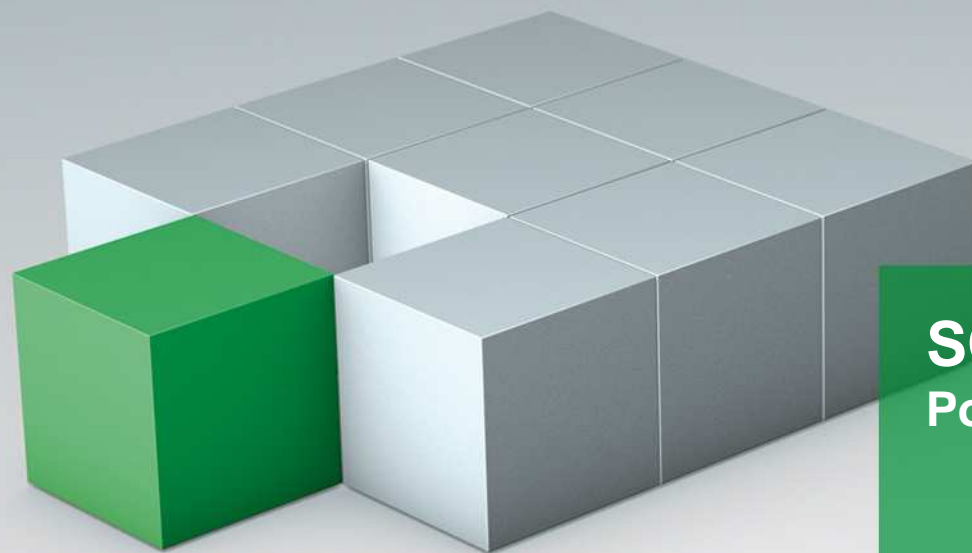


Quality Services and
Testing Solutions at Work



SQS Portugal Portfólio de Serviços

SQS Software Quality Systems

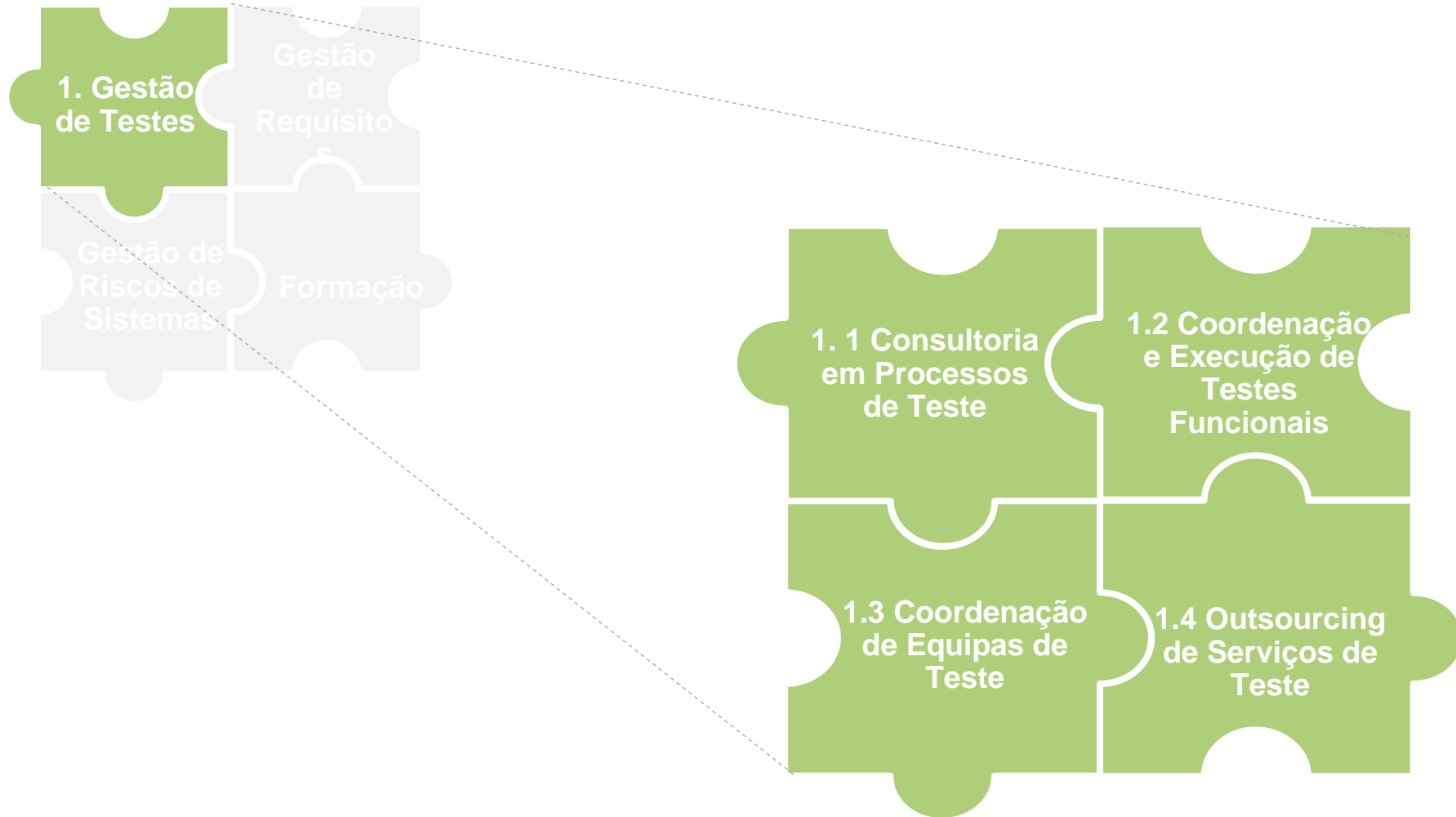
Portfólio de Serviços

Grupos de Serviços



Portfólio de Serviços

Grupo de Serviços 1: Gestão de Testes



1.1 Consultoria em Processos de Teste

Apoiar as empresas na implementação ou reestruturação de áreas de teste aplicacional

- Analisar o processo, recursos e ferramentas de teste actuais do cliente
- Definir/ Redefinir o processo de teste do cliente
- Definir/ Redefinir a organização da equipa/ área de testes do cliente
- Apoiar a selecção de recursos a integrar na equipa de testes do cliente
- Apoiar a selecção de ferramentas de suporte ao processo de teste do cliente
- Formar/ Requalificar recursos de teste do cliente em procedimentos, técnicas e/ou ferramentas
- Apoiar a Implementação/ Consolidação do processo de teste (re)definido
- Monitorizar o funcionamento da área de testes do cliente (pós-implementação) e identificar oportunidade de melhorias

1.2 Coordenação de Equipas de Teste

Enquadrar e coordenar equipas de teste no cliente responsáveis pela elaboração, planeamento e execução de actividades de teste, numa perspectiva de serviços continuados

- Definir com o cliente as áreas/ equipas de teste a enquadrar e quais os recursos internos e/ou externos associados
- Definir com o cliente o domínio aplicacional de intervenção e o tipo de testes funcionais a executar:
 - testes de sistema e/ou
 - testes de integração e/ou
 - testes de aceitação (UAT) e/ou
 - testes de regressão
- Elaborar os planos de teste inerentes ao domínio de actuação definido, tendo por base a metodologia de testes preconizada pela SQS (PractiQ)
- Avaliar o tipo de recursos, esforço e timings associados à execução dos planos de teste no âmbito de actuação das equipas de teste geridas



1.2 Coordenação de Equipas de Teste

(cont.)

- Alocar recursos às actividades de teste planeadas
- Gerir as equipas e coordenar a execução das actividades de teste
- Executar testes e reportar eventuais defeitos detectados
- Produzir relatórios, com periodicidade a acordar, com as métricas do processo e das actividades de teste (ver Serviço de Coordenação e Execução de Testes Funcionais)

