INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2012/2013

TII

Reorganização das TIC na Defesa Nacional

DOCUMENTO DE TRABALHO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IESM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS E DA GUARDA NACIONAL REPUBLICANA.

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

REORGANIZAÇÃ DAS TIC NA DEFESA NACIONAL

FERNANDO JORGE FERREIRA SEUANES

Capitão-de-mar-e-guerra

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL DO CURSO DE PROMOÇÃO A OFICIAL GENERAL

Pedrouços 2013

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

REORGANIZAÇÃ DAS TIC NA DEFESA NACIONAL

FERNANDO JORGE FERREIRA SEUANES

Capitão-de-mar-e-guerra

Trabalho de Investigação Individual do CPOG 2012/2013

Orientador: CORONEL ADMAER JOÃO CARLOS BONIFÁCIO DA SILVA MATOS

Pedrouços 2013

Agradecimentos

Agradeço em primeiro lugar ao Coronel João Carlos Bonifácio da Silva Matos, orientador deste trabalho, pela sua prestimosa colaboração, ajudando a orientar a pesquisa, a clarificar as múltiplas dúvidas que foram surgindo, mas sobretudo pela paciência e disponibilidade demonstradas.

Gostaria de expressar o meu sincero agradecimento o Contra- almirante Gameiro Marques, CMG Alves Francisco, CMG Pinto e Lobo, CMG Borges Gaspar e ao CTEN Dias Marques, porque sem eles, não teria ultrapassado os diversos obstáculos encontrados na elaboração deste trabalho.

Aos camaradas de curso pelo apoio e franca camaradagem, sempre prontos a auxiliar na realização de contactos necessários

As últimas palavras são para expressar o meu profundo reconhecimento à minha mulher, por ter compreendido e apoiado o meu empenhamento neste trabalho.

Índice

Índice de Apêndices:

Índice de Figuras:

Índice de Tabelas:

Índice de Gráficos:

Resumo

As Tecnologias de Informação (TI) desempenham hoje um papel fundamental no quotidiano e serão cada vez mais um pilar da superioridade da informação, da resiliência e da agilidade que caraterizarão as Forças Armadas do futuro.

Com efeito, atenta a realidade atual e os desenvolvimentos que se perspetivam no médio e longo prazo, salientando-se a título de exemplo as iniciativas relacionadas com a partilha de informação no âmbito da NATO e da UE, a necessidade de otimização das Forças Armadas, fruto da crise económica e financeira que se faz e fará sentir, e as ameaças crescentes no domínio virtual, não será difícil perspetivar que as TI assumirão, cada vez mais, um papel central na Defesa Nacional, contribuindo de forma cada vez mais significativa para o cumprimento eficaz e eficiente das missões.

Consequentemente, a governação das TI na Defesa Nacional é assim um assunto muito relevante, e atual, porquanto a sua adequabilidade determinará o grau com que este setor irá contribuir para os objetivos estratégicos da organização o qual, como se referiu, terá de ser cada vez mais elevado.

Neste trabalho apresentamos pois uma proposta de modelo de governação para as TI da Defesa Nacional, que resulta da seguinte metodologia. Numa primeira fase, analisou-se o estado da arte da governação das TI na Defesa Nacional segundo três perspetivas diferentes; a que transparece da organização em vigor, a do ambiente interno, que resulta de uma auditoria conduzida pela IGDN em 2011, e de uma autoavaliação realizada pela própria Defesa Nacional, e ainda a do ambiente externo, sistematizada através de uma análise de oportunidades e desafios. De seguida, foram analisados modelos relevantes e relacionados, nomeadamente o da NATO, o da defesa Australiana e o do Reino Unido. Posteriormente, foram definidos um conjunto de critérios de avaliação para modelos de governação de TI e, finalmente, foram concebidas e avaliadas várias alternativas, à luz dos critérios mencionados.

O modelo proposto para a governação das TI na Defesa Nacional é um modelo híbrido, com a governação centralizada por um órgão colegial em que estão representados as principais entidades da Defesa Nacional, cuja principal função é alinhar a estratégia das TI com a da Defesa Nacional. Este órgão é apoiado ao nível da gestão pela estrutura do CIO que procura otimizar os recursos existentes. Os Ramos serão responsáveis pela gestão dos

serviços estratégicos de apoio à decisão, serviços específicos de apoio à sua missão e pelos núcleos de competências que permitirão aliviar a estrutura do CIO.

Abstract

In this day and age, Information Technology (IT) plays a key role in daily life and it will increasingly become the pillar of strength in the information, resilience and agility that characterizes the Armed Forces of the future.

Indeed, given the current reality and the perspective medium and long term developments, emphasizing for example the initiatives related to information-sharing within the framework of NATO and the EU, the need for optimization of the Armed Forces, as a result of the economic and financial crisis that is and will continue to be felt, and the rising threats in the virtual domain it is not difficult to foresee that IT will take a progressively central role in the National Defense, contributing more and more to the effective and efficient fulfillment of the missions.

Consequently, IT governance in the National Defense is a very important, and current, subject because its adequateness will determine the degree to which this sector will contribute to the strategic objectives of the organization which, as mentioned, should always be higher.

In this research we present a proposal for a model of governance for the IT in the National Defense, which results in the following methodology. As a first step, we analyzed the state of the art IT governance in the National Defense according to three different perspectives; one which is in place in the organization, one which is the internal environment, this being the result of an audit conducted by the IGDN in 2011, and a self-assessment carried out by the National Defense, and lastly one which is the external environment, the latter having been systemized by the analysis of opportunities and challenges. Then, relevant and related models were analyzed, namely NATO and the Australian and the United Kingdom Defense. Later, a set of evaluation criteria for IT governance models were defined and, finally, several alternatives were conceived and evaluated, based upon the criteria mentioned.

The proposed model for IT governance in the National Defense is a hybrid model, with centralized governance by a collegiate body in which the main entities of National Defense are represented, its main function being the alignment of the IT strategy with that of the National Defense. This body is supported, on a management level, by the structure of the CIO which seeks to optimize existing resources. The Branches will be responsible for the management of strategic services to decision making support, specific services to support their mission and the skill clusters that will lighten the CIO structure.

Palavras-Chave

Chief Information Officer, Defesa, Governação, Tecnologias da Informação, Modelo Híbrido TI

KeyWords

, Chief Information Officer, Defence, Governance, Information Technology, Hybrid IT Model

Lista de abreviaturas

AUI	Ambiente Único de Informação
AMA	Agência para a Modernização Administrativa
ANAO	Australian National Audit Office
AP	Administração Pública
C2	Comando e Controlo
C4	Command, Control, Communications and Computing
C3B	C3 Board
CDD	Centro de Dados da Defesa
CDIACM	Centro de Documentação, Informação e Arquivo Central da Marinha
CEMCONJ	Chefe do Estado-Maior Conjunto
CEMFA	Chefe do Estado-Maior da Força Aérea
CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CEO	Chief Executive Officer
CFT	Comando das Forças Terrestres
CGE	Comité de Governação Estratégica
CGExec	Comité de Governação Executiva
CIO	Chief Information Officer
CIOG	CIO Group
CIS	Comunicações e de Sistemas de Informação
CLAFA	Comando Logístico e Administrativo da Força Aérea
CLD	CIS Logistics Depot
CM	Comité Militar
COBIT	Control Objectives for Information and Related Technology
CSI	Comunicações e Sistemas de Informação
CTOD	Chief Technology Officer Division
D	Desafios
DAE	Divisão de Arquitetura Empresarial
DAF	Divisão de Apoio Financeiro
DAGI	Direção de Análise e Gestão da Informação

DAL	Divisão de Apoio Logístico
DCM	Data Communication Module
DCSI	Direção de Comunicação e Sistemas de Informação
DDC	Divisão de Desenvolvimento de Capacidades
DEIO	Divisão de Estatística e Investigação Operacional
DGAIED	Direção -Geral de Armamento e Infra – Estruturas de Defesa
DGPDN	Direção -Geral de Política de Defesa Nacional
DGPRM	Direção -Geral de Pessoal e Recrutamento Militar
DGT	Divisão da Gestão da Transição
DICSI	Divisão de Comunicações e Sistemas de Informação
DICTC	Defence ICT Committee
DIPLAEM	Divisão de Planeamento Estratégico Militar
DIREC	Divisão de Recursos
DITIC	Direção de Tecnologias de Informação e Comunicações
DN	Defesa Nacional
DoD	Department of Defence
DOMC	Divisão de Operações e Manutenção de Capacidades
DOTMLPII	Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infra-estrutura e Interoperabilidade
DQNS	Divisão de Qualidade Normalização e Segurança
DSAG	Divisão de Sistemas de Apoio à Gestão
DSC	Divisão de Serviços e Comunicações
DSI	Divisão de Sistemas de Informação
DSSI	Direção dos Serviços dos Sistemas de Informação
EMA-DIV PLAN	Estado-Maior da Armada – Divisão de Planeamento
EMC	Estado-Maior Conjunto
EME-DIV CSI	Estado-Maior do Exército – Divisão de Comunicações e Sistemas de Informação
EMFA-DIV CSI	Estado-Maior da Força Aérea – Divisão de Comunicações e Sistemas de Informação
EMGFA	Estado-Maior-General das Forças Armadas

FA	Força Aérea
FFAA	Forças Armadas
GP	Grupos de Projetos
GPTIC	Grupo de Projeto para as Tecnologias de Informação e Comunicação
Hip	Hipótese
HRDD	Human Resource Development Division
I&D	Investigação e Desenvolvimento
IASFA	Instituto de Ação Social das Forças Armadas
IBM	International Business Machines Corporation
ICTDD	Information and Communications Technology Development Division
ICTOD	Information and Communications Technology Operations Division
ICTRD	Information and Communications Technology Reform Division
IDN	Instituto da Defesa Nacional
IGDN	Inspeção-Geral da Defesa Nacional
ITGI	IT Governance Institute
MDN	Ministério da Defesa Nacional
MMHS	Military Message Handling System
NAF	NATO Architecture Framework
NATO	Organização do Tratado do Atlântico Norte
NC&IA	NATO Communications and Information Agency
NCA	Network Capability Authority
NTA	Network Technical Authority
O	Oportunidades
OCAD	Órgão Central de Administração e Direção
OE	Objetivo Específico
OG	Objetivo Geral
NATO	Organização do Tratado do Atlântico Norte
P	Potencialidades
PAEF	Programa de Assistência Económica e Financeira
PAS	Plano de Ação Setorial

PCM	Presidência do Conselho de Ministros
PGETIC	Plano Global Estratégico de Racionalização e Redução de Custos TIC na Administração Pública
PJM	Polícia Judiciária Militar
QC	Questão Central
QD	Questão Derivada
RCM	Resolução de Conselho de Ministros
REP	Repartição
RFCM	Rede Fixa de Comunicações
SACEUR	Supreme Allied Commander Europe
SAM	Strategic Alignment Model
SC	Serviços Centrais
SDG	Systems Direction Group
Seg. INFO	Segurança da Informação
SET	Stakeholder Engagement Team
SG	Secretaria-geral
SI	Sistemas de Informação
SI/TIC	Sistemas de Informação/ Tecnologias da Informação e Comunicações
SIGDN	Sistema Integrado de Gestão da Defesa Nacional
SLA	Service Level Agreements
SOG	Senior Officials Group
SSTI	Superintendência das Tecnologias da Informação
TI	Tecnologias da Informação
TIC	Tecnologias de Informação e Comunicação
EU	União Europeia
V	Vulnerabilidades
VCEMA	Vice-Chefe de Estado-Maior da Armada
VCEME	Vice-Chefe de Estado-Maior do Exército

Introdução

> *Coming together is a beginning; keeping together is progress; working together is success.*
>
> *Henry Ford*

- **Justificação**

No decorrer dos últimos anos as Tecnologias da Informação (TI) têm vindo a assumir um papel cada vez mais relevante no sucesso das organizações, sendo considerado, por muitos, que a última grande revolução pela qual a humanidade passou foi, indubitavelmente, a revolução tecnológica e da informação, que nos posicionou na atual "Era da Informação e do Conhecimento". No quadro desta dinâmica pós-industrial e amadurecido que está o processo tecnológico subjacente, "*os investimentos em TI estão a deixar de ter o seu enfoque na tecnologia, propriamente dita, e têm vindo a centrar-se ultimamente na potenciação da informação e do conhecimento em suporte à decisão, à criação de valor e como agente de diferenciação, inovação e transformação das organizações*" (ITGI, 2008, p. 7), permitindo que estas se mantenham adaptadas ao ambiente competitivo em que se inserem e alinhadas com respetivos desígnios estratégicos.

Na opinião de diversos autores, a forma como as TI são interpretadas e se encontram alinhadas com os processos de negócio de qualquer organização tem um impacto determinante na forma como esta alcança a sua visão e prossegue a sua missão e objetivos estratégicos.

No universo da Defesa Nacional (DN) este facto não constitui exceção, embora os diversos intervenientes abordem o assunto de formas substancialmente distintas, claramente com enfoques e níveis de maturidade diferenciados, de onde decorrem organizações desiguais o que, só por si, não contribui para promover a identificação de sinergias, sobretudo naquilo que é, claramente, de utilização potencialmente comum e partilhada.

Acreditando ser a governação das TI uma questão da maior relevância para a DN, entendeu-se oportuno escolher o tema em apreço. Pretende-se, com esta investigação, analisar o estado da arte das TI na DN, identificando, não apenas as eventuais insuficiências, como também as boas práticas, de forma a idealizar um novo modelo de governação que promova sinergias, racionalize custos e garanta a segurança.

- **Enunciado do tema, a identificação do contexto e a base conceptual em que a investigação se insere.**

Esta investigação tem como tema: "*Reorganização das TIC na Defesa Nacional*."

O quadro conceptual que enforma o trabalho encontra-se plasmado no Apêndice 1. No entanto, para efeitos do presente estudo, importa desde logo definir alguns conceitos, com especial enfase na diferenciação entre os relacionados com a governação das TI e a gestão das TI.

Tal como referido por Grembergen[1], a "*gestão TI tem por objetivo o provimento interno efetivo de serviços e produtos TI e a gestão de operações TI correntes*" (Grembergen, 2004b, p. 4). A um nível diferente encontra-se a governação TI que, sendo responsabilidade dos Conselhos de Administração/Direção e dos gestores executivos "*é parte integrante da governação de uma organização e consiste na liderança e na criação de estruturas e processos organizacionais que asseguram que as TI suportam e estendem a estratégia e objetivos da organização*" (ITGI, 2003, p. 11). A este respeito, Grembergen refere que "*a governação TI é a capacidade organizacional exercida pelo Conselho de Administração, gestor executivo e gestor de TI para controlar a formulação e a implementação da estratégia TI e dessa forma assegurar a fusão do negócio e as TI*" (Grembergen, 2004a, p. 1). Esta estreita relação é igualmente evidenciada por diversos outros autores que, de forma consensual, identificam como um fator crítico de sucesso para a governação das TI e, provavelmente, como o grande desafio que se lhe coloca, a necessidade de existência de alinhamento entre a estratégia das TI e a estratégia de negócio da organização.

Como forma de medir esse alinhamento, as organizações utilizam modelos de maturidade que lhes permitem a realização de uma autoavaliação com recurso a critérios elencados numa escala numérica de níveis mensuráveis. Torna-se possível, desta forma, a identificação do estado da arte (lacunas) e das ações necessárias para atingir o nível estratégico de alinhamento pretendido (*end state*).

Assim, enquanto a gestão TI se encontra focada no presente, a governação TI, sem descurar a situação atual, está orientada para a transformação, tendo como objetivo fundamental que a organização se mantenha continuamente adaptada ao ambiente competitivo em que está inserida e preparada para os desafios futuros de um mundo em constante evolução.

[1]Wim Van Grembergen: Professor da MIS Department at Business Faculty of UFSIA-RUCA e professor executivo da University Antwerp Management School

- **Objeto de Estudo e sua Delimitação**
  - **Objeto de Estudo**

O presente trabalho de investigação centra-se nas estruturas de governação e de gestão das TI da DN, em que se englobam os Serviços Centrais do Ministério da Defesa Nacional (MDN), o Estado-Maior-General das Forças Armadas (EMGFA), os três Ramos (Marinha, Exército e Força Aérea (FA)) e o Instituto de Ação Social das Forças Armadas (IASFA).

  - **Delimitação do Tema**

Face à grande abrangência do tema, afigura-se conveniente delimitá-lo a fim de melhor centrar a investigação e aprofundar a análise. Assim, a abordagem ao modelo organizacional das TI na DN, irá situar-se, sobretudo, ao nível estratégico. Por esse motivo, não serão detalhados, no decorrer do trabalho, os sistemas incorporados em plataformas operacionais, designadamente, em sistemas de armas ou sensores dos meios orgânicos das Forças Armadas (FFAA). Este tipo de sistemas serão incluídos naquilo que adiante se denomina por sistemas próprios de cada Ramo.

Desta forma, o trabalho restringir-se-á à caracterização de um modelo organizacional aplicável à governação das TI na DN, não detalhando a forma como os Ramos se deverão organizar, embora, por uma questão de coerência, se considere ser fundamental que estes se organizem tendo por base um modelo interoperável ao nível doutrinário, dos procedimentos e tecnológico.

No que concerne ao enquadramento legislativo, a análise focar-se-á, exclusivamente, em diplomas posteriores ao ano de 2009, dado que toda a legislação anterior, com alguma relevância para o tema, foi entretanto revogada.

- **Objetivos da Investigação**
  - **Objetivo Geral (OG)**

O presente trabalho procura contribuir para a identificação de um modelo de governação coerente e harmonioso das TI da DN que potencie a redução de custos de exploração e configure a superioridade da informação. Apenas desta forma será possível que as TI concorram para que o processo de tomada de decisão esteja alinhado com os objetivos da Defesa, sejam eles estratégicos ou operacionais, permitindo que estes sejam alcançados e controlados.

- **Objetivos Específicos (OE)**

São objetivos específicos do estudo os seguintes:

Tabela nº1 Objetivos Específicos

Fonte: (Autor, 2012)

OE 1	Identificar o atual "estado da arte" da governação das TI da DN.
OE 2	Analisar modelos implementados em países de referência nesta área.
OE 3	Definir os critérios e princípios subjacentes ao modelo a implementar na governação das TI da DN.
OE 4	Contribuir para a identificação de um modelo organizacional e de governação das TI da DN.

- **A Pergunta de partida**

Concluída a fase de exploração, face ao objeto do estudo, ao OG e aos OE, estabeleceu-se a questão central (QC), e deduziram-se as questões derivadas (QD) e hipóteses (Hip), que de seguida se explicitam e que se encontram articuladas no Apêndice 1.

Tabela nº2 Questão Central e Questões Derivadas

Fonte: (Autor, 2012)

QC	*Qual o modelo organizacional e de governação mais adequado para as TI da DN?*
QD 1	*Em que medida é que o atual modelo organizacional e de governabilidade das TI não satisfaz as necessidades da DN?*
Hip 1	O atual modelo organizacional e de governabilidade seguido pelos Serviços Centrais do MDN, EMGFA, três Ramos (Marinha, Exército e Força Aérea) e pelo IASFA não permite uma racionalização dos recursos, não promove sinergias, não garante a segurança, e não fomenta a interoperabilidade.
QD 2	*Que modelos organizacionais e de governabilidade TI têm vindo a ser adotados por organizações congéneres e por países aliados e amigos, na área da Defesa?*
Hip2	As organizações congéneres e os países aliados e amigos têm evoluido para um modelo de governação hibrido das TI que privilegia a centralização dos serviços nucleares e de rede colocando, concomitantemente, o seu enfoque na informação, no conhecimento e na superioridade que daí advém.
QD 3	*Que critérios e princípios devem ser considerados na escolha e edificação do modelo organizacional e de governação TI mais adequado à DN?*
Hip 3	É possível deduzir critérios objetivos, de cariz essencialmente estratégico, gestionário e operacional, que permitem selecionar de forma criteriosa a melhor solução organizacional e de governação TI para a DN.
QD 4	*Que modelo organizacional e de governação TI melhor responde aos critérios e princípios estabelecidos para o modelo organizacional e de governação no âmbito da DN?*
Hip 4	Estando identificados os critérios objetivos da governação da TI é possivel encontrar uma solução organizativa e de governabilidade que permita mitigar as lacunas identificadas.

- **Procedimento Metodológico**

O trabalho desenvolver-se-á, de acordo com o estabelecido na NEP/ACA – 018, de 15 de julho de 2012, do IESM e respetivos anexos, através da adoção do método hipotético-dedutivo. Na fase de dedução e formulação da QC e das QD, bem como das hipóteses associadas, e para efeitos de clarificação dos conceitos implícitos ao tema, recorreu-se à leitura de diversos artigos e obras sobre a matéria, bem como a entrevistas exploratórias a entidades com reconhecida competência nesta área.

