Governação DSIC	25	1ª	60k – 90k €				6 a 9 meses
	5.2. Revisão do modelo de custeio do PESI	13	4ª				60k - 75k €	4 a 8 meses
	5.3. Melhoria das Práticas de Segurança SI e *Compliance*	20	2ª		120k – 160k €	60k – 90k €		18 a 24 meses
	5.4. Melhoria do Controlo e comunicação de SLAs	26	1ª	35k - 60k €				3 a 5 meses
Totais				4,9M – 5,4M €	1,8M – 2,2M €	4,9M – 5,5M €	4,1M – 4,6M €	15,7M – 17,7M €

*1 - Manutenção incluída

*2 – licenciamento SaaS incluído para 36 meses

Tabela 2 - Roadmap detalhado de implementação

Eixo	Iniciativa	Total	Prioridade	2024	2025	2026	2027	Implementação
1. + Digital	1.1. Revisão dos conteúdos de informação Pública (Internet)	22	2ª					6 a 12 meses
	1.2. Balcão Único Online PSP	24	2ª					10 a 12 meses
	1.3. Melhoria na Qualidade de Dados	19	3ª					13 a 16 meses
	1.4. Cartão digital PSP	18	3ª					6 a 9 meses
	1.5. Gestão Documental	26	1ª	1.5.1 1.5.2				12 a 18 meses
	1.6. Nova solução de Licenciamentos	14	4ª					9 a 12 meses
2. + Auto-Serviço	2.1. Evolução Intranet PSP	25	1ª	2.1.1 2.1.2 2.1.3 2.1.4				18 a 24 meses
	2.2. App PSP (colaborador e familiar)	22	2ª		2.2.1			4 a 6 meses
	2.3. Implementação de ERP (RH, Financeiro e Patrimonial)	26	1ª	2.3.1 2.3.2 2.3.3				9 a 12 meses
	2.4. Implementação de Gestão Académica	17	3ª					5 a 8 meses
3. + Cooperação	3.1. Implementação de Extranet	19	3ª			3.1.1 3.1.2 3.1.3		5 a 7 meses
	3.2. Ação de Fiscalização / Contraordenação	14	4ª			3.2.1		7 a 9 meses
	3.3. Nova solução de gestão de ocorrências	13	4ª				3.3.1 3.3.2	9 a 12 meses
	3.4. Nova solução de Gestão Meios e Planeamento	25	1ª	3.4.1				9 a 18 meses
	3.5. Implementação de solução CRM com pesquisa global	20	2ª		3.5.1			9 a 12 meses
4. + Infraestrutura	4.1. Desenvolvimento da Arquitetura tecnológica e comunicações	25	1ª					4 a 6 meses
	4.2. Melhoria dos ativos e serviços de alojamento	18	3ª			4.2.1		18 a 24 meses
	4.3. Melhoria Gestão de Acessos e de Identidades	20	2ª					6 a 8 meses
	4.4. Implementação de política *Bring Your Own Device* (BYOD)	14	4ª				4.4.1	6 a 12 meses
	4.5. Implementação solução de observabilidade	16	3ª					6 a 8 meses
5. + Eficácia	5.1. Modelo de Governação DSIC	25	1ª					6 a 9 meses
	5.2. Revisão do modelo de custeio do PESI	13	4ª					4 a 8 meses
	5.3. Melhoria das Práticas de Segurança SI e Compliance	20	2ª					18 a 24 meses
	5.4. Melhoria do Controlo e comunicação de SLAs	26	1ª					3 a 5 meses

X.X.X - Quick wins (ver descrição no slide seguinte)

- Possível extensão do período de implementação.

Tabela 3 - Roadmap de implementação com quick wins

Lista de *quick wins*:

Eixo 1:

1.5.1: Implementação da etapa de captura de documentos

1.5.2: Etapa de identificação, classificação e criação de formulários.