1.3 Coordenação e Execução de Testes Funcionais

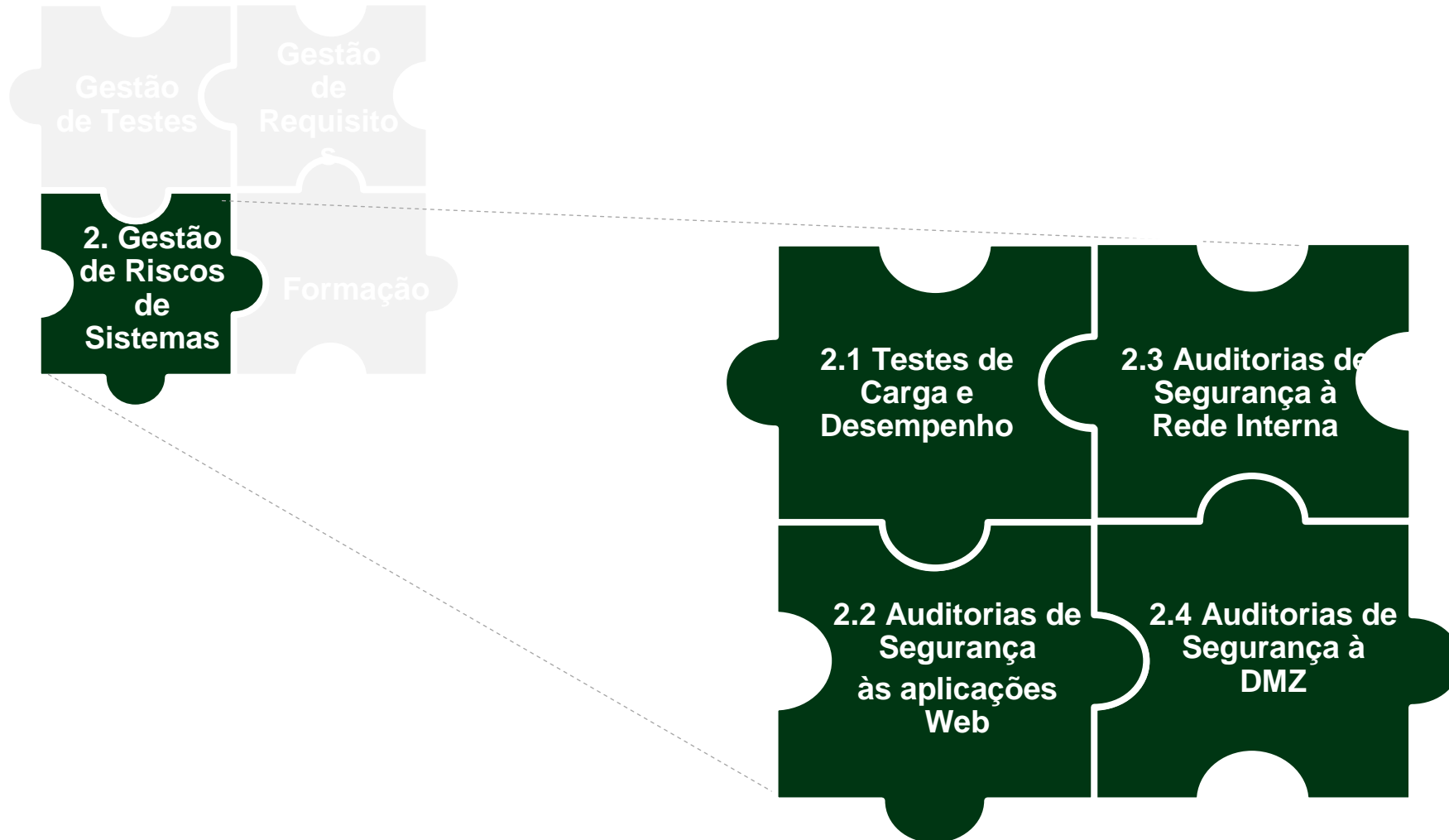
Planear e executar projectos de testes funcionais com âmbito definido pelo cliente

- Definir com o cliente o âmbito do projecto – domínio aplicacional de intervenção e tipo de testes funcionais a executar:
 - testes de sistema e/ou
 - testes de integração e/ou
 - testes de aceitação (UAT) e/ou
 - testes de regressão
- Definir o plano de testes tendo por base a metodologia de testes preconizada pela SQS (PractiQ)
- Avaliar o tipo de recursos, esforço e timings associados à execução do plano de testes
- Identificar os recursos a afectar ao projecto (pelo cliente e/ou pela SQS)
- Coordenar o projecto e a execução do plano de testes
- Executar os testes e reportar eventuais defeitos detectados

1.4 Outsourcing de Serviços de Teste

Assegurar serviços de teste continuados com âmbito e níveis de serviços previamente contratualizados, sendo a gestão e os recursos alocados da responsabilidade da SQS