Seguidamente, procedeu-se a recolha da legislação e normativo que sustenta a atual arquitetura das TI na DN, com o objetivo de definir o quadro concetual da governação das TI, bem como de identificar o estado da arte no universo em causa. Numa fase posterior, procedeu-se à realização de uma autoavaliação, a qual permitiu aferir as potencialidade e as vulnerabilidades do modelo atualmente em uso na DN.

Seguiu-se o estudo de modelos de governação das TI existentes em países aliados de referência, com especial enfoque ao modelo em uso na Organização do Tratado do Atlântico Norte (NATO), por forma a identificar um modelo de governação que melhor se adeque à realidade da DN.

Por último, foram deduzidos critérios de avaliação objetivos, de cariz essencialmente estratégico, gestionário e operacional que permitam identificar qual o modelo de governação e correspondente arquitetura de referência que melhor responda aos requisitos da DN.

- **Estrutura do documento**

O trabalho está organizado em quatro capítulos, para além da introdução. No primeiro capítulo, carateriza-se o estado da arte da governação das TI na DN e analisa-se a envolvente interna e externa da DN. No segundo capítulo, são analisados os modelos de governação em utilização noutros países, com especial atenção à NATO. Por fim, nos terceiro e quarto capítulos identificam-se os critérios e princípios a considerar na escolha do modelo, bem como o modelo de governação das TI que, obedecendo aqueles critérios e princípios, apresenta um nível de maturidade que permita centrar a organização na gestão da informação e do conhecimento.

1. As TI na Defesa. O Estado da Arte

A avaliação sobre o grau de satisfação das necessidades da DN, no que concerne às TI, passa em primeiro lugar, pela descrição do estado da arte do modelo organizacional e de governabilidade das TI na DN, a qual será efetuada em dois planos: o primeiro, de natureza legal, onde se pretende capturar a realidade atual, em termos de organização e competências TI, com especial enfoque nos atores internos da Defesa; o segundo, expresso em termos do desempenho, medido com base numa avaliação independente e numa autoavaliação realizada pelas entidades envolvidas.

a. Modelo organizacional e de governação

(1) Serviços Centrais (SC) do MDN

No atual enquadramento legal e de acordo com a Lei Orgânica do MDN, integram a administração do Estado, no âmbito do MDN, os SC, constituídos pela Secretaria-geral (SG), a Inspeção-Geral da Defesa Nacional (IGDN), a Direção-Geral de Política de Defesa Nacional (DGPDN), a Direção-Geral de Pessoal e Recrutamento Militar (DGPRM), a Direção-Geral de Armamento e Infraestruturas de Defesa (DGAIED), o Instituto da Defesa Nacional (IDN) e a Polícia Judiciária Militar (PJM) (MDN, 2011, p. 5475).

À SG compete "*Implementar uma política integradora para toda a área dos sistemas de informação (SI) e tecnologias de informação e comunicação (TIC) no universo da defesa nacional, competindo-lhe coordenar os SI/TIC e administrar os SI/TIC de gestão, sem prejuízo da atribuição às Forças Armadas da definição dos requisitos operacionais e técnicos, da segurança e da gestão dos sistemas de comando e controlo militares*" (idem, 2011, p.5477). A responsabilidade sobre as duas áreas relacionadas com as TI, uma área mais aplicacional, a Direção dos Serviços dos Sistemas de Informação (DSSI) e outra área mais ligada às infraestruturas, o Centro de Dados da Defesa (CDD), recai sobre o secretário-geral adjunto, diretamente dependente do secretário-geral.

A orgânica da SG estabelece, como principais atribuições da DSSI, "*Elaborar e propor o plano estratégico e o modelo de governação dos SI da defesa nacional*" (MDN, 2012b, p. 1536), que têm vindo a ser materializadas, essencialmente, no desenvolvimento e gestão do ciclo de vida do Sistema Integrado de Gestão da Defesa Nacional (SIGDN). Este sistema, transversal ao universo da Defesa, foi concebido com o intuito de suportar os processos da área financeira, logística, de recursos humanos, bem como abranger uma área de indicadores de gestão, através da implementação de processos comuns e padronizados que

privilegiem a normalização. O seu ciclo de vida é gerido por uma equipa conjunta do MDN e dos Ramos, tendo estes últimos intervenção fundamental na evolução do sistema.

Constitui, igualmente, competência da DSSI, tal como estabelecido na Portaria n.º 86/2012, de 30 de março, "*Elaborar e propor as orientações para a integração dos sistemas de informação (SI) da defesa nacional, em colaboração com a estrutura das Forças Armadas*" (ibidem)

Este mesmo diploma atribui ao CDD competências para a administração da infraestrutura tecnológica partilhada, dos sistemas aplicacionais e de bases de dados da Defesa e da rede informática, para além do apoio ao utilizador.

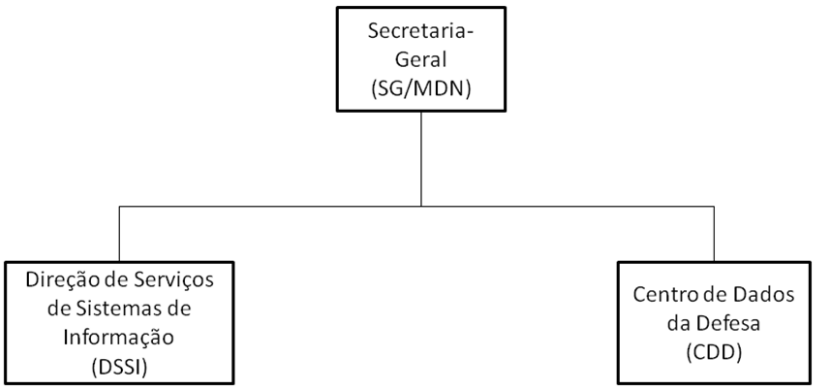


Figura 1 – Organograma da área funcional das TI da SG

Fonte: (Autor, 2012)

É, ainda, atribuição da SG "*Apoiar (...) os serviços centrais de suporte (...) sem prejuízo da autonomia administrativa dos mesmos, no âmbito dos recursos humanos, financeiros, patrimoniais, técnicos e Informáticos*." (MDN, 2012a, p. 310). Nesse sentido, os restantes SC, em matéria das TI, são apoiados pela SG, ficando apenas com estruturas residuais. Na DGPRM, a Divisão de Gestão de Recursos, na dependência direta do Diretor-Geral, é detentora de algumas competências a nível local. Por seu lado, a DGPDN dispõe de um núcleo de apoio, na dependência da Direção de Serviços de Planeamento Estratégico de Defesa, Estudos e de Apoio à Gestão. Na DGAIED existe um núcleo de apoio informático, criado pelo despacho do Diretor-Geral n.º 29/DGAIED/2010, de 10 de março. Na PJM, as competências no âmbito das TI residem na Unidade de Administração e Apoio Técnico. O IDN dispõe, de forma idêntica, de um núcleo de informática.

(2) EMGFA

A lei orgânica do EMGFA estabelece que o Estado-Maior Conjunto (EMC) compreende, entre outras, a Divisão de Comunicações e Sistemas de Informação (DICSI) que "*tem por missão prestar apoio de estado – maior nas áreas de planeamento, direcção e controlo dos sistemas de informação e tecnologias de informação e comunicação inerentes ao comando e controlo nas Forças Armadas*" (MDN, 2009a, p. 6446).

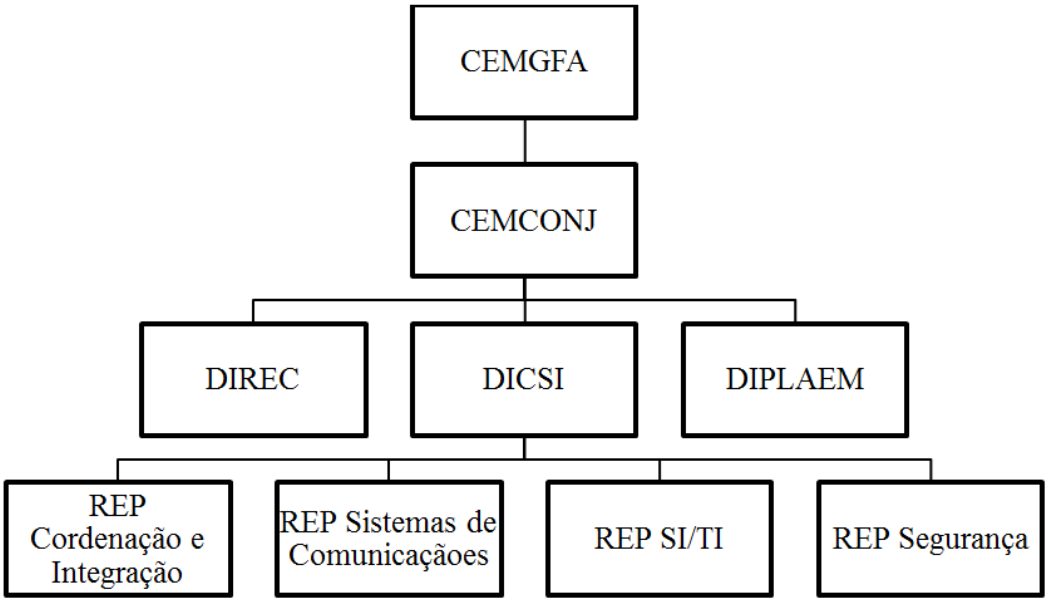


Figura 2 – Organograma da área funcional das TI do EMGFA

Fonte: (Autor, 2012)

Numa lógica de serviços partilhados, a qual tem permitido coerência tecnológica e economia de escala, o EMGFA é responsável pela gestão, administração e sustentação da Rede Fixa de Comunicações (RFCM) e do *Military Message Handling System* (MMHS), sistemas transversais aos Ramos. O primeiro disponibiliza serviços de transporte de voz e dados. O segundo constitui-se como um sistema de informação de cariz militar que satisfaz os requisitos de funcionamento dos Ramos sendo, ainda, interoperável com a NATO.

À semelhança do que acontece com a DSSI, no âmbito da SG, é também atribuição da DICSI "*Colaborar na elaboração da proposta de orientações para a integração dos SI/TIC da defesa nacional*". (ibidem)

(3) Marinha

Na Marinha, a área das TI é da responsabilidade da Superintendência das Tecnologias da Informação (SSTI), a qual tem por missão "*assegurar as actividades da Marinha no domínio da gestão da informação e da administração das tecnologias da informação, sem prejuízo da competência específica de outras entidades e em observância da política integradora estabelecida pelo Ministério da Defesa Nacional para toda a área dos sistemas de informação e tecnologias de informação e comunicação (SI/TIC) no universo da defesa nacional*" (MDN, 2009b, p. 6438). A SSTI é o Órgão Central de Administração e Direção (OCAD) que dispõe de "*autoridade funcional e técnica sobre todos os órgãos do Ramo no domínio da gestão e análise da informação e das subjacentes tecnologias da informação e comunicações*" (SSTI, 2012, p. 6).

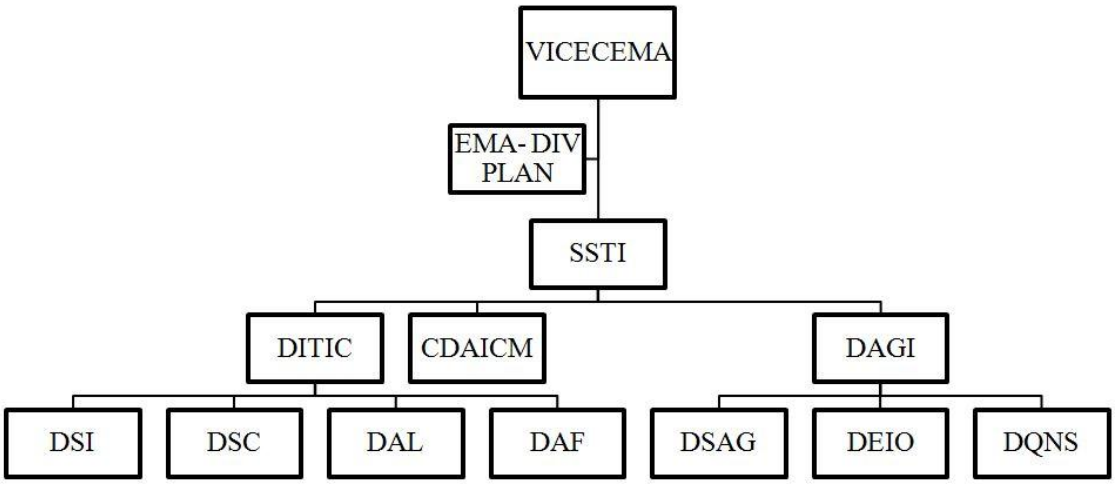


Figura 3 – Organograma da área funcional das TI da Marinha

Fonte: (Autor, 2012)

Os seus principais esforços têm sido dirigidos para a transformação da informação em conhecimento, garantindo um alinhamento com a estratégia da estrutura superior da Marinha. Para o efeito, dispõe de duas direções técnicas, a Direção de Análise e Gestão da Informação (DAGI) e a Direção de Tecnologias de Informação e Comunicações (DITIC), bem como do Centro de Documentação, Informação e Arquivo Central da Marinha (CDIACM), "*numa perspetiva de gestão global e integrada do ciclo de vida da informação e de potenciação da informação em conhecimento*" (Marques, 2012).

O Estado-Maior da Armada, através da Divisão de Planeamento, é responsável pelo apoio de estado-maior ao planeamento e estudos TI.

(4) Exército

O Exército aborda a área das TI em dois planos distintos. À Divisão de Comunicações e Sistemas de Informação (EME - DIVCSI), integrada no Estado-Maior do Exército, compete "*estudar, planear e coordenar as actividades do Exército do âmbito das comunicações, da guerra electrónica, dos sistemas e tecnologias de informação e da segurança das comunicações e sistemas de informação e difundir as normas, os planos e as directivas que orientem e determinem as acções a realizar no âmbito das suas áreas de responsabilidade*" (Repartição de Comunicação, 2013).

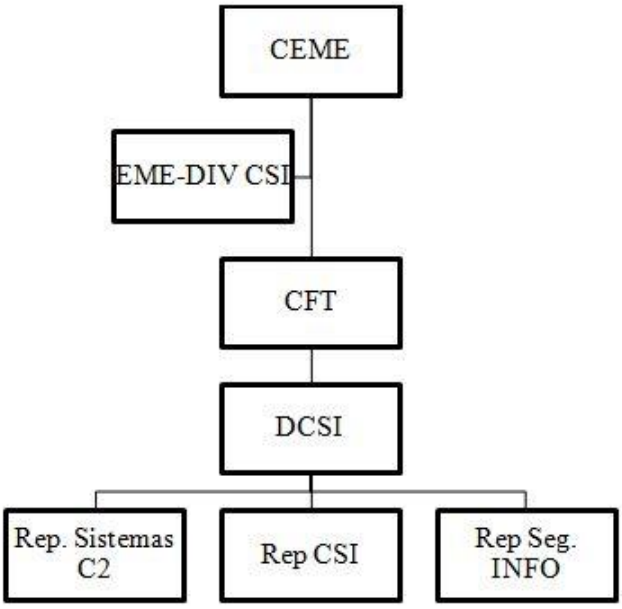


Figura 4 – Organograma da área funcional das TI do Exército

Fonte: (Autor, 2012

Por outro lado, o Comando das Forças Terrestres (CFT) "*dispõe de autoridade funcional e técnica nas matérias de natureza operacional, de comunicações e sistemas de informação e de segurança e informações militares, em observância da política integradora estabelecida pelo ministério para toda a área dos sistemas de informação e tecnologias de informação e comunicação (SI/TIC) no universo da defesa nacional (...)*" (MDN, 2009c, p. 6426). Para o efeito, tem sobre a sua dependência a Direção de Comunicações e Sistemas de Informação (DCSI), responsável pela conceção, desenvolvimento, implementação e manutenção técnica dos sistemas e serviços TIC, e a quem compete, nomeadamente, "*Assegurar a direcção, a coordenação, o controlo e a execução das actividades do Exército em matéria de sistemas e tecnologias de informação e comunicações (...)*" (MDN, 2007).

(5) Força Aérea

À semelhança do Exército, a FA encara, igualmente, a área funcional das TI sob duas vertentes. No entanto, ao contrário do Exército que integra essas vertentes na área operacional, a FA incorpora-as na área logística. Assim, como elemento orgânico do Estado-Maior da FA, está constituída a DCSI, responsável pela definição da política de comunicações da FA e dos requisitos operacionais e de logística dos sistemas de comunicação e informação e de comando e controlo. Por outro lado, a nível dos OCAD, encontra-se o Comando da Logística da FA (CLAFA) o qual "*tem por missão administrar os recursos materiais, de comunicações e sistemas de informação e infraestrutura da Força Aérea, para a execução dos planos e diretivas aprovados pelo CEMFA (...)*" (MDN, 2009d, p. 6431).

O CLAFA dispõe de "*autoridade funcional e técnica sobre todas as unidades e órgãos da Força Aérea no domínio das comunicações e sistemas de informação*" (ibidem). Na sua dependência encontra-se a Direção de Comunicações e Sistemas de Informação à qual incumbe a administração dos sistemas de comunicações, comando e controlo, navegação e vigilância, e de informação, e respetivas infraestruturas tecnológicas da FA.

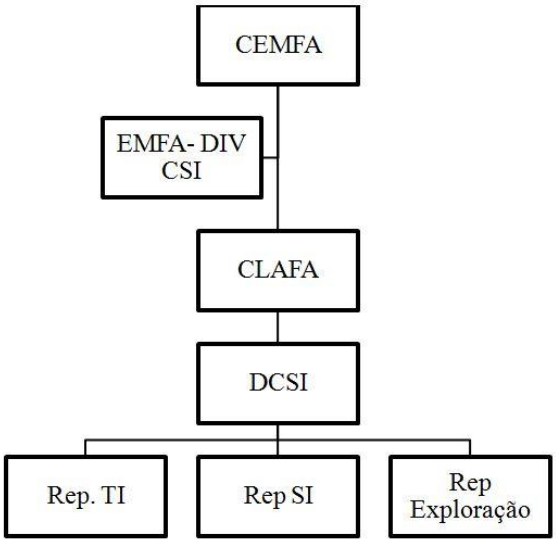


Figura 5 – Organograma da área funcional das TI da Força Aérea

Fonte: (Autor, 2012)

b. Análise do Ambiente Interno

A avaliação sobre o grau de satisfação das necessidades da DN, no que concerne às TI, não se pode considerar concluída sem que antes sejam aferidas as potencialidade e as

vulnerabilidades do modelo atualmente em uso na DN. Assim, afigura-se necessário proceder à análise do ambiente interno através da identificação dos descritores das variáveis ("Potencialidades" (P) e "Vulnerabilidades" (V)) que, no seu conjunto, caracterizam o contexto no qual a atividade da organização se desenrola. Neste grupo está incluída a estrutura organizacional, a estratégia e cultura e os recursos.

(1) Auditoria da IGDN

No âmbito do Plano de Atividades da IGDN para 2011, os órgãos do MDN foram objeto de uma auditoria com o intuito de avaliar o grau de integração dos sistemas de informação que envolvessem tecnologias de informação e comunicação do MDN, o processo de *" (…) aquisição, gestão e manutenção de aplicações (…)* " e "*avaliar os recursos humanos afetos ao sistema de manutenção e desenvolvimento e custos associados*" (IGDN, 2011, p. 7).

A metodologia utilizada caraterizou-se pela recolha e análise de informação documental, reuniões de trabalho com pessoal da área das TI, finalizando com a elaboração de um Relatório de Auditoria. As conclusões elencadas naquele relatório permitem constatar o seguinte (IGDN, 2011):

– Inexistência de um plano estratégico de médio e longo prazo e de um modelo de governação que defina os níveis de responsabilidade e os mecanismos de controlo que potenciem a rentabilização de recursos e redução de custos (V);

– As competências atribuídas à SG, no âmbito das TI, não tinham sido objeto de implementação, nomeadamente nos processos de aquisição e desenvolvimento das TI em que os organismos do MDN deveriam solicitar um parecer técnico prévio (V);

– O SIG encontrava-se em exploração nas áreas logística e financeira, embora com graus de implementação diferentes nos diversos Ramos, o que constitui um exemplo de boas práticas e de racionalização de recursos (P);

– Devido a uma gestão TIC descentralizada, incluindo nos processos de aquisição, existia dificuldade de coordenação e controlo dos sistemas de informação existentes e das necessidades, levando à aquisição de ferramentas redundantes, dificuldades de interoperabilidade, ineficiências e custos acrescidos (V);

– Os sistemas comuns de gestão não são geridos de forma centralizada (V);

– Pelo Despacho nº 2579/2006 do MDN de 18 de janeiro foi criada a Comissão de Politicas e Auditoria do Sistema de Informação da DN, constituída pelo SG e os

representantes do MDN, do EMGFA e dos Ramos. Esta comissão tem como missão elaborar as políticas de SI/TI da DN e auditar as atividades e tarefas inerentes à implementação das soluções SI/TI, tendo a sua última reunião ocorrido em 2009. A auditoria realizada, não localizou nenhuma evidência de trabalhos realizados (V).