Eixo 2:

2.1.1: Criação de nova versão do relatório de estatísticas por atividade (incluindo registos ainda não validados pela hierarquia).

2.1.2: Reformulação dos relatórios estatísticos que apresentam duplicados.

2.1.3: Disponibilização de *dashboard* de informação interna PSP atualizada relativa a: atividade, recursos, distribuição da receita e despesa. Acessos específicos para entidades externas.

2.1.4: Alojamento e partilha segura de informação confidencial e sensível, da Investigação Criminal, Divisão de Segurança da Informação e Deontologia e Disciplina.

2.2.1: Disponibilização de app para dispositivo móvel, com autenticação com CMD (autenticação.Gov) e atributos de Funcionário, para acesso *mobile-ready* a *backoffice* PSP.

2.3.1: Extração mensal de mapa de vencimentos GIRe para integração no SIREC.

2.3.2: *Web service* de integração da receita entre sistemas SIGAE-SIREC.

2.3.3: *Web service* de integração das remunerações entre sistemas SEI e SIREC.

Eixo 3:

3.1.1: Criação de novo ponto de acesso *backoffice* PSP, com autenticação 2-fatores Nacional e Europeia (autenticação.Gov).

3.1.2: Estabelecimento de protocolos e integração com Autenticação.Gov para recolha de dados mestre de outras entidades: IRN, SEF, SS, AT.

3.1.3: Reencaminhamento (sem nova autenticação) para diferentes aplicações *backoffice* PSP.

3.2.1: Permitir um fluxo de trabalho flexível e iterativo. O relatório de auditoria/fiscalização deverá poder ser gerado sempre que se pretende.

3.3.1: Atualização do *web service* de envio de ocorrências, para a base de dados de violência doméstica (incluir aditamentos).

3.3.2: Atualização do *web service*, com o CITIUS, de envio/receção de estado de processo-crime.

3.4.1: Implementação da plataforma de gestão incidentes/ocorrências e meios, com os requisitos principais a serem definidos pela PSP.

3.5.1: Implementação de interface de pesquisa global integrada interna: SEI, SIGAE, SIGESP, SerOnline e SIGESP Online.

Eixo 4:

4.2.1: Instalar equipamentos de WiFi nas esquadras, comandos e escolas EPP

4.4.1: Definir os trabalhadores abrangidos pela política de BYOD;

5.3. Recrutamento e formação

Destaca-se que atualmente a PSP não possui capacidade de contratar recursos para o quadro da entidade, sendo necessário considerar a contratação de entidades externas para suprimir essa necessidade. No entanto, existem funções mais confidenciais que devem preferencialmente ser ocupadas por recursos internos da PSP, a fim de evitar a externalização. Além disso, é importante garantir a qualificação e capacitação dos recursos internos, visando prepará-los para enfrentar os desafios crescentes e contribuir para a retenção e transmissão interna do conhecimento. Isto pode aumentar a atratividade das posições disponíveis e melhorar a atração e retenção de talentos.

Para avaliar a situação atual do Departamento de Sistemas de Informação e Comunicações (DSIC) da PSP em termos de capacitação, experiência e necessidades dos recursos humanos, foi aplicado um questionário que obteve 18 respostas. Dos colaboradores que responderam, 17% são especialistas em Informática, enquanto os demais (83%) possuem o grau de Técnico de Informática. Todos têm mais de 10 anos de experiência na área.

Em relação à formação de base, os resultados mostram que 6 participantes têm o 12º ano de escolaridade, 6 têm uma licenciatura e 2 possuem formação profissional na área de Informática. Quanto a ações de formação e certificados, 70,6% dos participantes já frequentaram algum curso ou formação relacionada com suas atividades, e 73,3% possuem algum certificado de formação em domínios da Informática. O interesse em realizar outras tarefas na área de Informática, diferentes das atividades atuais, é baixo entre os colaboradores do DSIC. A maioria (73,3%) não tem interesse em mudar de atividade, mas os que têm mostraram preferências diversas, como estratégia e planeamento (2), exploração de informação e suporte à decisão (1), comunicações rádio (1), administração de sistemas e infraestruturas (3), desenvolvimento e manutenção (1), segurança informática (2), *service desk* (2) e gabinete de projeto (2).