- Definir com o cliente o âmbito do serviço e o tipo de testes a executar:
 - testes de sistema e/ou
 - testes de integração e/ou
 - testes de aceitação (UAT) e/ou
 - testes de regressão
- Definir volumetria e níveis de serviço a assegurar.
- Definir mecanismos de gestão e controlo do serviço.
- Definir período de transição, caso exista transferência de serviços ou de equipas actuais do cliente
- Contratualizar o serviço



2.1 Testes de Carga e Desempenho

Execução de testes por forma a verificar se o sistema suporta a carga prevista, e avaliar a sua robustez quando submetido a uma carga acima do previsto, assim como determinar o seu limite de capacidade com um tempo de resposta considerado aceitável para o sistema e infraestrutura em causa

- Verificar se o sistema suporta o número de utilizadores esperado de acordo com os objectivos definidos para tempos de resposta
- Identificar eventuais estrangulamentos, nomeadamente os que possam ter mais impacto no desempenho do sistema
- Identificar o limite de capacidade do sistema após terem sido introduzidas as melhorias decorrentes da identificação dos eventuais estrangulamentos
- Avaliar a robustez do sistema quando submetido a uma carga superior ao previsto
- Optimizar a capacidade instalada



2.1 Testes de Carga e Desempenho

(cont.)

- Obter baselines de desempenho no sentido de permitir a comparação com resultados de testes futuros (testes de regressão) e avaliar eventuais impactos negativos ou positivos de alterações efectuadas no sistema, arquitectura ou topologia.
- Fornecer relatórios intermédios de cada teste executado e um relatório final, onde constam os resultados principais dos testes, a identificação dos eventuais estrangulamentos e oportunidades de melhoria, assim como recomendações no sentido de otimizar o desempenho do sistema

2.2 Auditoria de Segurança a Aplicações WEB

Identificação de vulnerabilidades e riscos presentes em aplicações Web. serviço ajuda o cliente a corrigir os eventuais problemas ou vulnerabilidades através do fornecimento de exemplos de código e boas práticas

- Efectuar um scan completo da aplicação Web, designado por Crawling, com o objectivo de “aprender” e compreender a aplicação e avaliar o seu modo de funcionamento e assim produzir o maior número de casos de teste de vulnerabilidades. Os casos de teste abrangem treze tipos diferentes de variantes de ataques conhecidos. Tipicamente, para uma aplicação de média dimensão, são criados aproximadamente 200.000 casos de teste
- Executar ds casos de teste criados, com o objectivo de identificar as áreas de vulnerabilidade da aplicação
- Elaborar três níveis de relatórios:
 - Executive - fornece uma avaliação do risco total da aplicação com uma descrição simples da correcção de cada vulnerabilidade encontrada;
 - Management - fornece um sumário geral das vulnerabilidades encontradas por tipo de ataque;
 - Detailed - fornece informação relativa aos dados utilizados em cada campo com o resultado que causou a exploração da vulnerabilidade.



2.2 Auditoria de Segurança a Aplicações WEB

(cont.)

- Efectuar Workshop(s) com a equipa do projecto e desenvolvimento, de forma a demonstrar como pode ser abordada e resolvida cada vulnerabilidade encontrada com exemplos de código fonte e de boas práticas.
- Classificar, em termos de factores de risco, as vulnerabilidades encontradas, tendo em linha de conta a probabilidade e facilidade de serem exploradas, o seu impacto na confidencialidade, integridade e disponibilidade dos sistemas em causa
- Verificar se os mecanismos/controles de segurança estão a desempenhar as suas funções de acordo com os requisitos e política de segurança específicos da infra-estrutura