(2) Questionário COBIT

Para implementar e melhorar a governação das TI da DN, torna-se necessário fazer um diagnóstico que avalie a eficácia da atual governação e que identifique oportunidades para a sua melhoria. Sendo que as tecnologias de informação na defesa são geridas, de forma autónoma e independente, por cinco entidades diferentes, avaliar o seu estado atual corresponde, na prática, a avaliar o estado atual das tecnologias de informação em cada uma destas entidades, nomeadamente no MDN, EMGFA, Marinha, Exército e FA.

Uma avaliação desta natureza pode ser realizada segundo variadas perspetivas. Contudo, considerando que os processos das TI são determinantes no fornecimento da informação necessária, de forma atempada e segura, para que a organização atinja os seus objetivos, optou-se por complementar a auditoria referida no parágrafo anterior com uma autoavaliação do estado atual das TI, através da avaliação do nível de maturidade, utilizando para o efeito o questionário do Apêndice 3. Esta autoavaliação está claramente dependente da precisão da informação fornecida, mas, lida em conjunto com as conclusões elencadas na auditoria, permite entender onde as TI da Defesa estão neste momento (*as is*) e para onde se pretende evoluir (*to be*).

O questionário elaborado foi baseado no *Control Objectives for Information and Related Technology* (COBIT). Esta ferramenta constitui uma moldura de apoio à governação das TI que compreende um modelo de maturidade da gestão e controlo dos processos das TI. Neste modelo são definidos 34 processos, agrupados segundo quatro domínios distintos (planear e organizar, obter e implementar, fornecer e apoiar, monitorizar e avaliar) cuja maturidade é estabelecida por um de seis níveis possíveis.

De acordo com o modelo, "*as organizações que são colocadas no nível 0 são caraterizadas por uma completa ausência de qualquer processo reconhecido de Governação TI. (…) O nível mais avançado implica, no mínimo, um conhecimento avançado dos assuntos e soluções relacionadas com a governação das TI, apoiada por processos, estruturas e mecanismos de relação assentes nas boas práticas*." (Grembergen, 2004b, p. 29)

A análise das respostas aos questionários recebidas plasmada no Apêndice 4 será efetuada segundo os processos de cada domínio identificado anteriormente. A análise con-

centrar-se-á, sobretudo, nos processos internos e individuais das diversas organizações que compõem a DN e que, potencialmente possam ser alavancados pela estrutura comum a detalhar no Capitulo 4.

c. Análise do Ambiente Externo

A análise do ambiente externo consiste na identificação dos descritores de variáveis (Oportunidades (O) e Ameaças (A)), cujo controlo não está ao alcance da organização e que caracterizam o contexto em que a mesma opera.

(1) Oportunidades

A Resolução de Conselho de Ministros (RCM) n.º 46/2011, de 14 de novembro, aprovou a constituição do Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC), com a missão de "*delinear e implementar uma estratégia global de racionalização das TIC na Administração Pública, com vista à melhoria da eficiência e à redução de custos*" (PCM, 2011, p. 4848), ficando este grupo na dependência do membro de governo responsável pela modernização da Administração Publica (AP). O GPTIC, no cumprimento dessa resolução, elaborou o Plano Global Estratégico de Racionalização e Redução de Custos TIC na Administração Pública (PGETIC), o qual foi aprovado pela RCM n.º 12/2012 (PCM, 2012a). Esse plano, com o desiderato de conseguir ganhos de poupança e eficiência, elencou 25 medidas estratégicas TI transversais a toda a AP e distribuídas por 5 eixos de atuação[2]. Da RCM n.º 12/2012 e do PGETIC é possível deduzir as seguintes oportunidades:

– "*Em cada ministério é identificado um organismo responsável pela coordenação das áreas das Tecnologias de Informação e Comunicação e nomeado o interlocutor único nessa área*" (PCM, 2012a, p. 596);

– O PGETIC estipula que "*cada ministério deverá elaborar a sua estratégia setorial, em cumprimento dos vetores estratégicos delineados*" (idem, p. 598). À data da realização do presente trabalho, o Plano de Ação Setorial (PAS) do MDN foi já enviado, estando a sua aprovação ainda pendente. O PAS foi coordenado pela SG-MDN tendo tido a colaboração do EMGFA e dos Ramos. Fora do domínio do PAS ficaram os sistemas de C2 militares, os quais serão alvo de um Plano Diretor de Sistemas específico;

[2] Eixos: (i) Melhoria dos mecanismos de governabilidade, (ii) Redução de custos, (iii) Utilização das TIC para potenciar a mudança e a modernização administrativa, (iv) implementação de soluções TIC comuns e (v) Estímulo ao crescimento económico.

– Ao nível da governação, o PGETIC preconiza "*um modelo que permita gerir de forma holística as TI*" (ibidem), em que esteja definida a autoridade e responsabilidade pela elaboração e implementação de políticas e normas que visem o alinhamento dos objetivos estratégicos das TI com os objetivos de negócio, tendo como referência três pilares: a Gestão da informação, os Sistemas TI e a Segurança da Informação;

– Garantir uma efetiva centralização da gestão das TI, ao nível da aquisição e gestão do ciclo de vida de todas as infraestruturas, comunicações e SI[3], em cada ministério, prevendo, para isso, a criação de um serviço de apoio e a unificação dos vários centros de processamento de dados, dos serviços de infraestrutura de rede, de administração e de governação;

– Estabelecer uma arquitetura SI/TI que sirva de guia para a sua conceção, aquisição, desenvolvimento, implementação e manutenção, e que inclua métricas de avaliação dos projetos;

– Definir e implementar uma metodologia de avaliação dos projetos e investimentos em TI de modo a garantir o retorno do investimento, numa ótica custo-benefício, e a evita dar a existência de redundâncias;

– Potenciar a interoperabilidade na AP, privilegiando o uso de uma plataforma central que concentre as redes dos diversos ministérios. Este desiderato está já plasmado, a nível militar, no Conceito Estratégico de Defesa Nacional, quando afirma que "*as Forças Armadas Portuguesas devem dispor de uma organização flexível e modular (...), privilegiando a interoperabilidade dos meios e, desejavelmente, com capacidades crescentes de (...) infraestruturas, comando, controlo, comunicações e informações*" (PCM, 2003, p. 286).

Por outro lado, o Despacho n.º 149/2012, de 12 de junho do MDN desencadeou o processo "*de reorganização da estrutura superior do Ministério da Defesa Nacional e das Forças Armadas, racionalizando órgãos e estruturas por forma a eliminar redundâncias desnecessárias (...)* " (MDN, 2012c, p. 2) entre os Serviços Centrais de suporte do MDN e as estruturas congéneres do EMGFA e dos Ramos e, por essa via, reduzir custos de funcionamento. Do supracitado despacho podemos inferir as seguintes oportunidades com aplicabilidade:

[3] Agregando a manutenção e desenvolvimento de todas as aplicações verticais do ministério.

– Incrementar a partilha das estruturas de direção e de comando e controlo do ministério e das FFAA;

– Incrementar, coordenar e explorar as sinergias entre as diferentes estruturas, numa lógica de partilha de recursos e boas práticas, que vise a racionalização do que é comum, uniformizando e padronizando procedimentos e processos, mas salvaguardando as especificidades de cada Ramo.

(2) Desafios

– O Governo Português, no âmbito do Programa de Assistência Económica e Financeira (PAEF), assumiu o compromisso de implementar uma estratégia que vise a "*racionalização da utilização das tecnologias de informação (TI) na administração central, através da implementação de serviços partilhados e da redução do número de entidades TI em ministérios ou outras entidades públicas*" (Governo, 2011, p. 16). Fruto das condicionantes do PAEF, o orçamento disponibilizado para a área das TI tem vindo a sofrer um decréscimo ao longo dos últimos 4 anos, correspondendo a uma redução de despesa com as TI de 33%, desde 2010 (SG, 2012, p. 12);

– O DL n.º 107/2012 de 18 de maio acomete à Agência para a Modernização Administrativa (AMA) a responsabilidade pelo "*processo de avaliação prévia, obrigatório e vinculativo, dos investimentos especialmente relevantes com a aquisição de bens e serviços no âmbito das TIC, com o objetivo de garantir que apenas são financiados e implementados os projetos que garantam um real contributo para o desenvolvimento e modernização da Administração (...)* " (PCM, 2012b, p. 2595), com aplicabilidade na aquisição de bens superiores a 10.000 euros, embora, no mesmo diploma, dispense desse procedimento a celebração de contratos secretos ou cuja execução seja acompanhada de medidas de segurança.

– A RCM n.º 12/2012 determina que o GPTIC "*identifica os sistemas operacionais críticos que ficam a regras específicas de salvaguarda, com vista à apresentação de planos sectoriais estratégicos (...) "* (PCM, 2012a, p. 596), tendo a RCM n.º 48/2012 de 12 de abril aprovado a listagem dos sistemas operacionais críticos na qual, paradoxalmente, não consta nenhum sistema da defesa (PCM, 2012c).

d. Síntese conclusiva

Neste capítulo, foi analisada a situação atual em que se encontram as TI da DN (*as is*), as oportunidades decorrentes da restruturação das TI da Administração Publica e da reorganização da estrutura superior da DN proposta pelo MDN, bem como os desafios de-

correntes da conjuntura económica que o país atravessa. Nesse sentido, foi descrito, através do enquadramento legal, qual o modelo organizacional e de governabilidade em uso pelas diversas entidades da DN.

Assim, constatou-se que cabe ao MDN integrar, coordenar e administrar os sistemas, serviços e tecnologias de informação e comunicações de gestão de todo o universo da Defesa Nacional, competindo ao EMGFA a gestão dos sistemas de C2 de cariz conjunto. No que respeita ao Ramos, verifica-se que, todos eles apresentam organizações distintas, com níveis de maturidade desiguais, o que por si só compromete a interoperabilidade e a identificação de potenciais sinergias.

Na avaliação do estado da arte recorreu-se a uma auditoria conduzida pela IGDN e a um questionário respondido pelas entidades envolvidas. Os dados recolhidos permitem deduzir, através de uma análise SWOT[4], os objetivos e linhas de ação indispensáveis à identificação que se pretende vir a efetuar de um modelo organizacional e de governabilidade das TI, centrado em torno da informação e do conhecimento e que contribua para que os objetivos estratégicos da DN sejam atingidos.

Das avaliações efetuadas, nomeadamente pela disparidade de níveis de maturidade dos processos considerados pelo COBIT, é possível deduzir que o atual modelo organizacional e de governabilidade das TI não é eficiente, não existe unidade de comando, nem é promovida a unidade de esforço. Desse modo, conclui-se que o atual modelo não permite uma racionalização dos recursos, não promove sinergias, não garante a segurança, e não fomenta a interoperabilidade, considerando-se validada e confirmada a Hip1, tendo sido dada resposta à QD1.

[4]Strenght, Weakness, Opportunities e Threats.

2. Modelos de outras organizações que possam servir de referência

A identificação de tendências e boas práticas a nível organizativo das TI, em uso por organizações que têm registado evoluções recentes nesta área, constitui um fator não despiciendo na edificação do modelo organizacional e de governação das TI da DN. Assim, neste capítulo, proceder-se-á à análise de alguns modelos implementados em organizações congéneres, com vista a aquilatar de que forma essas organizações têm abordado esta problemática.

a. Modelo organizacional da NATO

O funcionamento da NATO depende, sobremaneira, da sua capacidade ao nível de serviços de Comunicações e de Sistemas de Informação (CIS[5]), pelo que *" (...) o fornecimento de apoio TI efetivo às diversas entidades da Aliança, estáticas ou projetáveis, não só é um elemento crítico para assegurar o camando e controlo e a condução de operações lideradas pela NATO, como é também crucial para a condução das tarefas rotineiras da NATO*" (NATO, 2010, p. 2). É, assim, patente a importância que a organização devota à sua capacidade TI.

De forma a aumentar a eficiência e a eficácia da área das TI, foi aprovado, na cimeira de Lisboa, que se encetasse uma reforma das agências fornecedoras de serviços TI. Para o efeito, foram avaliados quatro possíveis modelos com base em cinco critérios de avaliação chave, nomeadamente, eficácia operacional, eficiência, governação e gestão, racionalização de recursos e riscos de transição, tendo o Comité Militar (CM) da NATO estabelecido, como pressuposto, que "*fossem mantidos diretamente sob o comando militar os serviços e capacidades TI projetáveis*" (idem, p. 4)

Por se considerar relevante para o estudo, nomeadamente na fase de identificação do modelo organizacional e de governação das TI que melhor se adeque à DN, analisar-se-á, não só o modelo implementado, como, também, os restantes modelos que foram considerados.

(1) Modelo 1 - baseado no relatório do *Senior Officials Group* (SOG)

O modelo baseado no relatório do SOG prevê a criação de duas estruturas distintas, embora com o mesmo campo de atuação: um grupo de 2.100 elementos, sob o comando do SACEUR, com responsabilidade pelos serviços TI de todos os comandos NATO; e uma

[5]Communications and Information Systems, passando a ser usado no âmbito deste estudo a sigla TI

Agência C&I responsável pelos mesmos serviços em todas as restantes estruturas da NATO (idem, p. 10). Este modelo, que à partida permitiria uma resposta mais efetiva aos requisitos chave do SACEUR, apresenta como desvantagem o fato de alguns dos seus requisitos não serem assegurados pelo grupo das TI a criar, nomeadamente, o CIS Logistics Depot (CLD) e os seis Data Communication Module (DCM), que ficariam a cargo das nações. Por outro lado, este modelo permitiria uma rápida implementação, sem riscos e com baixos custos associados, estabelecendo, de forma clara, as responsabilidades de cada órgão. É um modelo que conduziria, inevitavelmente, à duplicação de estruturas, carecendo, consequentemente, de unidade de esforço e de comando.

(2) Modelo 2 - baseado na *Internacional Business Machines Corporation* (IBM)

À semelhança do modelo anterior, o modelo baseado na IBM apresenta, também, dois fornecedores de serviços: uma "Agência C&I"; e um "centro de serviços partilhados". Este último seria responsável, transversalmente à Aliança, por todos os serviços comuns, nos domínios dos recursos humanos, aquisição e apoio TI, e nos quais se incluem a gestão da rede NATO e a ciberdefesa. A "*Agência C&I"* assumiria a responsabilidade *"dos serviços especializados para uso, quer nos ambientes estáticos como projetáveis*" (idem, p. 10), do CLD e dos DCM's.

Uma vez que nenhuma destas duas entidades estaria sob o comando direto do SACEUR, o modelo obrigaria a que fossem encontradas soluções que assegurassem o cumprimento dos requisitos TI durante a condução de operações, as quais poderiam passar por uma transferência de controlo da agência para o SACEUR. Por outro lado, permitiria uma prestação de serviços coerente e eficiente, transversalmente a toda a Aliança, bem como uma significativa poupança de recursos, tendo, no entanto, como desvantagens, a pouca consideração das necessidades do ambiente operacional e a necessidade de grandes mudanças nas estruturas civis e militares, com os elevados riscos de transição associados. A ter em conta, igualmente, o facto de que a separação dos serviços TI em duas entidades viria dificultar, de sobremaneira, a governação e a gestão das TI.

(3) Modelo 3 - Agência única

Este modelo, claramente centralizado, prevê uma agência única responsável pela "*gestão do ciclo de vida total dos serviços TI*" (idem, p. 11), absorvendo os CLD e os seis DCM's. Tal como no modelo anterior, o facto de o SACEUR não ter comando direto sobre os meios TI necessários ao cumprimento da sua missão operacional obrigaria a que fossem

estabelecidos acordos com a "Agência C&I" para a transferência operacional dos meios com vista à satisfação dos requisitos operacionais. No entanto, este modelo "*fornece oportunidades significativas para a coerência, sinergia e eficiência no fornecimento dos serviços TI a todas as entidades através de uma aproximação de ciclo de vida total*" (ibidem), diminuindo o risco de duplicação e permitindo poupanças significativas. Por outro lado, a centralização do fornecimento dos serviços numa agência única requereria uma adequada estrutura de governação para não se correr o risco "*da atenção da agência C&I nas operações militares seja reduzida ao longo do tempo, resultando num abaixamento dos níveis de serviço e degradação da satisfação dos utilizadores*" (ibidem). O modelo não era absolutamente claro sob a forma como, a curto prazo, seria alcançado o necessário equilíbrio entre os requisitos chave do SACEUR e os dos outros atores, como por exemplo, o Secretário-geral. Este modelo é o que menos satisfaz os critérios chave de avaliação, uma vez que a sua eficácia é questionável e os custos e os riscos de transição seriam elevados.

(4) Modelo 4 – Modelo híbrido

O quarto e último modelo analisado, designado por Modelo Híbrido, foi o que melhor respondeu aos critérios chave de avaliação tendo sido, por esse motivo, implementado na NATO. O modelo baseia-se em dois fornecedores de serviços, a "Agência C&I", responsável pelos serviços TI das estruturas civis e militares estáticas da organização, agregando todas as agências de comunicações e de sistemas de informação que existiam na NATO, e um "grupo das TI destacável" que, sob o comando do SACEUR, suporta a estrutura projetada da NATO, sendo responsável, perante a Aliança, por toda a infraestrutura e serviços de rede, bem como pelos serviços de ciberdefesa e segurança da informação. É, igualmente, responsável pelos CLD e pelos seis DCMs.

Embora o SACEUR tenha na sua linha de comando o "grupo das TI destacável", no que concerne à "Agência C&I", subsiste a necessidade, à semelhança do modelo anterior, de serem estabelecidos acordos com vista à utilização de alguns serviços TI de posições estáticas que sejam identificados como necessários ao cumprimento da missão operacional. Seguindo uma lógica "*apoiada numa aproximação orientada para o utilizador e numa aproximação funcional TI*" (idem p. 12), permite racionalizar os respetivos meios e recursos, emprestando, em simultâneo, maior coerência e eficiência a estes mesmos serviços e gerando a consequente redução de custos. As grandes vantagens que relevam deste modelo resultam do facto de "*satisfazer todos os requisitos chave do SACEUR através de uma es-*

trutura única, responsiva e focada" (ibidem), colmatando, nomeadamente, a sua atual incapacidade para gerar requisitos de utilizador.

Embora de conceito semelhante ao modelo 1, também ele híbrido, este quarto modelo apresenta uma diferença significativa. No modelo 1, a responsabilidade de gestão da rede NATO e do fornecimento de serviços de cibernética e da segurança da informação de toda a Aliança não permaneciam sob a alçada do grupo das TI e, desta forma, sob comando do SACEUR.

Na prática, veio a constatar-se que a transição para esta nova estrutura decorreu de forma rápida, com custos mínimos e sem riscos de transição na sua implementação. De referir, no entanto, que este modelo terá que assentar num processo de governação bem estruturado para não se correr o risco de, face à separação dos serviços TI destacáveis dos serviços TI estáticos, vir a ocorrer, futuramente, uma divergência das aproximações às questões técnicas, com a correspondente perda de coerência. Este modelo obedece ao pressuposto do CM da NATO manter as capacidades TI projetáveis sob comando direto do SACEUR.

Para garantir que o produto gerado por esta estrutura está alinhado com os objetivos estratégicos e operacionais estabelecidos, respetivamente, pelo *North Atlantic Council* e pelo CM, existe um órgão de governação das TI da NATO, o designado C3 Board (C3B), onde se encontram representadas todas as nações aliadas, os comandos estratégicos da NATO e a agência criada para o efeito (NC&IA), e do qual dependem grupos especialistas, nas diversas componentes da NAF[6].

b. Modelo organizacional das TI da Defesa Australiana

A Austrália encetou, em 2007, um programa de reforma estratégica das TI da Defesa, com a finalidade de alinhar os investimentos e objetivos estratégicos das TI com os requisitos estratégicos da Defesa. Para o efeito, foi aprovado, pelo Ministro da Defesa, o documento estruturante que estabelece a estratégia das TI da Defesa[7], a qual assenta em dois pilares:

– Criação de um Ambiente Único de Informação (AUI), de grande capacidade e transversal a todos os domínios (marítimo, terrestre, aéreo e *Intelligence, Surveillance* e *Reconaissance),* que ligue toda a Defesa com vista a garantir a satisfação das necessidades

[6] NATO Architecture Framework
[7] Defence Information and Communications Technology Strategy 2009

de comunicação do pessoal militar, nos teatros de operações, e a transferência segura de informação com os seus aliados.

– Atribuição de carácter prioritário a uma aproximação conjunta no que se refere a projetos das capacidades e sistemas de cada Ramo.

Desse mesmo documento é possível extrair os imperativos estratégicos determinantes em que se baseia o modelo organizacional das TI da Defesa:

– Maximização do retorno do investimento nas TI;

– Desenvolvimento de um modelo de organização centrado nos utilizadores;

– Edificação de um modelo de operação das TI transversal à Defesa e com uma arquitetura que promova a padronização e a consolidação;

– Fortalecimento das capacidades das TI através de melhorias na cultura, liderança, processos, técnicas e planeamento de recursos.