Com o intuito de aumentar a atratividade das posições sugeridas, a PSP deve abordar as limitações existentes no modelo de contratação, que tornam o setor público menos competitivo para atrair e reter talentos. Algumas das lacunas apontadas são a competição no mercado por perfis de tecnologia, as condições pouco atrativas em relação a salários e flexibilidade de trabalho, a infraestrutura tecnológica antiquada e a elevada média de idades da equipa. Para contornar essas limitações, é sugerido que a PSP avalie a possibilidade de contratar a prestação de serviços em continuidade, tanto com recursos internos como com recursos do mercado (contratação vs *outsourcing*), dependendo do nível de confidencialidade do trabalho e da informação envolvida em cada perfil. O plano de recrutamento e formação deve contemplar o desenvolvimento dos trabalhadores da PSP interessados em Informática, por meio do *upskilling* e *reskilling*, além de buscar recursos no mercado através de diferentes soluções, como o BEP (Bolsa de Emprego Público), recrutamento de civis ou *outsourcing* de serviços.

Conforme reforçado anteriormente, existem perfis que, pelo seu nível de confidencialidade e sensibilidade da informação, não podem ser externalizados, logo têm de ser garantidos por recursos da PSP.

Logo, de acordo com a nova estrutura organizacional proposta, tem-se a seguinte proposta de recrutamento dos perfis

Área do DSIC	Perfil	Recursos internos (Capacitação ou contratação)	*Outsourcing*	Notas
N/A	Diretor do DSIC	X		Recurso de extrema importância, sendo o principal responsável pela definição e operacionalização da estratégia do DSIC
Estratégia e Planeamento	Consultor Estratégico	X	X	Estes perfis poderão ser garantidos tanto por recursos internos ou com o recurso à externalização do serviço
	Business Architect	X	X	Estes perfis poderão ser garantidos tanto por recursos internos ou com o recurso à externalização do serviço
Administração de Sistemas e Infraestruturas	Administrador de Base de Dados	X		
	Administrador de Redes	X	X	Estes perfis poderão ser garantidos tanto por recursos internos ou com o recurso à externalização do serviço
	Administrador de Sistemas	X		
	Responsável de Backups	X	X	Estes perfis poderão ser garantidos tanto por recursos internos ou com o recurso à externalização do serviço
Manutenção de Sistemas	Analista funcional	X	X (algum projeto em específico)	
	Programador	X	X (algum projeto em específico)	
	Especialista de Testes e Documentação	X	X (algum projeto em específico)	
	UX/UI Designer	X	X (algum projeto em específico)	
	Analista de BI	X	X (algum projeto em específico)	
	Product Owner	X	X (algum projeto em específico)	
Segurança Informática	Cibersecurity Implementer (Analista)	X		
	Cibersecurity Implementer (Engenheiro)	X		
	Penetration Tester (Hacker Ético)	X		