2.3 Auditoria de Segurança às redes internas

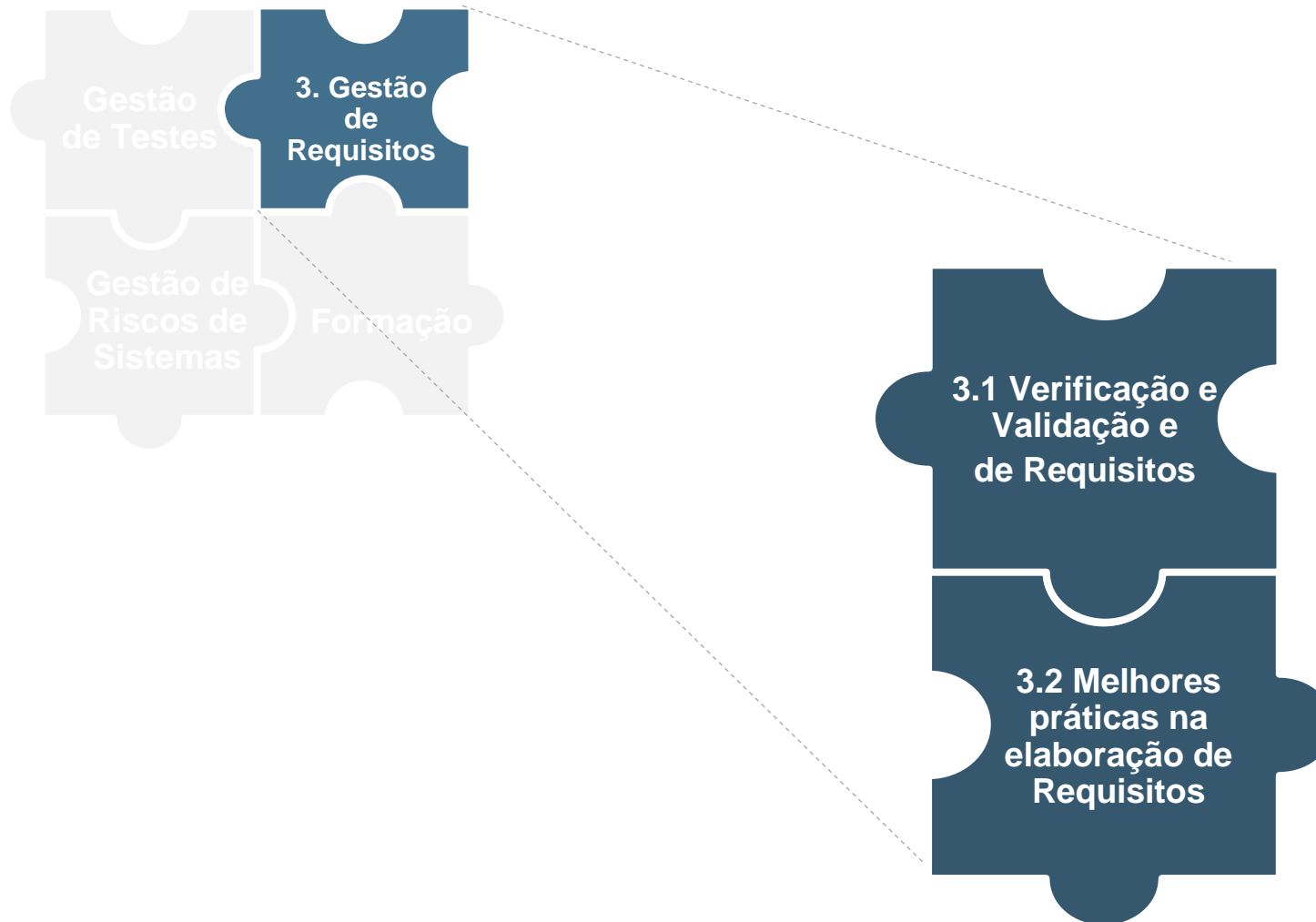
Realizar testes de segurança, manuais e automatizados, que simulam actividades típicas de um ataque interno, com o objectivo de identificar vulnerabilidades nos sistemas informáticos, serviços e aplicações que se encontram nas redes internas e, com base nos resultados, propor recomendações

- Avaliar condições de segurança dos equipamentos, serviços e aplicações que se encontram nas redes internas
- Elaborar relatório de análise, por cada endereço IP, com os resultados dos testes de segurança realizados e recomendações para resolução das vulnerabilidades encontradas
- Identificar áreas com potencialidade de melhoria em matéria de segurança, de acordo com a missão, objectivos e política de segurança definidos
- Classificar, em termos de factores de risco, as vulnerabilidades encontradas, tendo em linha de conta a probabilidade e facilidade de serem exploradas, o seu impacto na confidencialidade, integridade e disponibilidade dos sistemas em causa
- Verificar se os mecanismos/controlos de segurança estão a desempenhar as suas funções de acordo com os requisitos e política de segurança específicos da infra-estrutura

2.4 Auditoria de Segurança à DMZ

Realizar testes de segurança, manuais e automatizados, que simulam actividades típicas de um ataque externo, com o objectivo de identificar vulnerabilidades nos sistemas informáticos, serviços e aplicações que se encontram na DMZ e, com base nos resultados, propor recomendações