Para a sua implementação, foi criado, a nível estratégico, um comité das TI denominado *Defence ICT Committee* (DICTC), da qual fazem parte o Secretário de Estado da Defesa, o Chief of Defense (CHOD) e os restantes dirigentes da estrutura de topo da Defesa. A principal preocupação desta comissão é promover as orientações estratégicas para o investimento em capacidades TI, sendo responsável por garantir que as despesas estão alinhadas com as prioridades da Defesa. Para o efeito, a DICTC "*revê e estabelece prioridades para todas as iniciativas e investimentos em TI*" (DoD, 2009, p. 8).

A identificação, por esta comissão, de lacunas na governação das TI da Defesa, deu origem a criação do Chief Information Officer (CIO) como gestor/coordenador das capacidades de todo o ambiente de informação da Defesa. É responsabilidade do CIO, que, para o efeito, responde perante o Secretário de Estado da Defesa e perante o CHOD "*desenvolver um ambiente de informação único na Defesa, controlar os custos de sustentação e garantir que a Defesa obtém vantagem das tecnologias emergentes*" (idem, p.7). Posteriormente, a referida comissão atribuiu, igualmente, ao CIO, responsabilidades acrescidas, nomeadamente no desenvolvimento de políticas, conceitos e doutrina das TI da Defesa e em garantir que estas sejam interoperáveis com outros organismos da AP, aliados e parceiros de coligação.

O CIO apoia-se numa estrutura denominada CIO Group (CIOG), responsável por assegurar *"(...) que a defesa possui um ambiente de informação único, integrado e seguro que seja capaz de apoiar as funções de negócio, Intelligence e militares da Defesa*" (ANAO, 2011, p. 34).

Na figura 6 apresentam-se os diversos níveis do ambiente de informação. O CIOG é responsável pela gestão dos serviços conjuntos, cabendo aos Ramos a administração dos serviços específicos. Desta forma, o CIOG administra a rede restrita e a rede secreta da Defesa, competindo aos Ramos a gestão das redes de comando e controlo específicas. No que respeita à informação, o CIOG é responsável pela informação que tem a ver com o conjunto e os Ramos pela de apoio à capacidade de gestão estratégica específica. O CIOG é, igualmente, responsável pelo interface das redes específicas dos Ramos com as redes a seu cargo.

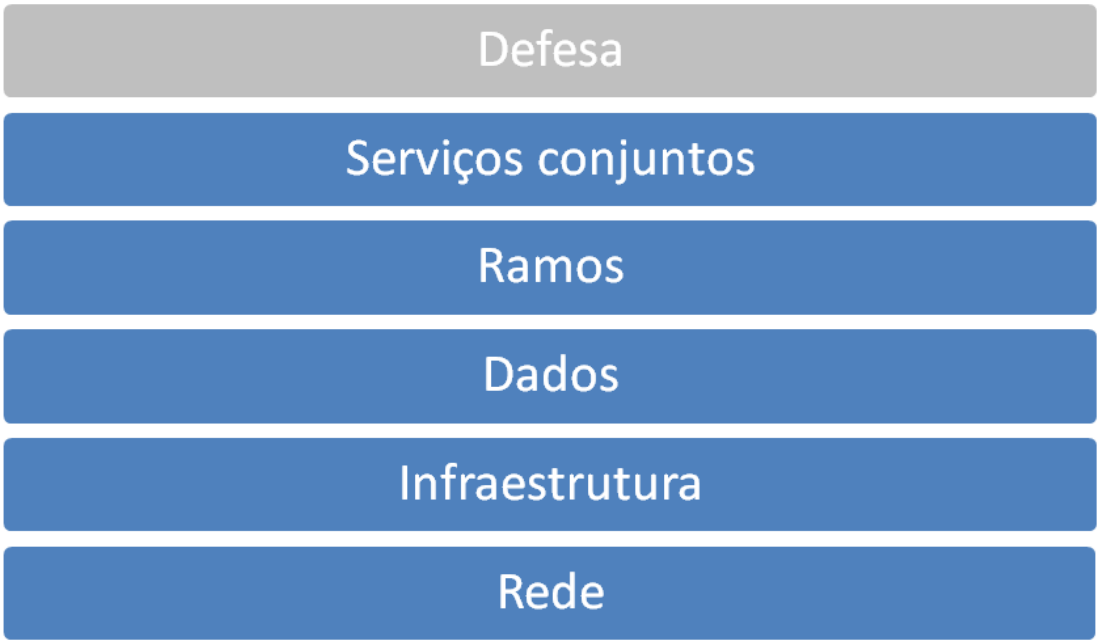


Figura 6 Níveis do Ambiente de Informação
Fonte: (ANAO, 2011) adaptado

No processo de aquisição de sistemas TI, a Defesa Australiana classifica as necessidades de negócio segundo quatro pilares (*Intelligence*, militar, corporativo e infraestruturas), cada um da responsabilidade de uma comissão distinta, garantindo o envolvimento dos utilizadores, em particular dos Ramos, e transparência no investimento:

Cada comissão integra membros dos Ramos e das Direções, representando aquilo que se poderá designar por "voz do cliente". Das suas funções destaca-se "*assegurar que as necessidades de negócio dos utilizadores são levadas em conta, que os seus requisitos são compreendidos no desenvolvimento de propostas para novas capacidades TI*" (ANAO, 2011, p. 53). Estas comissões são apoiadas por um *Stakeholder Engagement Team* (SET), edificado a partir da estrutura do CIOG, com a responsabilidade de "*traduzir as priorida-*

des e requisitos dos atores em requisitos de negócio, procurando inicialmente uma solução dentro das capacidades existentes para que sejam evitadas duplicações" (DoD, 2009, p. 23).

A Defesa australiana aborda as TI sobre uma perspetiva matricial, seguindo o modelo apresentado na figura 7.

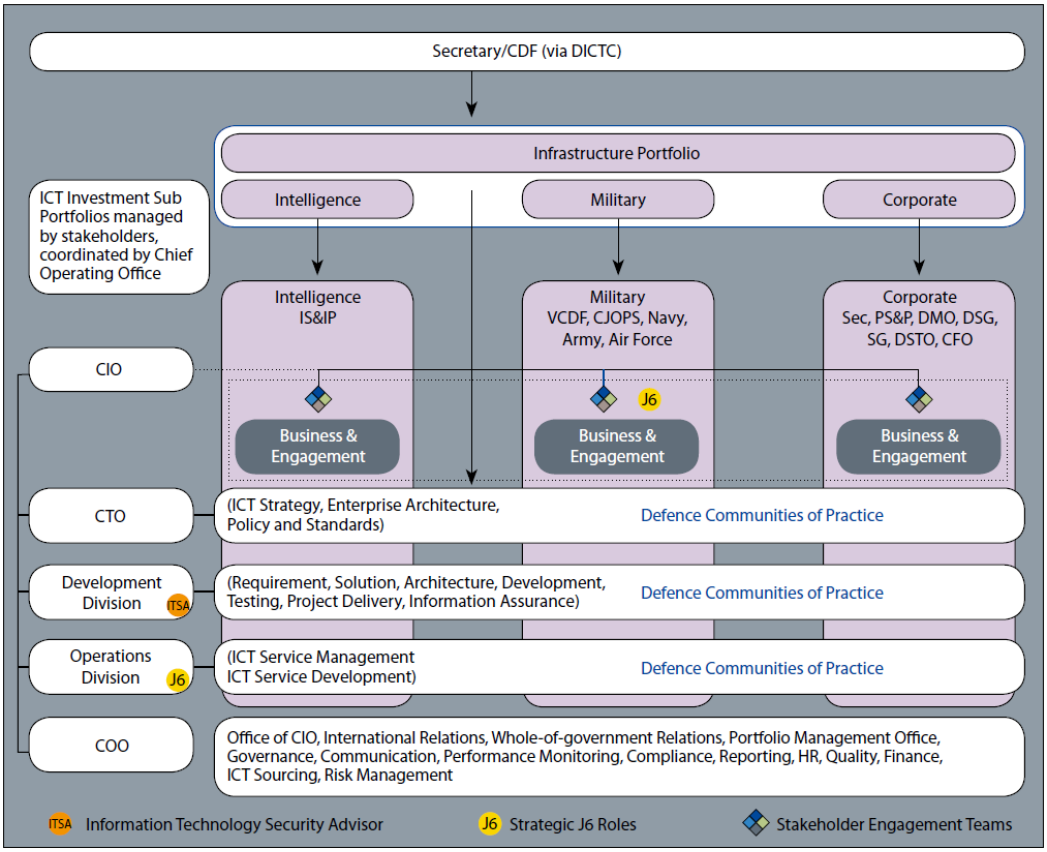


Figura 7 – Modelo Matricial das TI da Defesa Australiana

Fonte: (ANAO, 2011) adaptado

As faixas horizontais ilustram todas as capacidades e recursos TI, alinhados com o planeamento, edificação, gestão e governação. As barras verticais representam os sub-portfolios. Os requisitos de negócio são priorizados e acordados, no DICTC, transversalmente a todo o portfolio TIC da Defesa. Cada sub-portfolio será convertido em requisitos de negócio pelo SET. Com este imperativo, a Defesa "*pretende migrar para um modelo organizacional alinhado com os Ramos e Direções, aumentando a comunicação entre os fornecedores das capacidades TI e os utilizadores, permitindo ter uma maior consciencialização dos serviços TI requeridos e consumidos em toda a defesa*" (DoD, 2009, p. 23).

Por fim, a nível organizacional, o CIOG, chefiado pelo CIO, integra divisões responsáveis por gerir as capacidades do ambiente da informação da Defesa, nomeadamente o

planeamento, priorização, desenvolvimento, implementação e sustentabilidade das capacidades TI. A figura seguinte corresponde ao organograma do CIOG:

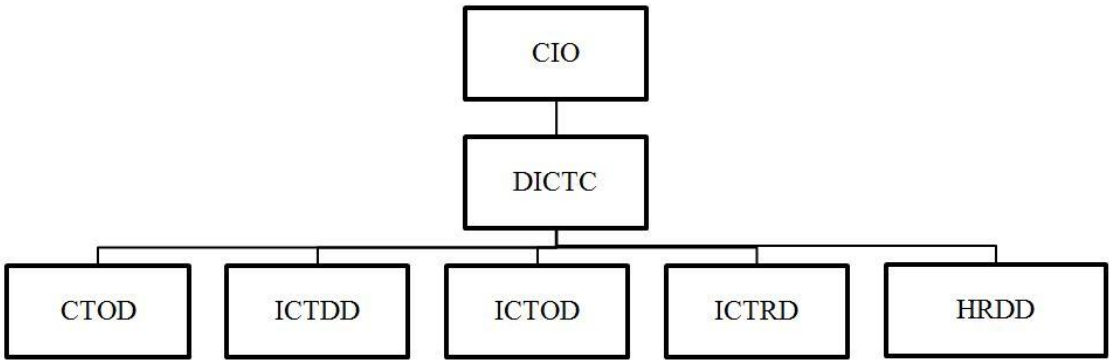


Figura 8 – Organograma da área do CIO da Defesa Australiana

Fonte: (Autor, 2012)

– *Chief Technology Officer Division* (CTOD), responsável pela arquitetura (empresarial e de infraestrutura) das TI da Defesa, por garantir o fornecimento de sistemas e aplicações TI, em linha com os objetivos e a estratégia da Defesa, e por proporcionar orientações e apoio aos projetos estratégicos, assegurando que as aplicações são criadas e implementadas de acordo com a arquitetura estabelecida pelo CIO;

– *Information and Communications Technology Development Division* (ICTDD), com responsabilidade no desenho arquitetural, desenvolvimento e apoio de terceiro nível no âmbito do ambiente de informação único da Defesa, bem como também na edificação do SET corporativo;

– *Information and Communications Technology Operations Division* (ICTOD) / J6, responsável por providenciar um ambiente de informação de capacidade global, incluindo a disponibilização de comunicações satélite, espectro eletromagnético e rede para apoio de operações militares. O chefe da divisão é o principal conselheiro estratégico do CHOD no âmbito dos sistemas de informação e comunicações e da utilização do espectro eletromagnético;

– *Information and Communications Technology Reform Division* (ICTRD), com responsabilidade no desenvolvimento e implementação do programa de reforma das TI da Defesa, com vista a reduzir os custos com as capacidades TI;

– *Human Resource Development Division* (HRDD), responsável pela gestão dos recursos humanos da área das TI.

c. Modelo organizacional das TI do Reino Unido

A estratégia das TI da Defesa Britânica foi desenhada com o intuito de " *alinhar as áreas operacionais com as de negócio (...) para que o fornecimento de serviços TI seja mais eficiente e efetivo*" (MoD, 2010, p. 4), garantindo o melhor retorno dos investimentos, uma melhor adaptação às mudanças de requisitos dos ambientes operacionais e de negócio e o acompanhamento constante dos avanços tecnológicos. No que concerne à edificação de capacidades TI, a Defesa Britânica apoia-se em quatro pilares:

– O perfeito alinhamento dos requisitos para o investimento com os objetivos estratégicos da Defesa, permitindo que "*os processos operacionais e de negócio sejam mais efetivos, eficientes e ágeis (...) permitindo a redução dos custos anuais com as TI*" (idem, p. 3);

– A potenciação do uso de capacidades de TI comuns, sempre que "*os requisitos sejam transversais a toda a Defesa, a outros departamentos governamentais, aos países Aliados e à indústria*" (ibidem), tendo, contudo, sempre presente que os objetivos da defesa são prioritários;

– A centralização da gestão dos orçamentos e dos investimentos, de modo a que os custos de funcionamento sejam reduzidos,

– Investimentos feitos de acordo com princípios orientadores comuns, que permitam a redução de custos através de medidas como a reutilização de serviços existentes, de modo a encontrar o equilíbrio desejável entre risco e benefício.

Com esta estratégia, a Defesa Britânica pretende, nos próximos anos, "*aumentar significativamente o uso de sistemas TI comuns, apenas permitindo o uso de serviços TI específicos onde os requisitos da defesa forem específicos, tais como operacionais, segurança e Intelligence*" (idem, p. 8), como sumarizado na Figura 9.

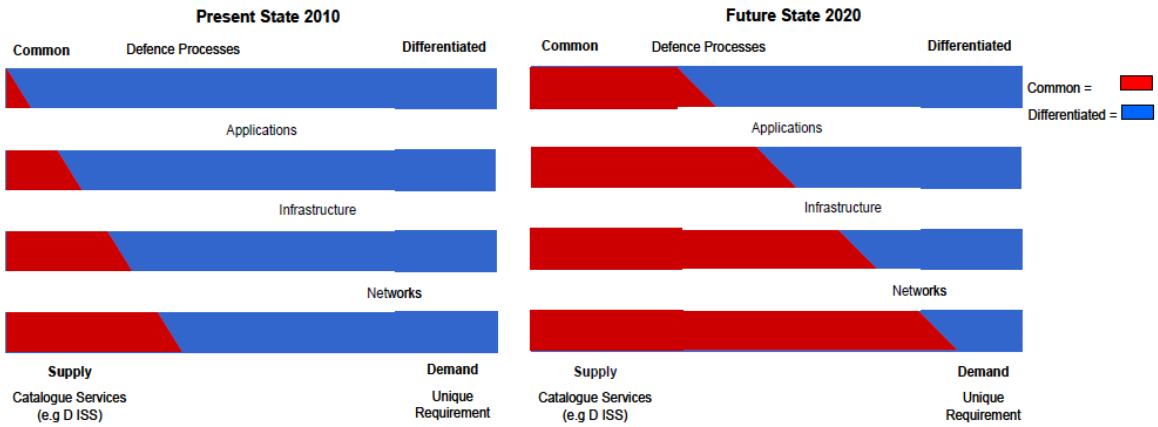


Figura 9 – Evolução da despesa com as TI na Defesa do Reino Unido

Fonte: (MOD, 2010)

Ao nível da governação, o CIO é responsável pela implementação da estratégia das TI da Defesa e das políticas relacionadas, tendo, para o efeito, definido os princípios orientadores dos serviços TI, de modo a garantir que "*os sistemas são coerentes pelo uso de uma arquitetura empresarial que ligue o negócio com os requisitos das TI assegurando uma solução completa, lógica e coerente*" (idem, p. 12), ou seja, que os processos de operação da defesa decorram sem problemas, alavancados por serviços TI eficientes e com um custo efetivo aceitável. Por se considerar elucidativo, apresentam-se, seguidamente, os princípios orientadores do CIO para as TI da Defesa, deduzidos do documento estratégico das TI da Defesa. Assim, a Defesa deverá adotar:

– Uma aproximação arquitetural na aquisição e uso das TI, permitindo que as necessidades operacionais e de negócio possam ser planeadas, compreendidas e fornecidas coerentemente;

– O uso de padrões comuns na arquitetura, de modo a facilitar o fornecimento de serviços TI e a sua interoperabilidade;

– O uso de processos e serviços comuns alinhados transversalmente no âmbito da Defesa e dos diversos departamentos do Governo;

– O fornecimento de aplicações comuns de um portfólio gerido de forma a maximizar a reutilização de aplicações, a exploração de aplicações prontas a utilizar, minimizando a dependência de soluções personalizadas;

– Uma gestão efetiva das redes e infraestrutura, privilegiando a segurança, sustentabilidade e o carácter comum a toda a Defesa, departamentos governamentais e países Aliados, sempre que apropriado;

– Um quadro de pessoal com as perícias necessárias à exploração das capacidades fornecidas e que desempenhem as suas responsabilidades de uma forma mais efetiva;

– Uma estrutura efetiva para a governação, aquisição e gestão das TI, de modo a satisfazer as necessidades da Defesa, tais como a redução de custos, a maximização dos efeitos e a minimização dos riscos operacionais.

Com vista à implementação destes princípios orientadores, em especial no que se refere ao objetivo estratégico de assegurar que os serviços TI assumam um carácter transversal a toda a Defesa e aos outros departamentos governamentais, o CIO tem à sua disposição o CIO *Systems Direction Group* (SDG), cuja organização, bastante similar à adotada pela Defesa Australiana, está materializada na Figura 10.

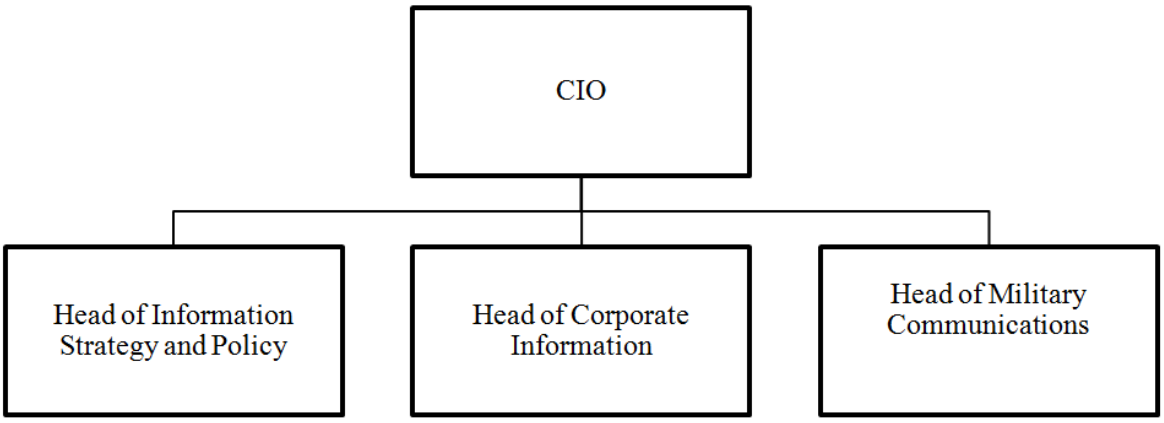


Figura 10 – Organograma da área do CIO da Defesa do Reino Unido

Fonte: Defence ICT Strategy

Com o objetivo de melhorar o fornecimento dos serviços TI, o CIO delegou, quer a administração das redes da Defesa, quer o desenvolvimento de capacidades TI, nas seguintes três autoridades:

– *Network Capability Authority* (NCA), que assegura a coerência de futuros investimentos em capacidades TI, bem como a identificação dos requisitos de informação necessários para apoiar o NTA no desenvolvimento de novas capacidades;

– *Network Technical Authority* (NTA), que assegura a coerência técnica da rede e os desenvolvimentos futuros da rede da Defesa. É igualmente responsável pela gestão dos elementos de *Command, Control, Communications and Computing* (C4) da rede

conjunta da Defesa, e, como atrás referido, pela materialização dos requisitos de capacidades desenvolvidos pelo NCA;

– *Network Operating Authority*, responsável pela operação segura e efetiva da rede. Para isso, "*fornecerá a configuração operacional e a gestão da rede de defesa e da defesa contra os Ciberataques*" (idem, p. 13).