Tabela 4 - Perfis de recrutamento

Área do DSIC	Perfil	Recursos internos (Capacitação ou contratação)	*Outsourcing*	Notas
Service Desk	Supervisor da equipa	X	X	Estes perfis poderão ser garantidos tanto por recursos internos ou com o recurso à externalização do serviço
	Técnico de Help Desk	X	X	
Gabinete de Projetos	Gestor de projetos	X	X	Este perfil pode ser garantido por um recurso interno ou por um recurso externo.
Governação e Qualidade	Gestor da Qualidade de processos TIC (Esp. em frameworks de Governação: COBIT, ITIL, PMI, Dados, etc)	X		
	Auditor de IT		X	Tendo em conta o carácter de independência adjacente ao perfil (na qualidade de auditor), poderá ser considerada a opção de externalizar este perfil.
Exploração de Informação e Suporte à Decisão	Data Scientist / Perito em BI	X		
Comunicações – Rádio	Especialista Eletricista	X		Este perfil atualmente tem sido garantido por recursos internos da PSP.
	Supervisão da Exploração de Comunicações	X		Este perfil atualmente tem sido garantido por recursos internos da PSP.
	Exploração de Comunicações	X		Este perfil atualmente tem sido garantido por recursos internos da PSP.
	Manutenção de equipamentos de comunicações	X		Este perfil atualmente tem sido garantido por recursos internos da PSP.
	Manutenção de redes de informática e comunicações	X		Este perfil atualmente tem sido garantido por recursos internos da PSP.
	Gestão de Meio e equipamentos	X		Este perfil atualmente tem sido garantido por recursos internos da PSP.

Tabela 5 - Perfis de recrutamento (cont.)

Para cada um dos perfis recomendados, devem ser desenvolvidas ações de capacitação e aumento de competências, de modo a estarem aptos para dar resposta a todos os desafios. Para materializar a estrutura proposta para o DSIC, é necessário assegurar um conjunto de novos perfis e competências que possam ir de encontro às necessidades e desafios inerentes à nova estrutura proposta. Logo, a absorção das novas competências só é possível com ações de formação e capacitação dos recursos humanos da PSP. Para cada perfil proposto, é sugerido um conjunto de formações e certificados que podem contribuir para criação de valor, detalhado no entregável da fase 5 – *Roadmap*.

5.4. Dimensionamento do DSIC

De modo a dar resposta à nova estrutura organizacional proposta e colmatar algumas limitações verificadas no DSIC, é recomendado um dimensionamento do departamento e dos recursos humanos necessários, de modo a estarem enquadrados com a nova estrutura proposta e alinhados com as metas que a PSP pretende atingir no ramo das tecnologias de informação.

Para o dimensionamento das áreas e perfis recomendados para o DSIC, foi feito um levantamento dos recursos humanos necessários para cada perfil (associado ao entendimento da situação atual e necessidades futuras). Conforme apresentado no capítulo anterior, existem alguns perfis que podem ser alocados com base à externalização (*outsourcing*) e outros, pela natureza das suas competências, devem ser garantidos por recursos internos. Este dimensionamento está detalhado no entregável da fase 5 – *Roadmap*, sendo que a proposta de estruturação do DSIC, com perfis associados a cada uma das áreas propostas, é a seguinte.