- Avaliar condições de segurança dos equipamentos, serviços e aplicações que se encontram na DMZ
- Elaborar relatório de análise, por cada endereço IP, com os resultados dos testes de segurança realizados e recomendações para resolução das vulnerabilidades encontradas
- Identificar áreas com potencialidade de melhoria em matéria de segurança, de acordo com a missão, objectivos e política de segurança definidos
- Classificar, em termos de factores de risco, as vulnerabilidades encontradas, tendo em linha de conta a probabilidade e facilidade de serem exploradas, o seu impacto na confidencialidade, integridade e disponibilidade dos sistemas em causa
- Verificar se os mecanismos/controlos de segurança estão a desempenhar as suas funções de acordo com os requisitos e política de segurança específicos da infra-estrutura



3.1 Validação e Verificação de Requisitos

Efectuar a análise de documentação de Requisitos de Utilizador e de Sistema, com o objectivo de identificar oportunidades de melhoria e, dessa forma, assegurar uma base para desenvolvimento mais correcta, completa e fidedigna.

■ Os requisitos são testados em conformidade com a norma IEEE 830 ⁽¹⁾ por forma a validar/ verificar se estão:

- Correctos
- Completos
- Consistentes
- Claros
- Verificáveis
- Modificáveis
- Rastreáveis

(1) IEEE Std 830-1998 - IEEE Recommended Practice for Software Requirements Specifications

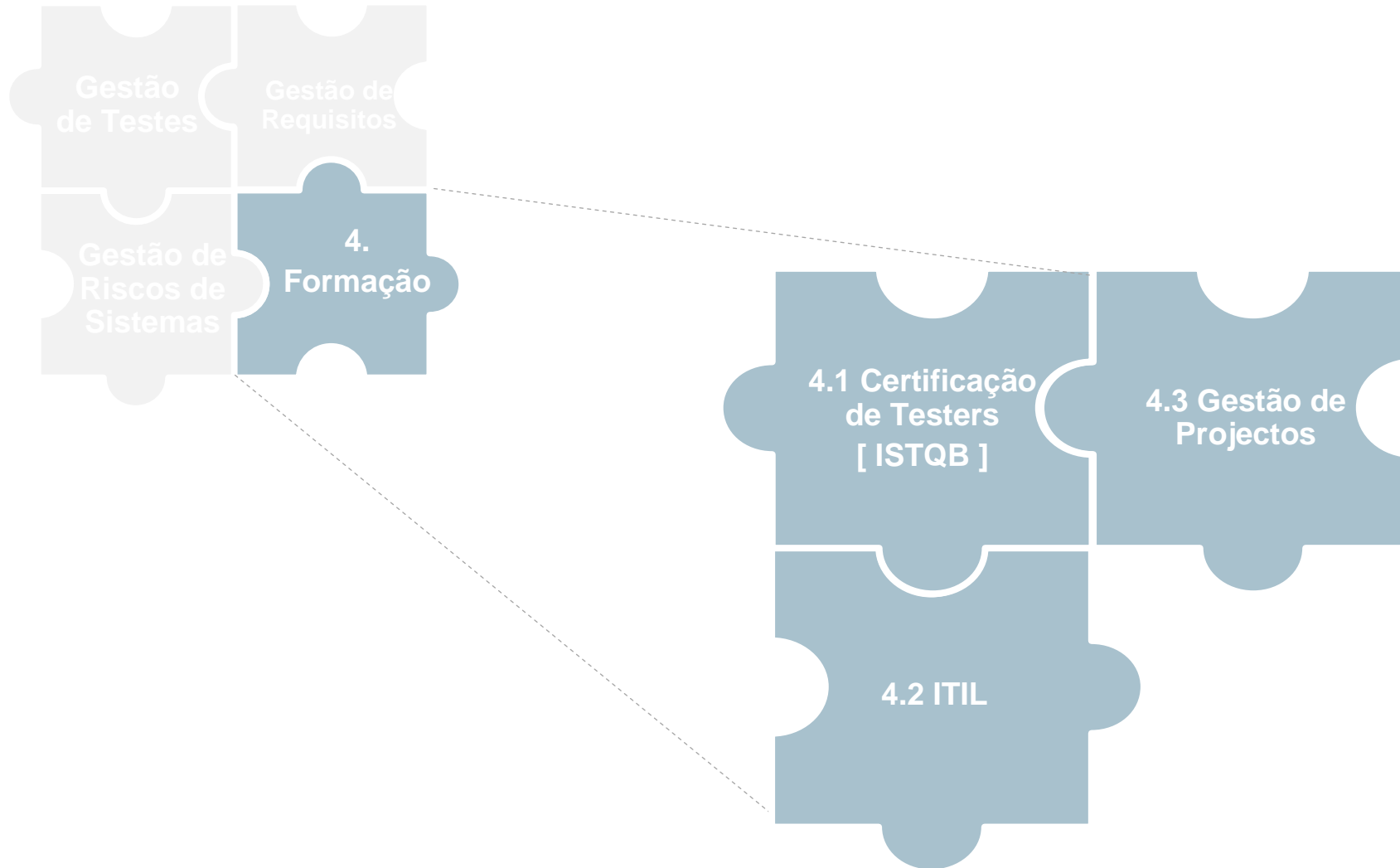
3.2 Melhores práticas na elaboração de Requisitos