Para aumentar a eficiência e a transversalidade das TI nos diferentes departamentos do governo, foi criado, a nível governamental, o "conselho dos CIO", no qual o CIO da Defesa tem acento. A presença do CIO da Defesa neste conselho visa assegurar que os interesses e ideias do departamento são tidos em conta nas iniciativas governamentais e que estas sejam compreendidas e implementadas dentro da defesa.

d. Síntese conclusiva

A análise efetuada a três organizações do âmbito da Defesa permite concluir que a utilização de um modelo híbrido para a governação e gestão das TI da Defesa é comum a todas elas.

A governação das TI da Defesa tem como principal finalidade alinhar os objetivos estratégicos das TI com os objetivos de negócio da organização, potenciando o uso de capacidades comuns, transversais a toda a Defesa, a outros departamentos governamentais, a países Aliados e à indústria, mas tendo sempre presente que os requisitos da Defesa são prioritários.

Foi também possível identificar, em todos os casos objeto de análise, a existência de uma estrutura, ao nível estratégico, que viabiliza a gestão estratégica das TI. Estas estruturas, embora com conceitos diferentes ao nível da sua constituição, têm em comum a figura do CIO (na NATO materializada na figura da agência) como responsável pela implementação da estratégia das TI da defesa, pelo desenvolvimento de políticas, conceitos e doutrina das TI e pela gestão dos serviços nucleares e de rede transversais à Defesa.

Quanto à governação, a NATO apresenta o C3B onde estão representadas as nações, os comandos estratégicos e a recém criada agência. A Defesa australiana tem constituído um *Defence ICT Committee* que envolve toda a estrutura da Defesa (CHOD, Secretário de Estado da Defesa, Ramos e Direções) e o CIO. No caso britânico, o CIO é apoiado na governação pelo *Systems Direction Group*, com um carácter mais especializado.

A estrutura do CIO é apoiada, no que concerne ao desenvolvimento e edificação de capacidades TI, por grupos de trabalho nos quais estão representados os utilizadores (Ramos e Direções), com o objetivo de garantir que estes sejam envolvidos ao longo de todo o

processo. Cabe aos Ramos e, no caso da NATO, ao SACEUR, a gestão dos sistemas de comando e controlo específicos e a administração dos serviços específicos de apoio à decisão.

Assim, ao verificar que o modelo híbrido de governação das TI tem prevalência considera-se validada e confirmada a Hip2, e consequentemente dá-se por respondida a QD2.

3. Critérios de Avaliação

A escolha de um modelo organizacional e de governação das TI, que se deseja otimizado para um AUI, alicerçado na transversalidade a nível de toda a Defesa e suportando utilizadores dispersos geograficamente, passa, antes de mais, pela dedução de critérios de avaliação objetivos, de cariz essencialmente estratégico, gestionário e operacional. Neste sentido, consiste objetivo deste capítulo a identificação dos critérios de avaliação a que o modelo a implementar para as TI da Defesa deverá responder.

a. Governação das TI

De acordo com o ITGI, o uso das TI tem potencial para ser o principal impulsionador da economia no século XXI. Parece ser ponto assente que o valor das empresas deixou de ser medido por ativos tangíveis (tecnologia) para passar a considerar ativos intangíveis (informação, conhecimento, confiança, etc.), todos eles com a sua génese nas TI. Daí que, na opinião de diversos autores, uma boa governação das TI seja crítica para o sucesso de uma organização.

A governação, cuja definição foi já apresentada na introdução, visa sobretudo estabelecer a estratégia das TI, gerindo os riscos da sua operacionalização e tendo, como objetivo final, que estas gerem valor para a organização. Assim, a governação não se pode circunscrever, apenas, às próprias TI, mas sim fazer parte da governação global da organização. É vital que a governação das TI assente numa "*comunicação efetiva entre todas as partes baseada em relações construtivas, numa linguagem comum e num comprometimento partilhado na abordagem aos assuntos relacionados com as TI*" (ITGI, 2003, p. 11), de modo a que seja efetiva, transparente e responsável.

Por esse motivo, a responsabilidade da governação TI, ao nível estratégico, é, nas melhores práticas da indústria, atribuída a um *IT Strategy Committee*[8], envolvendo toda a estrutura superior da organização, e que pauta a sua atuação por alinhar a estratégia das TI com a estratégia da organização. A este respeito, Loggeremberg, citando Exler, refere que "*o sucesso da estratégia de uma organização depende de sobremaneira em como os gestores integram as TI no ambiente da organização*" (Loggerenberg, 2006, p. 2). Como já anteriormente constatado, este conceito é também usado pelas organizações militares estudadas no capítulo 2. Na NATO, com o C3B, na Defesa Australiana, com o *Defence ICT Stra-*

[8] Por uma questão de uniformização com a nomenclatura a utilizar no modelo a propor para as TI da DN, passará no âmbito deste trabalho, a ser designado por Comité de Governação Estratégico

tegy Committee e, no caso Britânico, com o *Systems Direction Group*. No entanto, e não obstante a governação das TI ser responsabilidade dos membros do Comité de Governação Estratégico (CGE), as atividades da governação deverão ocorrer transversalmente, em todos os níveis da organização. À semelhança do que acontece ao nível executivo, é estabelecido o *IT Steering Committee*[9] com o objetivo de "*rastrear os investimentos das TI, estabelecer prioridades e em alocar os escassos recursos disponíveis*" (ITGI, 2003, p. 16). A Defesa Australiana, com os SET, é um exemplo da aplicação deste conceito.

O processo da governação inicia-se no âmbito do CGE com a definição dos objetivos para as TI e o estabelecimento de orientações estratégicas iniciais. Posteriormente, a área funcional das TI, em resposta às orientações recebidas, concentra-se "*em realizar valor através do aumento dos processos automatizados e em tornar a organização mais efetiva, em reduzir os custos e fazer a organização mais eficiente, e em gerir os riscos (segurança, confiança e observância)* " (ITGI, 2003, p. 13).

De acordo com o ITGI, a governação das TI foca-se em duas realidades, às quais devem ser alocados os recursos e as métricas de avaliação necessárias: que as TI acrescentem valor à organização, através do seu alinhamento estratégico com o negócio da organização; e que os riscos TI sejam mitigados através da responsabilização. Para atingir esse desiderato, a governação das TI abrange a cultura, a organização, as políticas e os procedimentos que proporcionam a gestão e controlo das TI, em cinco áreas chave, que se passarão a desenvolver.

(1) Alinhamento estratégico

Segundo Duffy citado por Grembergen, o alinhamento estratégico é "*o processo e o objetivo de alcançar vantagem competitiva através do desenvolvimento e sustentação de uma relação simbiótica entre o negócio e as TI*" (Grembergen, 2004b, p. 7). Para concretizar este objetivo Henderson e Venkatraman desenvolveram um modelo, *o Strategic Alignemet Model* (SAM), que identifica a necessidade de integração entre os domínios das TI e do negócio, ao nível estratégico e ao nível operacional.

O primeiro é "*a ligação entre a estratégia de negócio e a estratégia das TI refletindo as componentes externas*" (Venkatraman, 1999, p. 412) de modo a que as TI suportem e formatem a estratégia de negócio da organização. O segundo, "*lida com os corresponden-*

[9] Por uma questão de uniformização com a nomenclatura a utilizar no modelo a propor para as TI da DN, passará no âmbito deste trabalho, a ser designado por Comité de Governação Executivo

tes domínios internos, nomeadamente, a ligação entre os processos e estrutura organizacional e os processos e estruturas TI" (ibidem), por forma a assegurar a coerência interna entre os requisitos da organização e o fornecimento das capacidades TI.

O domínio interno, âmbito deste estudo, deve abordar três componentes: arquitetura, processos e perícias TI. Como se pode inferir do anteriormente exposto, o alinhamento estratégico visa, essencialmente, providenciar orientações para as TI e garantir que estas estejam alinhadas com o negócio, no que diz respeito aos serviços e projetos. Por alinhamento entende-se, não só a integração ao nível estratégico, mas também, o alinhamento das operações TI com as operações correntes da organização. Os TI, desde que objeto de uma adequada governação contribuem para que a organização disponha de superioridade da informação, para que os custos sejam reduzidos e para um aumento da eficiência administrativa e da eficácia gestionária

Na elaboração da estratégia das TI deverão ser contemplados os objetivos de negócio, as tecnologias em uso e a sua evolução futura, a avaliação dos custos associados, riscos e benefícios, e, igualmente, incorporadas as lições aprendidas. Competirá ao CGE assegurar que a estratégia implementada seja continuamente revista, de modo a que se adapte às mudanças de tecnologia ou dos objetivos da organização.

Para medirem o grau de alinhamento estratégico, as organizações têm à sua disposição modelos de maturidade, os quais permitem uma aferição com base na comparação com as melhores práticas e padrões da indústria. No presente trabalho, foi utilizado o COBIT que, por recurso a uma autoavaliação, possibilitou determinar o "*as is*" da Defesa e escalpelizar o "*to be*".

(2) Criação de Valor

Para a organização, a criação de valor traduz-se na otimização dos investimentos feitos nas TI, segundo os princípios básicos de "*providenciar, atempadamente e dentro do valor orçamentado, a qualidade necessária que permita alcançar os benefícios prometidos*" (ITGI, 2003, p. 25), que resultam na superioridade da informação, na interoperabilidade e no apoio efetivo às missões operacionais da organização. Para que a criação do valor seja efetiva, terá, antes de mais, que existir uma gestão criteriosa dos custos, um retorno garantido do investimento e as áreas funcionais das TI e do negócio estarem alinhadas.

De acordo com Broadbent e Weill, existem quatro níveis de criação de valor. O primeiro nível é providenciado pela disponibilidade da infraestrutura TI e pelo custo por cada posto de trabalho. O segundo nível tem a ver com o custo e tempo de implementação

de novas aplicações, enquanto o terceiro nível é obtido pelo desempenho operacional do negócio. O último nível situa-se na avaliação do retorno dos ativos. A chave para o sucesso da criação de valor prende-se com a avaliação dos investimentos nos primeiros dois níveis e com a avaliação do desempenho nos quatro níveis (P.Weill, 1998, p. 9).

(3) Gestão de Risco

No âmbito das TI, a gestão de risco refere-se "*à salvaguarda dos ativos TI e à recuperação de desastres. A gestão de risco consagra a segurança TI para a proteção dos ativos e em permitir que o negócio recupere de eventuais falhas. Permite privacidade para os utilizadores e edifica resiliência nos sistemas*" (Guldentops, 2002). Atualmente, as organizações estão particularmente atentas aos riscos operacionais e sistémicos, nos quais se incluem o risco tecnológico e a segurança da informação. Para fazer face a estes desafios, o CGE deverá:

– Definir políticas que caracterizem a forma com que a organização pretende lidar com o risco (mitigar ou aceitar), tendo a consciência de que a responsabilidade final pela gestão do risco recai em si própria;

– Implementar um sistema interno de controlo que, em última instância, tenha potencialidades para gerar custo-eficiência e, por fim,

– Garantir que a gestão de risco esteja incorporada, de uma forma intrínseca, na organização. Ou seja, a gestão de risco tem a ver com a preservação do valor criado pelas TI.

(4) Gestão de Recursos

A gestão de recursos que, como seria expetável, constitui um fator chave para o sucesso de uma organização, consiste no investimento otimizado em capacidades TI e no uso e alocação dos recursos TI[10] cuja atividade tenha por objetivo satisfazer as necessidades de negócio. Neste sentido, o CGE deverá assegurar que estão a ser utilizados os métodos apropriados, que os projetos são geridos ao longo de todo o ciclo de vida por pessoal possuidor das valências necessárias para o fazer, e que os investimentos em recursos contribuem para gerar valor acrescentado à organização.

[10] Por recursos TI entende-se pessoal, aplicações, tecnologia, infraestruturas, dados.

Ao nível da gestão, "*os ativos TI deverão estar organizados de modo a fornecer a qualidade de serviço requerida através de uma infraestrutura com o melhor custo-eficácia*" (ITGI, 2003, p. 28).

(5) Avaliação de Desempenho

No âmbito das TI, a avaliação de desempenho é conduzida em dois planos: no acompanhamento dos projetos e na monitorização dos serviços TI. Como anteriormente referido, o valor das organizações está a passar de ativos tangíveis para os ativos intangíveis, tornando impraticável que as métricas para a avaliação de desempenho tenham como base os meios financeiros tradicionais. As organizações modernas recorrem à elaboração de *Balenced Scorecards*, introduzidos pela primeira vez por Kaplan & Norton, os quais têm como premissa fundamental que "*a avaliação da organização não deve ser restrita a uma avaliação financeira tradicional mas deve ser ampliada com medidas relacionadas com a satisfação dos utilizadores, processos internos, e capacidade para inovar*" (Kaplan, 1996, p. 16). No entanto, é importante que sejam estabelecidas, em conjunto com as duas perspetivas, as métricas para avaliação da criação de valor (*Balanced Scorecard*), e que estas sejam entendidas transversalmente por toda a organização.

A governação das TI, embora transversal a toda a organização, tem a sua génese no nível estratégico (de que resultarão atividades de governação para os restantes níveis da organização), constituindo, por esse mesmo motivo, o critério com maior peso na definição do modelo das TI a implementar no universo da Defesa. Os critérios agora apresentados, embora com aplicabilidade ao nível estratégico, têm maior enfoque no nível gestionário e operacional, porque são esses os domínios onde a estratégia tem o seu impacto e se materializa.

b. Melhorar a Eficácia Operacional

O ambiente de informação que, atualmente, carateriza a Defesa, baseia-se em serviços e redes com enfoque nos Ramos, particularmente no que se refere aos processos de gestão de acessos, centros de dados, aplicações, *software* e *hardware*, de que resulta uma infraestrutura que não privilegia, com eficácia, o conjunto. A Defesa, para o cumprimento efetivo da sua missão, tem a necessidade de criar um AUI que seja ágil, que potencie a superioridade da informação, assente em procedimentos, processos, normas e padrões comuns e numa governação centralizada, de modo a que a informação e conhecimento produzido "*seja relevante para os processos de negócio e, disponibilizado atempadamente*

num formato correto e consistente" (ITGI, 2007, p. 10), permitindo aos utilizadores tomar decisões, informadas na execução das suas missões.

A adoção de soluções comuns e homogéneas, em que o acesso à informação seja baseado nas necessidades e níveis de autorização em detrimento da localização fixa, permite remover as barreiras à interoperabilidade operacional e administrativa, colocadas pelas redes algo compartimentadas e serviços frequentemente não interoperáveis atualmente em uso. Por outro lado, a adoção de soluções comuns e uniformes, naquilo que for transversal ao universo da Defesa, terá como reflexo a minimização da duplicação dos SI, reduzindo a fragmentação dos dados e serviços, potenciando economias de escala e obviando "*a necessidade de voltar a treinar os utilizadores quando estes são transferidos, mobilizados ou projetados*" (DoD, 2011, p. 4). Contribuirá, desta forma, para o aumento da eficácia operacional e da unidade de comando. Em suma, a infraestrutura TI deve ser encarada como "*um recurso interoperável e integrado que produza com rapidez a informação certa, no tempo certo e no lugar certo, em qualquer parte do mundo*" (idem, p. 8).

c. Aumentar a Segurança da Informação

As redes da Defesa estão sob constantes ataques cibernéticos externos (através da *internet*, anexos de mails ou software malicioso) e internos (atores maliciosos, operando dentro da organização). A este facto incontornável acresce que a necessidade de novos sistemas, com redes dedicadas, levou à criação de um "*ambiente de informação onde sistemas, redes e padrões foram desenvolvidos de uma maneira compartimentada e a segurança da organização é susceptível de ser explorada através de áreas de fraca proteção*" (idem, p. 8). O modelo a implementar, através da consolidação do AUI, deverá aumentar o acesso seguro à informação e serviços TI por parte de quem disponha da necessária autorização, potenciando a proteção da informação sensível, de divulgação não autorizada.

Por outro lado, a redução do número de centros de dados e de redes operadas pela Defesa, complementada por uma gestão de acessos baseada na identidade, autorização e autenticação na partilha da informação, permitirá uma melhor proteção contra ameaças internas e/ou externas. Deverá constituir, igualmente, objetivo do modelo a implementar a garantia da manutenção dos níveis de prontidão e a recuperação rápida das capacidades na eventualidade do AUI ser atacado ou degradado.

d. Produzir Eficiência

O modelo a adotar, privilegiando soluções comuns e a consolidação do AUI na Defesa, deverá, incontestavelmente, potenciar a redução dos custos, por via, designadamente, da racionalização e de economias de escala. Para o efeito, quer as infraestruturas TI, quer as aplicações e os serviços comuns ou específicos, deverão assentar o seu desenvolvimento, manutenção e operação no estrito cumprimento dos melhores padrões e práticas. Haverá, assim, que ser encontrado um equilíbrio entre o aumento de custos afeto às TI e o aumento do valor da informação, para que seja obtido retorno dos investimentos efetuados nas TI. Para tal, dever-se-á potenciar sinergias interinstitucionais, evitando que mais do que uma entidade desenvolva as mesmas capacidades.

Embora os Ramos continuem a possuir as suas infraestruturas, aplicações e serviços específicos, a sua edificação, desenvolvimento e manutenção deve sujeitar-se aos padrões e práticas comuns, permitindo, assim, que a edificação de novas capacidades seja obtida com menor dificuldade e que aquelas capacidades sejam mais interoperáveis, evitando-se assim duplicações e redundâncias.

Na figura 11 apresenta-se devidamente sintetizados os conceitos desenvolvidos anteriormente elencados.

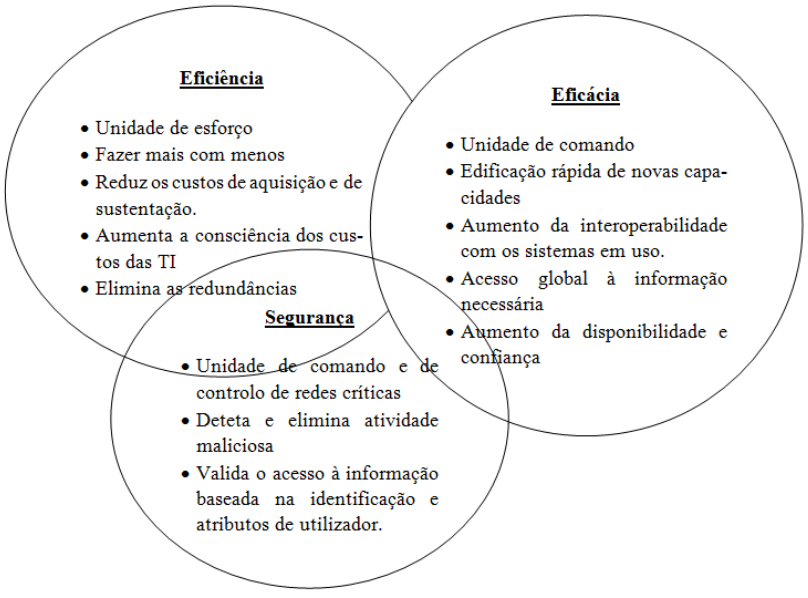


Figura 11 – Quadro resumo dos critérios de Eficiência, Eficácia e Segurança

Fonte: Adaptado (DOD, 2011)

e. Risco de Transição

Todas as mudanças numa organização, independentemente das perícias do pessoal envolvido, em particular quando incluem ativos intangíveis, estão sujeitas a riscos de transição. O balanço entre as perdas que organização poderá vir a sofrer em relação aos possíveis ganhos, vem realçar a importância das organizações entenderem e abordarem esta problemática. A título de exemplo, a NATO, na avaliação do modelo a implementar, considerou oportuno colocar as seguintes questões: Qual a magnitude da mudança? Qual o custo estimado da transição? Qual o risco de rotura no apoio às entidades apoiadas?

f. Síntese conclusiva

Na sociedade da informação em que atualmente vivemos, é cada vez mais importante que a governação das TI seja parte integrante da governação estratégica das organizações, principio basilar aplicável na plenitude à DN. Neste capítulo, foram deduzidos critérios de avaliação objetivos, de cariz essencialmente estratégico, gestionário e operacional, que, devidamente pesados ajudarão a definir o modelo de governação e organizacional que melhor sirva os interesses da Defesa. Assim, pensar na reorganização das TI da Defesa, passa, antes de mais, por pensar nos seguintes aspetos fundamentais:

– Numa reorganização com base num modelo de governação que potencie as suas cinco áreas fundamentais (alinhamento estratégico, criação de valor, gestão de risco, gestão de recursos e avaliação de desempenho);

– Que a informação necessária, que seja relevante e pertinente para o processo de negócio, tem que ser providenciada atempadamente, de uma forma precisa e consistente (eficácia);

– Que essa informação será obtida através de uma utilização otimizada dos recursos (eficiência);

– Que é imprescindível que informação sensível não seja disponibilizada a terceiros sem autorização e que os ativos TI da defesa estejam protegidos (segurança da informação);

– Que a transição para a nova estrutura seja feita de modo a minimizar o esforço, risco e custos da transição (risco de transição).