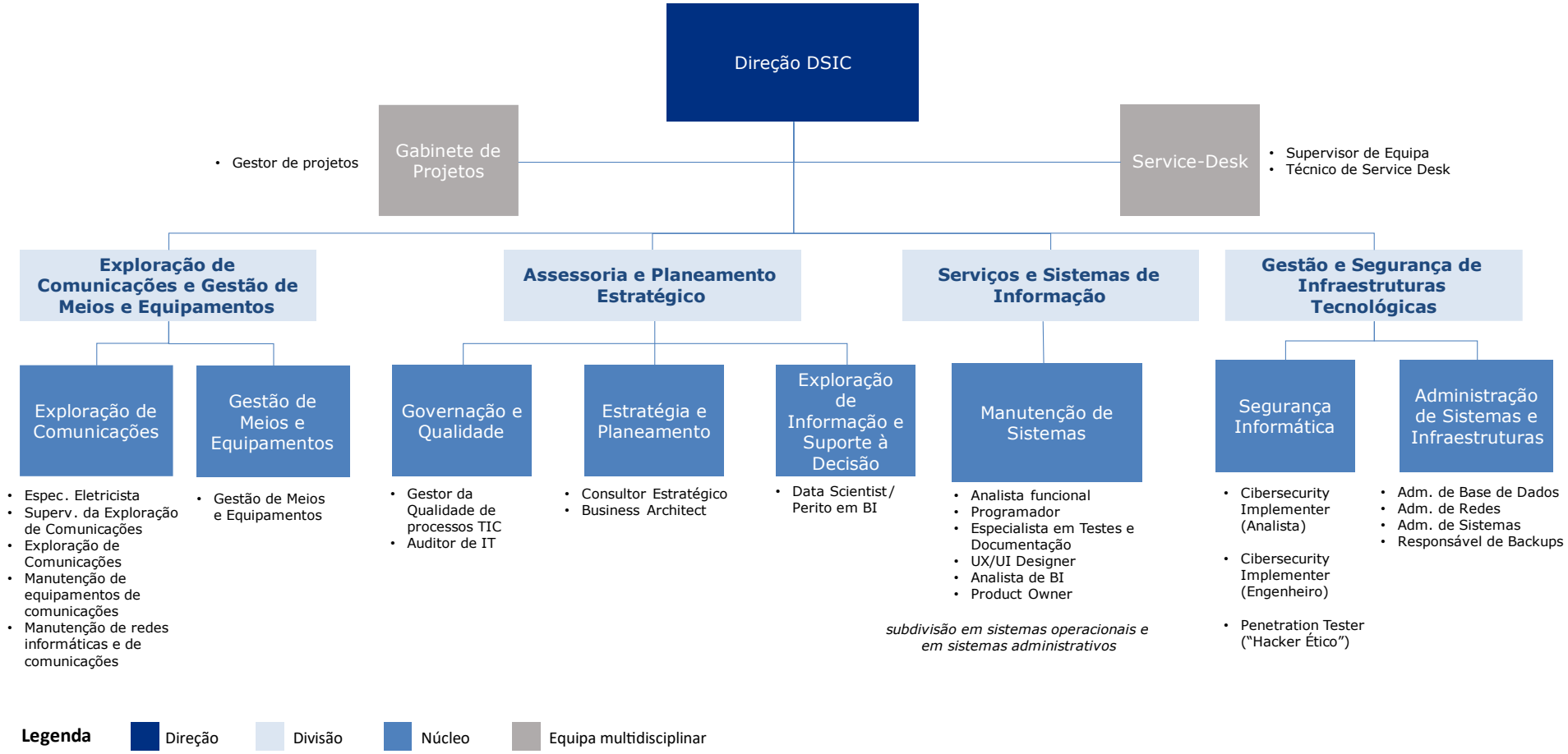

Tabela 6 - Organograma DSIC proposto

5.5. Fatores Críticos de Sucesso

Com vista a dar seguimento ao presente trabalho com sucesso, foram definidos os seguintes fatores cruciais:

Equipa de Projeto	•Liderança de um gestor de projeto da PSP, preferencialmente alguém de alta hierarquia com influência sobre vários departamentos e várias pessoas. •Externalização dos restantes membros da equipa, recorrendo a serviços de PMO, visto que o trabalho requererá um acompanhamento direto a tempo inteiro ao longo da implementação das diferentes iniciativas.
Apoio Alto-Nível	•Apoio Alto-Nível politíco por parte de entidades públicas que poderão colaborar com a PSP neste processo (AMA, MAI, CEGER, ANS,...) •Apoio Alto-Nível interno por parte das hierarquias da PSP.
Recursos Humanos	•Desenvolvimento de uma estratégia para gestão de recursos humanos, relativamente a recrutamento, formação e competências.
Gestão da Mudança	•Introdução da gestão da mudança de forma a garantir o sucesso da implementação e adoção das diferentes iniciativas, garantindo os *quick-wins* como primeiros fatores de sucesso, incluindo a consequente mudança cultural da PSP nos seus processos e operações. Está intrinsecamente associado ao fator de sucesso relacionado com os Recursos Humanos. Deverá iniciar-se com o PESI, podendo ser integrado na equipa de PMO.
Financiamento	•Garantia da disponibilidade de financiamento plurianual que acompanhe o projeto. Fator intrinsecamente relacionado com o Apoio Alto-Nível.