Fornecer os fundamentos para a elaboração de Requisitos, com o objectivo de melhorar à partida a qualidade intrínseca dos mesmos e dessa forma criar uma base para o desenvolvimento de software mais correcta, completa e fidedigna.

- Identificar modelos/ templates a utilizar
- Melhorar modelos/ Templates existentes.
- Apresentar e discutir erros típicos/ situações a evitar
- Fornecer “Checklists” para utilização pelos autores dos requisitos

Portfólio de Serviços

Grupo de Serviços 4: Formação



4.1 Certificação de Testers ISTQB

Dotar de competências chave e certificar a comunidade de profissionais desta área tecnológica.

Certificação obtida

Formação avançada + Avaliação

Formação base

Sensibilização

Tipo de formação



• ISTQB, Foundation Level

• ISTQB, Advanced Level



NOVO

4.2 ITIL

Dotar de competências chave e certificar a comunidade de profissionais, desta área de gestão.

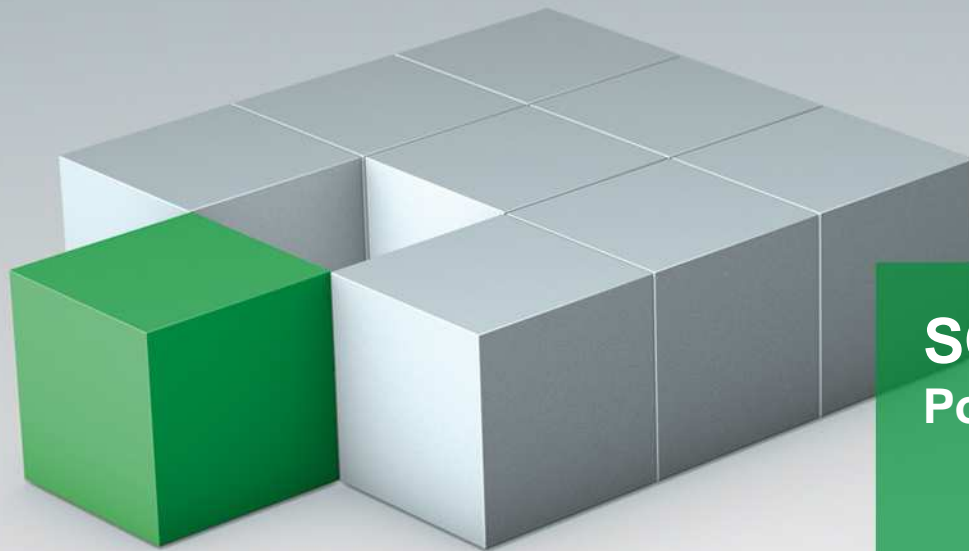


4.3 Gestão de projectos

Dotar de competências chave e certificar a comunidade de profissionais, desta área de gestão.



Quality Services and
Testing Solutions at Work



SQS Portugal Portfólio de Serviços

Av. 5 de Outubro, 293 - 4ºEsq

1600-035 Lisboa

Tel.: +351 217 983 109 | Fax: +351 214 229 071

E-Mail: info@sqs.pt

Internet: www.sqs.pt | www.sqs-group.com

SQS Software Quality Systems