Assim, evidenciando os critérios essenciais que devem ser considerados na reorganização das TI da DN, considera-se validada e confirmada a Hip3, e em consequência dada resposta à QD 3.

4. O modelo organizacional e de governação mais adequado para as TI da DN

A identificação de uma solução organizativa e de governabilidade que melhor responda aos critérios anteriormente identificados e que, esteja alinhada, na medida do adequando, com a AP, com os países Aliados e com a congénere da NATO, passa, em primeiro lugar, por caraterizar os diversos modelos conceptuais (centralizado, federado ou híbrido e descentralizado) e, em seguida, por determinar aquele que, no contexto da DN, melhor responde aos critérios definidos. Numa segunda fase, identificado o modelo que melhor serve a DN, será então possível proceder à edificação da arquitetura em que este deverá assentar.

A estrutura a edificar, terá que potenciar a " *inter-relação entre as diferentes camadas de interesse: a camada de criação de valor organizacional e seus processos de suporte*" (SSTI, 2012, p. 4), segundo a metodologia apresentada na Figura 12 e que será deduzida de seguida.

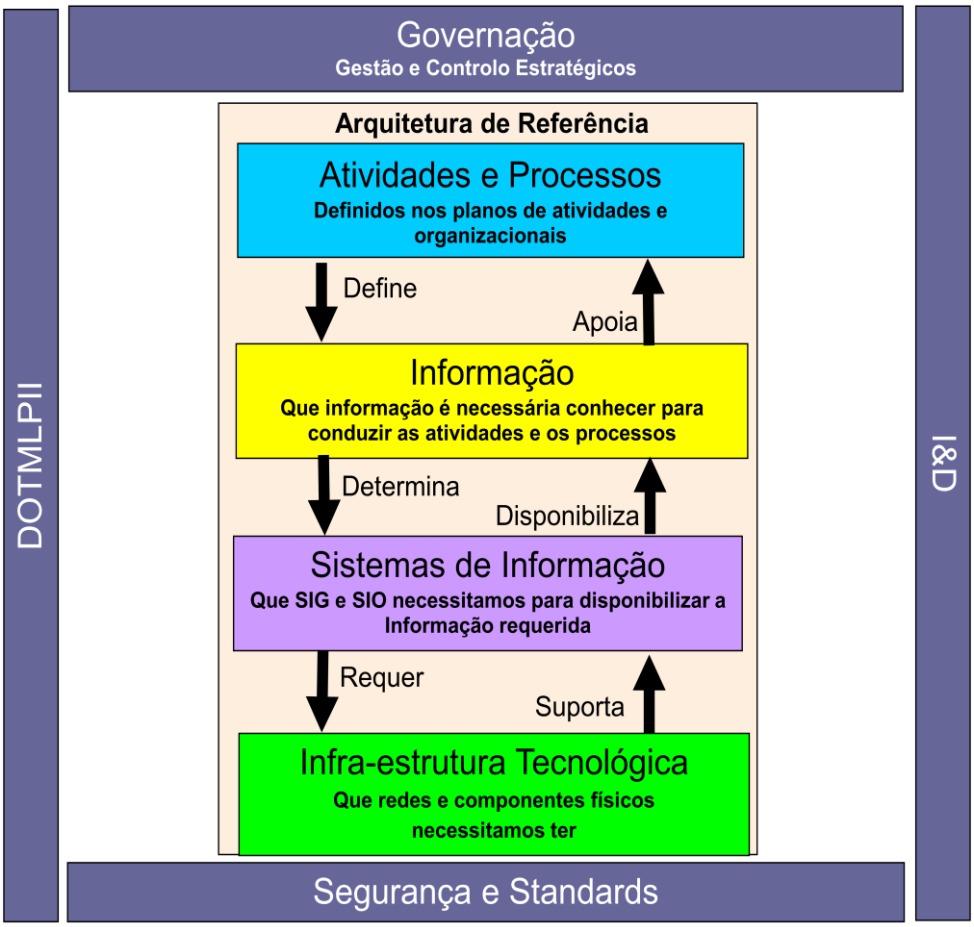


Figura 12 – Representação lógica da arquitetura organizacional e respetivas dependências

Fonte: (SSTI, 2012)

De acordo com o modelo, o principal contributo das TI é ajudar a explicitar o conhecimento de maneira a habilitar o decisor a tomar decisões de forma mais fundamentada e atempadamente. Por conseguinte, a arquitetura a implementar terá que ter como propósito governar as TI da Defesa de acordo com as orientações estratégicas emanadas pela sua estrutura superior. Dessas orientações, são vertidos os planos organizacionais onde se encontram plasmados os processos e atividades. Edificados os planos de atividades, com os objetivos, indicadores e metas, haverá que definir que "*tipo de informação é requerida para conduzir as atividades e os processos, a qual, por sua vez, determina que SI de gestão e operacionais são necessários para disponibilizar a referida informação, os quais, por último, determinam os requisitos da Infraestrutura Tecnológica que se devem edificar, no sentido de suportar a interligação e a interoperabilidade em rede dos SI*" (ibidem).

A arquitetura organizacional edificada no sentido descendente é lida no sentido ascendente: a infraestrutura tecnológica suporta os SI, que disponibilizam a informação que irá apoiar os processos e atividades da Defesa. Este método deverá ser concretizado de uma forma holística, implementando uma governação nos quatro níveis através de processos de investigação, desenvolvimento e inovação, tendo em consideração a segurança e os padrões vigentes, sempre numa lógica de edificação de capacidades segundo a metodologia DOTMLPII[11] e aproveitando as oportunidades e desafios (I&D) já identificados.

Conforme a Figura 13, a abordagem do modelo conceptual deverá ser feita segundo uma lógica de arquitetura de serviços segundo quatro vertentes: serviços estratégicos, específicos, nucleares e de rede. Os dois últimos têm um caracter essencialmente comum e, portanto, transversal a toda a Defesa. Os dois primeiros acumulam essa vertente com a necessidade dos Ramos deterem essa valência para a sua gestão interna, nomeadamente no que respeita à capacidade de C2 e de apoio à decisão da sua estrutura superior.

[11]Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade.

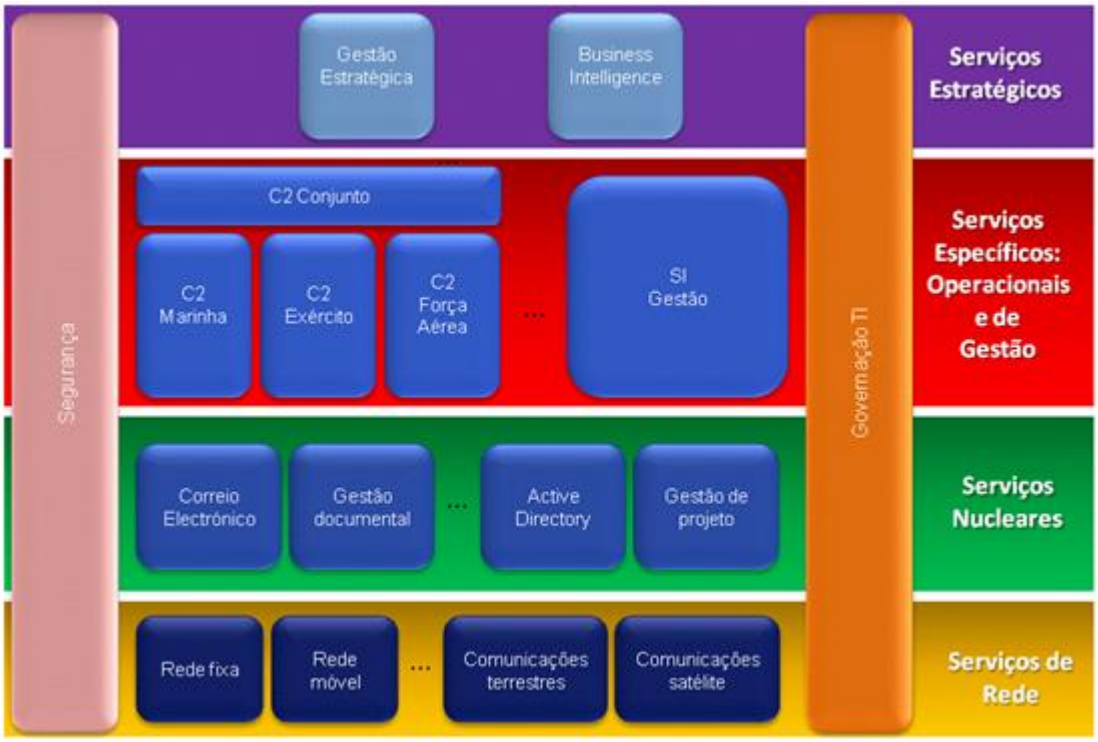


Figura 13 – Arquitetura de serviços

Fonte: NATO Architecture Framework (adaptado SSTI)

a. Modelos Conceptuais

De uma forma genérica, os três modelos conceptuais comumente em uso poderão ser caraterizados da seguinte forma:

(1) Modelo Centralizado

Este modelo é caracterizado por todas as infraestruturas e serviços TI serem fornecidos por uma entidade única, responsável pelo fornecimento, conceptualização, desenvolvimento e implementação de soluções TI em toda a organização. Todas as atividades TI na organização são controladas, a nível central, pelo CIO, com uma adequada estrutura na sua dependência, com responsabilidade na gestão do orçamento, recursos, infraestruturas e parcerias externas (através da identificação das atividades que são candidatas ao *outsourcing*). Neste contexto, o CIO é o responsável por determinar onde são alocados os investimentos e os recursos necessários ao fornecimento dos serviços TI.

Ao nível da Defesa, a materialização deste modelo passaria por concentrar os quatro níveis de serviço numa entidade, EMGFA ou SG, à semelhança da proposta do modelo 3 (agência única) da NATO anteriormente aduzida. Esta centralização dos serviços teria evidentes implicações ao nível dos serviços estratégicos e específicos que contribuem para a missão dos Ramos, nomeadamente na capacidade de C2 e, por exemplo, no caso da Marinha, nos serviços que contribuem para o conhecimento situacional marítimo, no Exército,

no Sistema de Informação e Comunicação Tático e, na FA, no Sistema Integrado de Vigilância, Fiscalização e Controlo das Atividades da Pesca.

O CIO das estruturas centralizadas reporta diretamente ao *Chief Executive Officer*[12], tendo como principal consequência a limitada autonomia dos Ramos em matéria de SI/TI, com as decorrentes implicações deduzidas na sua gestão estratégica específica e capacidade de C2.

Este tipo de modelo, ao nível civil, tem uma melhor aplicabilidade em organizações de pequena e média dimensão, em que o volume de informação processada é relativamente baixo e que estejam inseridas num ambiente estável. A centralização conduz a uma racionalização dos custos e permite uma economia de escala, devida a uma menor complexidade, mas nenhuma literatura consultada aponta para uma melhoria da qualidade do serviço prestado.

(2) Modelo Descentralizado

Este modelo é caracterizado por cada unidade de negócio gerir as suas unidades TI e o orçamento associado, operando independentemente das outras unidades de negócio. Assim, ao nível global da organização, constata-se a existência de múltiplas organizações TI, potencialmente redundantes. As organizações que adotam este conceito têm uma governação descentralizada, uma vez que, as unidades de negócio executam as suas atividades com muito pouco controlo ou coordenação central. Este modelo, ao nível da sociedade civil, encontra-se plasmado em organizações de grande dimensão, com grande intensidade de informação, e inseridas em ambientes pouco estáveis.

Da análise dos capítulos anteriores poder-se-á concluir que é este o modelo atualmente em uso na Defesa. Os Ramos têm as suas próprias organizações TI, todas elas com enfoques e níveis de maturidade diferenciados, de onde decorrem organizações distintas o que só por si é pouco promotor de sinergias e com claras redundâncias, de que a gestão do correio eletrónico é um claro exemplo (neste momento, cada Ramo, EMGFA e SG têm a sua própria equipa a gerir o seu correio eletrónico, com a agravante de quatro possuírem a mesma tecnologia).

[12] MDN no caso da Defesa

(3) Modelo Híbrido

Este modelo pretende obter a eficiência e a padronização através da centralização e a eficácia e a flexibilização através da descentralização. Para o efeito, um grupo central estabelece práticas e padrões comuns, cria procedimentos que sejam relevantes transversalmente a toda a organização e é responsável pela arquitetura comum da organização. As atividades, por seu lado, são desenvolvidas localmente pelas unidades de negócio. Assim, de uma forma geral, no modelo híbrido os serviços de infraestrutura são fornecidos a toda a organização por uma entidade central (controlo de infraestrutura centralizado), e os serviços de aplicações são providenciados pelos departamentos das TI nas unidades de negócio (controlo de aplicação descentralizado).

A adoção deste modelo para a Defesa passa pela criação de um Comité de Governação Estratégica (CGE) com a responsabilidade de governação das TI. Este Comité é apoiado logística, administrativa e técnico-funcionalmente por uma estrutura centralizada, liderada pelo CIO, com competências a nível da gestão dos serviços nucleares e de rede (todos eles transversais à Defesa), dos serviços específicos conjuntos, nomeadamente os de Comando e Controlo conjunto e, por fim, com capacidade de apoio à gestão estratégica da Defesa. Para os Ramos remanesciam os serviços específicos e os estratégicos de apoio à sua gestão de negócio. Este modelo permite acomodar a natureza autónoma dos Ramos com a economia de escala do modelo centralizado. Tem que assentar numa grande liderança do CIO e num respeito pelas fronteiras institucionais, que, no entanto, deverão ser flexíveis. A mistura de culturas institucionais, de que é apanágio a Defesa, poderá ser um óbice à sua implementação.

Na Figura 14, apresenta-se de uma forma integrada as principais características dos três modelos conceptuais

Figura 14 – Quadro resumo dos modelos conceptuais

Fonte: (Autor, 2013)

Caracterizados os modelos, é possível agora confrontá-los com os critérios anteriormente identificados. Para a sua análise recorreu-se à ferramenta Project Server 2010, embebida no Enterprise Project Manager. Do processo de comparação dos diferentes modelos sujeitos aos fatores acima enumerados, plasmada no Apêndice 6, decorreu a seleção do modelo híbrido como sendo aquele que melhor se adequa ao universo da Defesa.

b. Linhas de ação decorrentes da análise SWOT

Identificado o modelo que melhor se adequa à DN, torna-se necessário deduzir como é que ele se enquadra na estrutura da DN. Da análise SWOT realizada no apêndice 5, foram deduzidas linhas de ação estruturais e ao nível dos processos que vão contribuir para a edificação do modelo organizacional a propor. Por ser relevante para a concretização da arquitetura organizacional, âmbito deste trabalho, passa-se, de seguida, a elencar as linhas de ação estruturais, reservando as relativas aos processos para o apêndice 7, onde serão elencados em maior detalhe as funções a desempenhar por cada elemento da estrutura:

– Estabelecer uma organização ao nível estratégico que garanta a governação das TI de uma forma coerente e holística e que sustente a estratégia da organização;

– Estabelecer uma organização ao nível executivo que monitorize a governação das TI;

– Estabelecer uma organização responsável pela formulação, implementação e gestão da estratégia das TI da DN, chefiada por um CIO, que defina os processos e relacio-

namentos de modo que sejam ágeis a responder à estratégia da organização, cumprindo ao mesmo tempo com os requisitos de governação;

– Edificar uma estrutura de gestão de projetos responsável pelos programas das capacidades ao longo do ciclo de vida total;

– Potenciar as valências dos Ramos criando núcleos de competências que permitam otimizar e racionalizar os recursos da DN.

c. Arquitetura de Referência

Tendo por base o anteriormente explanado, nomeadamente, os modelos organizacionais em uso em outras organizações, o modelo concetual deduzido (híbrido) e as linhas de ação decorrentes da análise SWOT do Apêndice 5, é possível agora avançar com a edificação da arquitetura de referência que materialize o modelo identificado.

Independentemente da arquitetura a edificar na DN, ela tem que ter em atenção que, "*os requisitos operacionais das FFAA para apoiar as operações militares e não-militares têm primazia sobre quaisquer outros considerandos, incluindo em relação aos aspetos de racionalização e eficiência, dando espaço às FFAA para que, com a articulação que for considerada adequada, possam gerir o ciclo de vida dos sistemas determinantes para o cumprimento das suas missões*" (SSTI, 2012, p. 3).

A definição das funções e responsabilidades de todas as partes envolvidas na arquitetura TI é um pré-requisito para a eficácia e sucesso do modelo a implementar, pelo que, como atrás referido, o Apêndice 7 detalha em pormenor os responsáveis pelos processos decorrentes das linhas de ação.

(1) Comité de Governação Estratégica

Como anteriormente referido, torna-se necessário criar um corpo comum que garanta a governação das TI de uma forma coerente e holística. Para o efeito, propõe-se a criação do CGE, equivalente ao C3B da NATO, que representa a estrutura superior das TI e do negócio da Defesa. Este fórum deverá ser chefiado simultaneamente pelo Comandante Operacional Conjunto e pelo SG do MDN, tendo nele assento o CIO e os Chefes dos OCAD das TI dos Ramos. Este órgão tem como principal finalidade definir a estratégia das TI da DN, assegurando que a estratégia TI se encontra alinhada e apoia de forma coerente, eficaz, eficiente e inovadora o modelo de negócio da DN e exercerá a supervisão e o controlo estratégico desta área funcional da Defesa. O CGE tem uma estrutura executiva, materializada pelo Comité de Governação Executiva (CGExec) definido abaixo.

(2) Comité de Governação Executiva

Chefiado pelo CIO e composto pelos diretores ou chefes executivos das áreas tecnológicas das TI dos Ramos e pelos Chefes de Divisão da estrutura do CIO, constitui-se como o órgão executivo do CGE para a operacionalização e controlo operacional da estratégia TI, sendo suportado em termos operacionais pela "Estrutura TI da Defesa". Responde perante o CGE sobre todos os aspetos executivos da estratégia TI da Defesa, incluindo processuais e organizativos, tecnológicos, arquiteturais e de estandardização, de segurança e de gestão e análise da informação e do conhecimento.

(3) CIO

Ao CIO da Defesa, conhecedor profundo em matéria das SI/TI, cabe a chefia do CGExec e da "Estrutura TI da Defesa", cujas responsabilidades incluem a gestão dos serviços nucleares e de rede transversais à Defesa (MDN e das Forças Armadas) e dos serviços específicos, operacionais e estratégicos do MDN e das Forças Armadas. Recai particularmente no CIO a responsabilidade de implementar de forma eficaz, os processos de cariz transversal, identificados no inquérito COBIT, de modo a melhorar a qualidade do serviço e o nível de maturidade dos serviços TI de que é responsável. O CIO deve depender simultaneamente da estrutura política (SG do MDN) e militar (Comandante Operacional Conjunto) da Defesa Nacional, consoante a natureza político-militares ou funcionais das matérias em questão. Contudo, dado que a área de responsabilidade do CIO e da estrutura que chefia incluir os sistemas TI e C2 militares, reconhecidamente de elevada criticidade, disponibilidade e segurança, a integração orgânica da "Estrutura TI da Defesa" e, logo, do CIO, deve ser no EMGFA, dependendo hierarquicamente do Comandante Operacional Conjunto.

(4) Estrutura de Apoio ao CIO

O CIO chefia a "Estrutura TI da Defesa", a qual é constituída por diversas Divisões técnico-operacionais TI, responsáveis pela conceção, desenvolvimento, implementação, gestão, operações e manutenção de soluções e serviços TI de cariz transversal à Defesa. Esta estrutura deve agregar duas categorias diferentes de SI/TI: A primeira abrange as capacidades TI que, pela sua transversalidade, são geridas pelo CIO e a sua estrutura; a segunda inclui os processos que, atualmente, se encontram distribuídos pelos Ramos e que, dada a sua natureza e baixa eficiência, se considera benéfico centralizar. Para o efeito, a "Estrutura TI da Defesa" deverá ser constituída pelas seguintes Divisões.

(a) Divisão de Arquitetura Empresarial (DAE)

A DAE atua como o «guardião» da visão, sendo responsável pela preparação dos padrões e da estratégia TI, a propor pelo CIO ao CGExec que após revisão a propõe a aprovação ao CGE. Esta Divisão é também responsável pelo planeamento de recursos e a gestão e priorização de projetos, sob orientação do CGExec. Deverá, igualmente, estar atenta à evolução do negócio e ir adaptando a arquitetura das TI para fazer face a qualquer mudança. Define as arquiteturas de referência (como deve estar estruturada a organização, identificar, otimizar e automatizar os processos organizacionais, alinhar e otimizar os processos TI com os de negócio, definir os padrões das TI a serem seguidos e definir os fluxos de informação, as redes e os serviços TI principais e a sua interligação). Finalmente, será também responsável por garantir a interoperabilidade entre as diversas entidades da DN, a NATO e a AP.

(b) Divisão de Desenvolvimento de Capacidades (DDC)

Esta Divisão focar-se-á, primariamente conceção e desenvolvimento de capacidades TI, serviços e *software* de natureza estratégica, gestionária e operacional, em suporte aos correspondentes processos transversais da Defesa (MDN e FFAA).

(c) Divisão de Operações e Manutenção de Capacidades (DOMC)

Esta divisão lidará com a parte tangível das TI (operações e manutenção de capacidades), sendo responsável pela operação e manutenção das infraestruturas comuns da Defesa (serviços nucleares e de rede).

(d) Divisão de Apoio Logístico (DAL)

Esta Divisão é responsável pela preparação, planeamento, condução e avaliação dos processos orçamentais, financeiros e logísticos da "Estrutura TI da Defesa". Gere o departamento TI do ponto de vista financeiro, de modo a que os orçamentos de investimento e de funcionamento não sejam excedidos. Será, também, responsável pela gestão dos contratos com os fornecedores. A DAL foca-se essencialmente na edificação de sistemas usando soluções de *outsourcing* e em integrá-las na infraestrutura da Defesa

(e) Divisão de Gestão da Transição (DGT)

A DGT deverá trabalhar em proximidade com a estrutura das TI dos Ramos, sendo responsável pela gestão da transição para a nova estrutura, que permita mitigar os riscos de

transição associados. As suas principais responsabilidades são preparar e gerir o plano de Transição, em sintonia com o CGExec. Complementarmente, esta Divisão atuará como estrutura primária de apoio aos CGE e CGExec. Esta Divisão será extinta quando o processo de transição for considerado completo pelo CGE, devendo estas últimas responsabilidades de apoio ao CGE e CGExec passar nessa altura para a DAE.

(f) Núcleo de Capacidades (NC)

Os NC são criados na dependência do CGExec para planearem e gerirem, com apoio técnico da "Estrutura TI da Defesa", o desenvolvimento harmonioso de uma determinada capacidade transversal (ex. Comunicações Satélite) ou um projeto transversal de elevada complexidade.

(5) Núcleos de Competências

A partilha de serviços tem sido identificada pelos especialistas como a forma mais eficaz de conferir agilidade às organizações, com benefícios associados de racionalização e eficiência. Pelo que, sempre que oportuno, as organizações deverão considerar essa possibilidade no seu planeamento estratégico. Nesse sentido, advoga-se, para efeitos de racionalização, a organização das TI, ao nível da execução, sob uma abordagem de núcleos de competências que aproveitem as competências, de reconhecido nível de maturidade, que os Ramos possuam.

Os núcleos de competências, embora transversais a todos os Ramos, deverão ser liderados por um deles. A título de exemplo, o MMHS embora seja transversal à DN e, por esse motivo o seu ciclo de vida deva ser gerido por quem gere os serviços nucleares, numa lógica de racionalização de recursos poderá a sua gestão global ser delegada no Ramo que esteja em melhores condições de liderar o processo. Este tem que assentar no estabelecimento de *Service Level Agreements* (SLA) que, de alguma forma, comprometam o Ramo no que respeita à qualidade do serviço a fornecer aos restantes. A função do SLA será definir não só que níveis de serviço são aceitáveis pelos utilizadores, como, também, que níveis são alcançáveis pelo fornecedor de serviços, mediante um conjunto de indicadores de qualidade dos serviços mutuamente aceites e acordados.

Na figura 15, apresenta-se o organograma das TI da DN proposta por este trabalho.

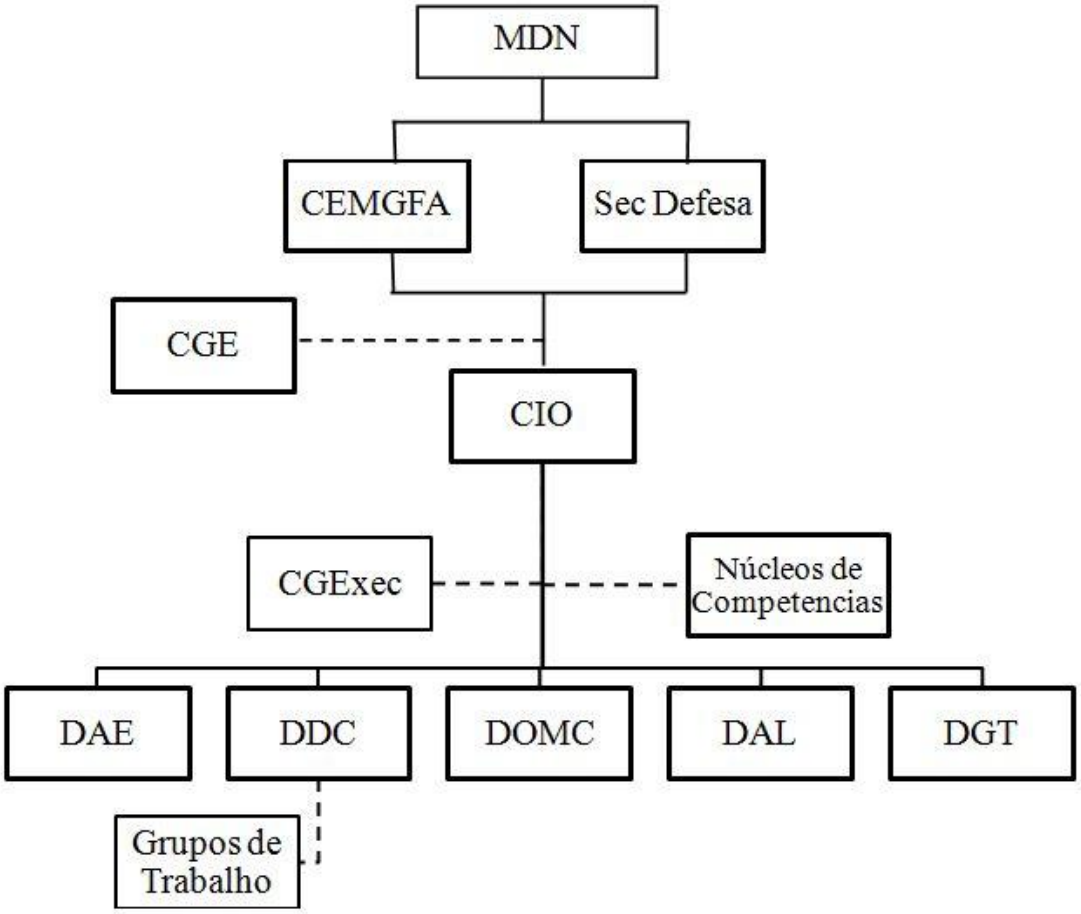


Figura 15 – Organograma da estrutura das TI da DN

Fonte: (autor, 2013)

d. Síntese conclusiva

Neste capítulo pretendeu-se identificar o modelo organizacional que melhor responde aos critérios já deduzidos. Para o efeito, a análise iniciou-se pelo escalonamento das camadas de interesse, quer da informação, quer do conhecimento. De seguida caracterizaram-se os três modelos concetuais (centralizado, descentralizado e híbrido), identificando as suas potenciais vantagens e eventuais desvantagens. Considerando os modelos concetuais de governação das TI, foi possível confrontá-los com os critérios previamente deduzidos, tendo-se identificado o modelo híbrido como aquele que melhor se adequa às necessidades da DN.

Da análise SWOT foram deduzidas linhas de ação, estruturais e ao nível dos processos, o que permitiu avançar para a proposta de uma arquitetura organizacional. Assim, a sua edificação terá que assentar numa lógica de serviços, centralizando a governação num órgão colegial (CGE), e a operacionalização e controlo operacional da estratégia TI num

órgão executivo do CGE, o CGExec. Nestes dois órgãos deverão estar representadas todas as entidades da DN. Por fim, a conceção, o desenvolvimento, a implementação, a gestão, as operações e a manutenção das soluções e dos serviços TI de cariz transversal à Defesa deverá ser centrada numa estrutura de referência cujo produto seja focado na informação e no conhecimento, de modo a que as TI potenciem o acesso à informação e ao conhecimento e apoiem o processo de decisão, no sentido de, em última análise, alavancarem o processo de criação de valor e o "negócio" da Defesa.

Aos Ramos caberá a responsabilidade de gerirem os seus serviços específicos, bem como aqueles que, pelas suas valências, potenciem a criação de núcleos de competências que permitam aliviar a estrutura do CIO, contribuindo, assim, para a racionalização de recursos. Considera-se assim ter identificado uma solução organizativa e de governabilidade, confirmando a Hip4 e dando resposta à QD4.

Conclusões

Atento o enunciado do tema proposto, ao longo do presente trabalho de investigação, pretendeu-se identificar qual o modelo organizacional e de governação mais adequado às TI da DN (QC). Neste contexto, para responder à QC utilizou-se, como procedimento metodológico, a formulação de quatro QD e das correspondentes Hip, que foram objeto de análise ao longo deste trabalho, e que serão, agora, abordadas sequencialmente, para, assim, se obter a resposta à QC formulada.

Assim, foi analisado o quadro legal das TI da DN, constituído pelo edifício normativo das cinco entidades da DN que se consideram atores relevantes para o presente estudo (SG, EMGFA, Marinha, Exército e FA). Da análise, contatou-se que todas elas apresentam organizações distintas, o que só por si compromete a interoperabilidade e a identificação de potenciais sinergias.

A avaliação do ambiente interno e externo conduziu à identificação das potencialidades, vulnerabilidades, oportunidades e desafios, o que, através de uma análise SWOT, permitiu que fossem deduzidas as linhas de ação em que assentará a edificação da estrutura que suportará o modelo organizacional a propor no âmbito deste trabalho. Para avaliação do ambiente interno, foi utilizada como fonte a auditoria às TI da DN realizada pelo IGDN e foi elaborado um questionário, baseado no COBIT, onde se pretendeu avaliar, individualmente, o nível de maturidade das entidades envolvidas nos 34 processos dos quatro domínios (planear e organizar, obter e implementar, fornecer e apoiar, monitorizar e avaliar) estabelecidos nesse conceito. Para a análise do ambiente externo, recorreu-se, em larga medida, à RCM n.º 12/2102, onde é aprovado o PGETIC, e ao Despacho n.º 149/12, do MDN, que estabelece os princípios para a reorganização da estrutura superior do DN. Da análise efetuada, foi possível concluir que o atual modelo não permite uma racionalização dos recursos, não promove sinergias, não garante a segurança e não fomenta a interoperabilidade, validando-se, assim, a Hip 1.

A análise de três organizações, do âmbito da Defesa, levou à constatação de que, todas elas assentam o seu modelo concetual num modelo híbrido. Para além deste facto, ficou patente que todas essas organizações apresentam, ao nível estratégico, uma estrutura que viabiliza a estratégia das TI, garantindo, por um lado, que esta esteja alinhada com os objetivos de negócio da Defesa, e por outro, o necessário alinhamento com as restantes entidades com quem interagem, tendo, no entanto, sempre presente que os requisitos da

Defesa são prioritários.

A implementação da estratégia das TI e a gestão dos serviços nucleares e de rede transversais à Defesa ficam a cargo do CIO, que é apoiado, nessa tarefa, por uma estrutura robusta. Para o desenvolvimento das capacidades mais complexas, fora da alçada da "Estrutura TI da Defesa", são constituídos "núcleos de capacidade" que representam a vontade dos utilizadores e os quais são apoiados tecnicamente pela referida estrutura. Confirma-se, assim, que as organizações congéneres estudadas evoluíram para uma estrutura hibrida, de governação centralizada e gestão descentralizada (Hip 2).

De seguida, deduziram-se os critérios de avaliação objetivos, de cariz essencialmente estratégico, gestionário e operacional, que servirão de suporte à edificação do modelo organizacional das TI da DN (Hip 3), e que se passam a elencar:

– Um modelo de **governação** que potencie as cinco áreas fundamentais (alinhamento estratégico, criação de valor, gestão de risco, gestão de recursos e avaliação de desempenho);

– A informação necessária, que seja relevante e pertinente para o processo de negócio, tem que ser providenciada atempadamente, de uma forma precisa e consistente (**eficácia**);

– Essa informação deverá ser obtida através de uma utilização otimizada dos recursos (**eficiência)**;

– A necessidade de garantir que a informação sensível não seja disponibilizada a terceiros, sem autorização, e que os ativos TI da defesa estejam protegidos (**segurança da informação**);

– A transição para a nova estrutura seja feita de modo a minimizar o esforço, risco e custos da transição (**risco de transição**).

Por fim, passou-se à edificação do modelo organizacional e de governação que melhor responda aos critérios deduzidos anteriormente, tendo para o efeito sido analisado três modelos conceptuais (centralizado, descentralizado e híbrido), segundo uma lógica de serviços. A análise efetuada permitiu concluir, de forma inequívoca, que o modelo híbrido é aquele que melhor responde aos requisitos da DN. Complementarmente, da análise SWOT efetuada foi possível deduzir as linhas de ação estruturais e ao nível dos processos que conduziram à materialização da arquitetura organizacional. Assim, o modelo organizacional das TI da DN deverá assentar numa governação através de dois órgãos colegiais, ao nível estratégico (CGE) e executivo (CGExec), ficando a gestão das TI transversais à DN

sob a responsabilidade do CIO, podendo algumas delas, serem delegadas em núcleos de competências que potenciem as valências dos Ramos e permitam a racionalização dos recursos. Para os Ramos remanescem, para além dos núcleos de competências, os serviços específicos e os serviços estratégicos de apoio à sua gestão de negócio, validando assim a Hip 4 e dando reposta à QD4

Como corolário das conclusões do estudo recomendam-se as seguintes linhas de ação:

– Estabelecimento de um órgão, ao nível estratégico, tutelado pelo Comandante Operacional Conjunto e SG, em que tenham assento o CIO e os OCAD das TI dos Ramos, e que garanta a governação das TI de uma forma coerente e holística, sustentando a estratégia da organização;

– Estabelecer uma organização ao nível executivo, chefiada pelo CIO, e composta pelos diretores ou chefes executivos das áreas tecnológicas das TI dos Ramos e pelos Chefes de Divisão da estrutura do CIO, responsável pela operacionalização e controlo operacional da estratégia TI;

– Edificar uma "Estrutura TI da Defesa", constituída por diversas Divisões técnico-operacionais TI, responsáveis pela conceção, desenvolvimento, implementação, gestão, operações e manutenção de soluções e serviços TI de cariz transversal à Defesa.

– Promover ao nível da DN a capacidade de gestão de projetos.

– Potenciar as valências dos Ramos criando núcleos de competências que permitam otimizar e racionalizar os recursos da DN.

Estas estruturas serão responsáveis pelos processos elencados no Apêndice 7.

Bibliografia

ANAO, 2011. *Overtsight and Management of Defence´s Information and Communication Technology*, Camberra, Austrália: Australian National Audit Office. Disponivel na Internet em: http://www.anao.gov.au/~/media/Uploads/Audit%20Reports/2011%2012/201112%20Audit%20Report%20No19.pdf. [Consultado em 09 dezembro 2012]

Correia, S. M. A., 2010. *factores criticos de sucesso da governança das ti - Universidade Técnica de Lisboa.* [Online] Disponivel na Internet em: https://www.repository.utl.pt/bitstream/10400.5/2216/1/Factores%20Criticos%20de%20sucesso%20da%20governana%20das%20TI%20%20-%20Documento%20Final.pdf. [Consultado em 03 dezembro 2012].

DoD, 2009. *Defence Information and Communications Technology Strategy 2009,* Austrália: Australia Department of Defence. Disponivel na Internet em: http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf. [Consultado em 06 janeiro 2013]

DoD, 2011. *Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap.* [Online] Disponivel na Internet em : http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf. [Consultado em 06 janeiro 2013].

Governo, 2011. *Memorando de Entendimento sobre as condicionalidades de Politica Económica.* [Online] Disponivel na Internet em: www.portugal.gov.pt/media/371372/mou_pt_20110517.pdf. [Consultado em 26 fevereiro 2013].

Grembergen, Wv, 2004a. *IT Governance and its Mechanisms.* [Online] Disponivel na Internet em: http://pdf.aminer.org/000/245/098/introduction_to_the_minitrack_it_governance_and_its_mechanisms.pdf. [Consultado em 28 novembro 2012].

Grembergen, W. V., 2004b. *Strategies for Information Technology Governance.* London: Idea Group Publishing. Disponivel na Internet em: http://www.sistemas.ith.mx/raymundo/Cobit/Idea%20Group,.Strategies%20for%20Informati-on%20Technology%20Governance.%5B2003.ISBN1591402840%5D.pdf. [Consultado em 05 fevereiro 2013]

Guldentops, E., 2002. *Knowing the environment: Top five IT issues.* [Online] Disponivel na Internet em: http://www.isaca.org/Journal/Past-Issues/2002/Volume-4/Pages/Knowing-the-Environment-Top-Five-IT-Issues.aspx [Consultado em 05 março 2013].

IGDN, 2011. *Auditoria Avaliar o Grau de Integração dos Sistemas de Informação que Envolvam Tecnologias de Informação e Comunicação,* Lisboa: MDN.

ITGI, 2003. *Board Briefing on IT Governance, 2nd edition,* Rolling Meadows, IL 60008 USA: IT Governance Institute. Disponivel na Internet em: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx. [Consultado em 05 março 2013]

ITGI, 2007. *Control Objectives for Information and Related rechnology (COBIT 4.1).* Rolling Meadows, USA: It Governance Institute.

ITGI, 2008. *unlocking value: An executive.* s.l.:IT Governance Institute. Disponivel na Internet em: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Unlocking-Value-An-Executive-Primer-on-the-Critical-Role-of-IT-Governance.aspx. [Consultado em 12 março 2013]

Kaplan, R. &. D., 1996. *The Balanced scorecard: translation vision into action.* s.l.:Harvard Business School Press. Disponível na Internet em: http://pom.ir/wp-content/uploads/PDF/book/10037-Kaplan-Norton-The-Balanced-Scorecard-Translating-Strategy-into-Action-1996.pdf [Consultado em o8 fevereiro 2013]

Loggerenberg, w. a. v., 2006. *IT Governance:theory and Pratices.* Pretoria, South Africa, s.n., p. 2. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.2838&rep=rep1&type=pdf. [Consultado em 12 fevereiro 2013]

Marques, C. A., 2012. *Reorganização das TI na Defesa* [Entrevista] (12 dezembro 2012).

Marques, G., 2008. *Cooperação Técnico-Militar com os PALOP. Prioridades, Linhas de Orientação e Estratégias. Articulação com a Sociedade Civil.Trabalho de Investigação Individual.* Pedrouços: IESM.

MDN, 2007. *Estabelece as competências e organização dos Órgãos Centrais de Administração do Exército (DR 74/2007 02 de julho.* Lisboa: Diário da República. Disponivel na Internet em: http://www.exercito.pt/pefex/Doc-E4/DR-OCAD.pdf. [Consultado em 14 novembro 2012]

MDN, 2009a. *Aprova a Lei Orgânica do Estado-Maior-General das Forças Armadas (DL 234/2009 de 15 de setembro).* Lisboa: Diário da República.. Disponível na Internet em: http://www.emgfa.pt/documents/4xcs0fzgnm8h.pdf. [Consultado em 14 novembro 2012]

MDN, 2009b. *Aprova a Lei orgânica da Marinha (DL 233/2009 de 15 de Setembro.* Lisboa: Díário da Républica. Disponivel em : http://www.emgfa.pt/documents/nyc9vxdb67sg.pdf. [Consultado em 14 novembro 2012]

MDN, 2009c. *Aprova a Lei Orgânica do Exército (DL 231/2009 de 15 de setembro).* Lisboa: Diário da Républica. Disponivel na Internet em: http://www.emgfa.pt/documents/87h9rcksmpfj.pdf. [Consultado em 14 novembro 2012]

MDN, 2009d. *Aprova a lei orgânica da Força Aérea (DL 232/2009 de 15 de setembro).* Lisboa: Diário da Républica. Disponivel na Internet em: http://www.emfa.pt/www/conteudos/informacaofap/legislacao/organizacaofarmadas/lofa15set2009.pdf [Consultado em 14 novembro 2012]

MDN, 2011. *Aprova a Lei Orgânica do Ministério da Defesa Nacional (DL nº 122/2011).* Lisboa: Diário da Républica. Disponivel na Internet em: http://www.portugal.gov.pt/media/381567/lo_mdn.pdf. [Consultado em 14 novembro 2012]

MDN, 2012a. *Aprova a Orgânica da Secretaria-Geral do Ministério da Defesa Nacional (Dr nº 7/2012).* Lisboa: Diário da Républica.

MDN, 2012b. *Aprova a estrutura nuclear da Secretaria-geral (portaria nº 86/2012.* Lisboa: Diário da Républica.

MDN, 2012c. *Directiva para a Reorganização da Defesa Nacional e das Forças Armadas.* Lisboa: Ministério da Defesa Nacional.

MoD, 2010. *Defence ICT strategy.* [Online] Disponivel na Internet em: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27373/modict_strategyv1.pdf [Consultado em 12 dezembro 2012].

NATO, 2001. *AAP 31 (A) - NATO Glossary of Communications and Information Systems Terms and Definitions.* Bruxelas: NATO Standirization Agency.

NATO, 2005. *Managing Transformation - Directive 80-7.* Brussels: NATO.

NATO, 2010. *Provision of Communications and Information Systems (CIS) support to NATO.* Bruxelas: NATO.

NATO, 2011. *AAP 6 - NATO Glossary of Terms and Definitions.* s.l.:NATO Standirization Agency.

NATO, 2013. *NATO Communications and Information Agency.* [Online] Disponivel na Internet em: http://www.ncia.nato.int/Pages/default.aspx [Consultado em 13 abril 2013].

P.Weill, M. .. B. &., 1998. *Leveraging the new infrastructure - How market leaders capitalize on Information Technology*. s.l.:Harvard Business School Press. Disponível na Internet em: http://karlknapp.com/resources/infotechnology/itinfrastructure.doc. [Consultado em 10 novembro 2012]

PCM, 2003. *Aprova o Conceito Estratégico de Defesa Nacional (CEDN) RCM nº 6/2003.* Lisboa: Diário da Républica.

PCM, 2011. *Aprova a criação do Grupo de Projeto para as Tecnologias de Informação e Comunicação (RCM 46/2011 27 outubro 2011).* Lisboa: Diário da República. Disponivel na Internet em: http://www.inst-informatica.pt/legislacao-e-directivas/administracao-publica-electronica/resolucao-do-conselho-de-ministros-n.o-46-2011-d.r.-n.o-218-serie-i-de-2011-11-14/view?searchterm=[Consultado em 14 novembro 2012]

PCM, 2012a. *Aprova o plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública, apresentado pelo Grupo de Projeto para as Tecnologias de Infoormação e Comunicação (GPTIC) (RCM nº 12 /2012 de 12 de janeiro).* Lisboa: Diário da Républica. Disponivel em: http://www.inst-informatica.pt/documentos/rcm-12-2012. [Consultado em 14 novembro 2012]

PCM, 2012b. *Atribui à AMA a responsabilidade dos investimentos em TIC na AP (DL nº 107/2012).* Lisboa: Diário da Républica. Disponivel na Internet em: http://m6.ama.pt/docs/DL107_2012.pdf [Consultado em 14 novembro 2012]

PCM, 2012c. *Aprova a Lista de Sistemas Operacionais Críticos - (RCM 48/2012).* Lisboa: Diário da Républica. Disponível em: http://m6.ama.pt/docs/RCM_48_2012.pdf. [Consultado em 14 novembro 2012]

Repartição de Comunicação, R. P. e. P. d. E., 2013. *Estado-Maior do Exército.* [Online] Disponivel na Internet em: http://www.exercito.pt/sites/EME/Paginas/Visao_e_Missao.aspx [Consultado em 03 fevereiro 2013].

SG, 2012. *Plano de Ação Sectorial de Racionalização das TIC no Ministério da Defesa Nacional,* Lisboa: MDN.

SSTI, 2012. *Contributos para a Reorganização das Tecnologias da Informação da Defesa Nacional,* Lisboa: Marinha .

Venkatraman, J. H. a. N., 1999. Satrategic alignement: leveraging Information Technology for transforming Organizations. *IBM Systems Journal, Vol 38 nº2&3,* p. 472.

Entrevistas:

Marques, CAlm AJG, 2012. Reorganização das TIC na Defesa Nacional. Lisboa, 08 nov. 2012.

Melo, MGen PJP, 2013. Reorganização das TIC na Defesa Nacional. Lisboa, 04 fev. 2013.

Francisco, Cmg RMA, 2012. Reorganização das TIC na Defesa Nacional. Lisboa, 06 nov. 2012

Marques, Cten FD, 2012. Reorganização das TIC na Defesa Nacional. Lisboa, 15 nov. 2012

Apêndice 1 - Corpo de conceitos

Administração – a provisão e implementação de regulamentos e procedimentos relacionados com a gestão de uma organização, em apoio do cumprimento da sua missão. (NATO, 2011, pp. 2-A-3)

Ambiente de informação da Defesa - Engloba a computação (computing) e as infraestruturas de comunicações da defesa juntamente com os sistemas de gestão e as pessoas que guarnecem essa infraestrutura. Inclui as redes de computadores, aplicações de negócio e os dados que estas geram e transportam.

Ambiente único de Informação – Compreende a informação usada pela Defesa e os meios pela qual é criada, gerida manipulada armazenada, disseminada e protegida. Os dois elementos principais são os domínios da informação e as infraestruturaras da informação, e compreende todos os meios e capacidades envolvidos na troca de informação por computadores e comunicações, em todos os domínios usados pela Defesa em operações militares e no negócio da Defesa (ANAO, 2011, p. 9)

Área Funcional – Área de responsabilidade dentro de uma organização onde funções técnicas, administrativas ou operacionais são executadas. (NATO, 2001, pp. 2-15)

Arquitetura – a estrutura dos componentes de um sistema, a relação entre eles e os princípios e orientações que governam o seu desenho e evolução ao longo do tempo.

Arquitetura TI - Descrição do desenho fundamental dos componentes TI do negócio , as relações entre eles e a forma como eles suportam os objetivos da organização (ITGI, 2007, p. 190)

Atividade - A ação principal para executar um processo (ITGI, 2007, p. 189)

Avaliar – Padrão usado para avaliar o desempenho em relação aos resultados esperados As avaliações são normalmente quantitativas mas também consignam informação de qualidade tal como satisfação do utilizador. Monitorizar as avaliações ajuda as organizações a aplicar efetivamente a sua estratégia

Balanced Scorecard- Um conjunto de medidas coerentes organizado em quatro categorias. Inclui medidas financeiras, processos internos de negócio e perspetivas de aprendizagem e de crescimento (ITGI, 2007, p. 189)

Boas práticas - Uma atividade ou processo provado que foi usada com sucesso em múltiplas organizações. (ITGI, 2007, p. 189)

Capacidade – O poder de produzir um efeito que utilizadores de meios ou serviços precisam de alcançar. Uma capacidade é constituída por uma ou mais componentes funcionais: Doutrina, Organização, Treino, Material, Liderança, Pessoal, Facilidades (infraestruturas), e Interoperabilidade (DOTMLPFI). (NATO, 2005)

Ciclo de vida – Período de tempo que se inicia com a avaliação do requisito para o sistema ou produto e termina com a sua alienação. O ciclo de vida da informação compreende as etapas de: planeamento; recolha, criação ou geração de informação; a sua organização, recuperação, utilização, acessibilidade e transmissão; o seu armazenamento e proteção; e, finalmente, a sua remoção (arquivo ou destruição). (NATO, 2001, pp. 2-20)

CIO— O individuo responsável por um grupo das TI dentro de uma organização. (ITGI, 2007, p. 189)

Comando e Controlo (C2) – Autoridade, responsabilidades e atividades dos Comandantes militares na direção e coordenação das forças militares e na implementação das ordens relacionadas com a execução das operações. (NATO, 2001, pp. 2-6)

Dados - Representação de factos, conceitos ou instruções, de um modo formal, adequado à comunicação, interpretação ou tratamento por seres humanos ou meios automáticos.

Desempenho – Implementação ou realização de um processo. (ITGI, 2007, p. 190)

Domínio— No âmbito deste trabalho é o agrupamento de objetivos de controlo em patamares lógicos no ciclo de vida das TI (planeamento e organização, Aquisição e implementação, Fornecimento e apoio, monitorização e avaliação)

Governação das TI – É da responsabilidade do Conselho de Diretores e da gestão executiva. É uma parte integral da governação da organização e consiste da liderança e estruturas organizacionais e processos que garantem que as TI da organização apoiam e projetam as estratégias e objetivos da organização. (ITGI, 2003)

Incidente TI - Qualquer evento que não seja parte da operação de um serviço e que causa, ou pode causar, uma interrupção ou redução na qualidade desse serviço**.** (ITGI, 2007, p. 191)

Maturidade – Indica o grau de confiança ou dependência, no entendimento do negócio, de um processo atingir os objetivos desejados. (ITGI, 2007, p. 191)

Métrica – Descrição específica de como uma avaliação de desempenho quantitativa e periódica pode ser medida. (ITGI, 2007, p. 191)

NC&IA – tem como finalidade ligar as forças, NATO e as Nações, quando e onde requerido garantindo a interoperabilidade dos serviços e sistemas de Informação (NATO, 2013)

Padrão – Um requisito mandatório. Também pode ser referido como uma prática ou especificação publicada por uma organização de padronização. (ITGI, 2007, p. 191)

Plano de infraestruturas tecnológico – UM plano para tecnologia, recursos humanos e facilidades que permite, agora e no futuro, o processamento e uso de aplicações. (ITGI, 2007, p. 191)

Plano estratégico das TI - Plano de longo prazo não qual as TI e o negócio descrevem em cooperação como é que a gestão das TI e do negócio contribuem para os objetivos estratégicos da organização. (ITGI, 2007, p. 191)

Politicas- Geralmente, um documento que regista os princípios nível superior ou uma linha de ação que tenha sido decidida. Tem como finalidade influenciar e orientar tanto o processo de decisão corrente como o futuro para que esteja em linha com a filosofia, objetivos e planos estratégicos estabelecidos pelo nível estratégico. (ITGI, 2007, p. 191)

Portfolio – Agrupamento de programas, projetos, serviços ou ativos selecionados, geridos e monitorizados para otimizar o retorno do investimento. (ITGI, 2007, p. 191)

Procedimento – documento que contêm os passos que especificam como atingir uma atividade. Os procedimentos são definidos como parte do processo. (ITGI, 2007, p. 191)

Processo – Conjunto de procedimentos influenciado pelas políticas e procedimentos da organização e que incorpora contributos de várias fontes, incluindo outros processos. Os processos têm que ter uma razão para existir, donos do processo, regras e responsabilidades claras para a sua execução e meios para avaliar o seu desempenho. (ITGI, 2007, p. 191)

Rede – Um conjunto de computadores ou sistemas ligados por canais de comunicações que facilitam as comunicações entre os utilizadores, e permite aos utilizadores partilhar os recursos (ANAO, 2011, p. 9)

Resiliência – A capacidade de um sistema ou rede de recuperar automaticamente de qualquer interrupção com o mínimo efeito reconhecido. (ITGI, 2007, p. 191)

Responsável – Refere-se à pessoa ou grupo que tem a autoridade para aprovar ou aceitar a execução de uma atividade.

Risco – Potencial que uma dada ameaça tem em explorar uma vulnerabilidade num ativo ou grupo de ativos que possa causar a sua perda ou danos. Normalmente é medida pela combinação do impacto e a probabilidade de ocorrer

Segurança da Informação – Proteção da informação contra disseminação não autorizada, transferência, modificação ou destruição, seja ela acidental ou intencional. (NATO, 2001, pp. 2-18)

Sistema de informação – o conjunto de equipamentos, métodos e procedimentos e, se necessário, pessoal, organizados para cumprir tarefas de processamento de informação (NATO, 2011, pp. 2-I-4).

TI **-** Arte e ciências aplicadas que lidam com operações sobre dados e informação. (NATO, 2001)

SLA – Um acordo preferencialmente documentado, entre o fornecedor de serviços e o utilizador que define o desempenho mínimo que um serviço deve ter e como este deve ser medido.

TIC – Compreende todo o hardware, software, pessoal e serviços envolvidos no desenho, desenvolvimento implementação, manutenção, apoio, sustentação, operação e gestão da tecnologia para armazenar, recuperar, manipular e comunicar informação baseada em sistemas de informação (ANAO, 2011, p. 9)

Utilizador - Qualquer pessoa que usa os serviços de uma organização

Apêndice 2 - Plano Geral de Investigação

OG	QC
Identificar um modelo de governação coerente e harmonioso das TI da DN que potencie a redução de custos de exploração e configure a superioridade da informação.	*Qual o modelo organizacional e de governação mais adequado para as TI da DN?*

OE	QD	Hip
OE 1 – Identificar o atual "estado da arte" da governação das TI da DN;	**QD 1 -** Em que medida é que o atual modelo organizacional e de governabilidade das TI não satisfaz as necessidades da DN?	**Hip 1:** O atual modelo organizacional e de governabilidade seguido pelos Serviços Centrais do MDN, EMGFA, três Ramos (Marinha, Exército e Força Aérea) e pelo IASFA não permite uma racionalização dos recursos, não promove sinergias, não garante a segurança, e não fomenta a interoperabilidade.
OE 2 - Analisar modelos implementados em países de referência nesta área;	**QD 2 -** Que modelos organizacionais e de governabilidade TI têm vindo a ser adotados por organizações congéneres e por países aliados e amigos, na área da Defesa?	**Hip 2:** As organizações congéneres e os países aliados e amigos têm evoluido para um modelo de governação hibrido das TI que privilegia a centralização dos serviços nucleares e de rede colocando, concomitantemente, o seu enfoque na informação, no conhecimento e na superioridade que daí advém.
OE 3 - Definir os critérios e princípios subjacentes ao modelo a implementar na governação das TI da DN;	**QD 3 -** Que critérios e princípios devem ser considerados na escolha e edificação do modelo organizacional e de governação TI mais adequado à DN?	**Hip 3:** É possível deduzir critérios objetivos, de cariz essencialmente estratégico, gestionário e operacional, que permitem selecionar de forma criteriosa a melhor solução organizacional e de governação TI para a DN.
OE 4 - Contribuir para a identificação de um modelo organizacional e de governação das TI da DN.	**QD 4 -** Que modelo organizacional e de governação TI melhor responde aos critérios e princípios estabelecidos para o modelo organizacional e de governação no âmbito da DN ?	**Hip 4:** Estando identificados os critérios objetivos da governação da TI é possivel encontrar uma solução organizativa e de governabilidade que permita mitigar as lacunas identificadas.

Apêndice 3 – Questionário - Avaliação da maturidade da gestão e controlo dos processos das TI

1. Introdução

No âmbito de um trabalho subordinado ao tema "Reorganização das Tecnologias de Informação na Defesa", realizado no contexto do Curso de Promoção a Oficial General (CPOG), torna-se necessário avaliar o estado atual das tecnologias de informação (TI) na defesa para, a partir daí, se definir o estado desejado e as linhas de ação mais apropriadas para essa reorganização.

Sendo que as tecnologias de informação na defesa são geridas, de forma autónoma e independente, por cinco entidades diferentes, avaliar o seu estado atual corresponde, na prática, a avaliar o estado atual das tecnologias de informação em cada uma destas entidades, nomeadamente o MDN, o EMGFA, a Marinha, o Exército e a Força Aérea.

Uma avaliação desta natureza pode ser realizada segundo variadas perspetivas; contudo, considerando que os processos das TI são determinantes no fornecimento da informação necessária, de forma atempada e segura, para que a organização atinja os seus objetivos, optou-se por avaliar o estado atual das TI através do nível de maturidade da gestão e controlo desses processos. Deste modo obter-se-á um bom indicador do sucesso do setor das TI resultante da forma como estas desempenham as suas atividades e, consequentemente, contribuem para os objetivos estratégicos da organização.

O COBIT (Control Objectives for Information and related Technology), do IT Governance Institute (ITGI), é uma moldura de apoio à governança das TI que compreende um modelo de maturidade da gestão e controlo dos processos das TI. Neste modelo são definidos 34 processos, agrupados segundo 4 domínios distintos, cuja maturidade é estabelecida por um de seis níveis possíveis.

A metodologia adotada para realizar a avaliação do estado atual das TI consiste assim na auto-avaliação de cada uma das entidades referidas através deste questionário, que se baseia no modelo de maturidade do COBIT4.1.

Os resultados obtidos serão utilizados apenas no contexto deste trabalho, o qual, após conclusão, será distribuído por todos os intervenientes, designadamente os que participaram neste questionário, esperando-se assim contribuir para o sucesso das TI na defesa.

2. **Instruções**

O questionário encontra-se dividido em cinco partes.

Nas primeiras quatro partes encontrará um conjunto de questões obrigatórias, cada uma com seis opções. Não existem respostas certas ou erradas. Deverá selecionar, para cada questão, apenas a opção com a qual considera que a sua organização melhor se identifica.

Na última parte encontrará duas questões abertas, de resposta livre e opcional.

Estimamos que demore aproximadamente 30 minutos no preenchimento do questionário.

Desde já agradecemos a sua colaboração.

3. **Questionário**

Parte I – Planear e Organizar

1. Definir um planeamento estratégico das TI

O processo "Definir um planeamento estratégico das TI" satisfaz o requisito das TI que consiste em sustentar ou complementar a estratégia da organização e os requisitos da governação, assegurando a transparência no que respeita a benefícios, custos e riscos. Como avalia a maturidade deste processo na sua organização?

0	O planeamento estratégico das TI não é realizado na organização e não é reconhecida a necessidade da sua existência para apoiar os objetivos estratégicos da organização	
1	O alinhamento dos requisitos, aplicações e tecnologia é feito reactivamente e não como uma estratégia global da organização.	
2	As decisões estratégicas são feitas projeto a projeto, sem consistência com uma estratégia global da organização.	
3	Existe uma política que define quando e como deve ser feito o planeamento estratégico das TI. O planeamento estratégico das TI é estruturado e documentado e conhecido de todo o staff.	
4	O planeamento estratégico das TI ocorre tanto a curto prazo como a longo prazo e é partilhado pela organização e atualizado sempre que necessário. A estratégia das TI e a estratégia da organização estão a ficar cada vez mais coordenadas através do contributo para os processos de negócio e capacidades de valor acrescentado.	
5	O planeamento estratégico tem em conta o modo como os novos desenvolvimentos tecnológicos alavancam novas capacidades, aumentando a competitividade da organização.	

2. **Definir uma arquitetura de informação**

O processo "Definir uma arquitetura de informação" satisfaz os requisitos das TI que consistem em ser ágil na resposta aos requisitos, em fornecer uma informação consistente e credível e em integrar sem problemas aplicações nos processo da organização. Como avalia a maturidade deste processo na sua organização?

0	Não é reconhecida por parte da organização a importância de uma arquitetura da informação.	
1	A gestão reconhece a necessidade de uma arquitetura de informação. O desenvolvimento de alguns componentes da arquitetura de informação ocorre sem critério.	
2	Começam a emergir processos da arquitetura da informação, embora informais e intuitivos. Os procedimentos começam a ser seguidos por diferentes indivíduos na organização.	
3	A importância de uma arquitetura da informação é compreendida e aceite, e a responsabilidade para o seu fornecimento está atribuída e claramente comunicada. Os procedimentos relacionados, as ferramentas e técnicas, mesmo que não sofisticadas, estão padronizadas e documentadas, e são parte das atividades de treino informal. Estão desenvolvidas políticas básicas da arquitetura da informação, incluindo alguns requisitos estratégicos, mas a observância dessas políticas, padrões e ferramentas não está consistentemente implementada.	
4	O desenvolvimento e implementação de uma arquitetura da informação está apoiado por métodos e técnicas formais e o sucesso da sua execução é avaliado. As ferramentas automatizadas de apoio estão espalhadas mas ainda não estão integradas. Foram identificadas métricas básicas e está em funcionamento um sistema para a sua medição.	
5	A informação produzida pela arquitetura da informação é aplicada consistentemente e extensivamente. São amplamente usadas as boas práticas da indústria no desenvolvimento e manutenção da arquitetura da informação, incluindo processos de melhoria continua.	

3. **Determinar uma direção tecnológica**

O processo de "Determinar uma direção tecnológica" satisfaz os requisitos de negócio das TI que consiste em ter capacidades, recursos, sistemas de aplicações padronizadas, integradas e estáveis que vão ao encontro das necessidades correntes e futuras do negócio. Como avalia a maturidade deste processo na sua organização?

0	Não é reconhecida pela organização a importância do planeamento de uma infraestrutura tecnológica.	
1	O desenvolvimento de componentes tecnológicos e a implementação da tecnologia emergente são feitos *ad hoc* e isoladamente. O planeamento da infraestrutura tecnológica é reativo e centrado na parte operacional.	
2	O planeamento é ao nível tático e está vocacionado para gerar soluções para problemas técnicos em vez potenciar o uso da tecnologia para satisfazer necessidades de negócio.	
3	Existe um plano tecnológico definido, documentado e suficientemente disseminado, mas é aplicado inconsistentemente.	
4	O potencial impacto das tecnologias emergentes é levado em conta. O processo de desenvolvimento do plano de infraestruturas tecnológicas é sofisticado e responsivo à mudança.	
5	A direção do plano de infraestruturas tecnológicas é orientada pelos padrões e desenvolvimentos internacionais e da indústria e não guiado pelos fornecedores de tecnologia. Existe uma aprovação formal para novas ou mudanças de direção tecnológicas.	

4. **Definir Processos TI, organização e relacionamentos**

O processo de "Definir processos TI, organização e relacionamentos" satisfaz os requisitos de negócio das TI de modo que sejam ágeis a responder à estratégia da organização, cumprindo ao mesmo tempo com os requisitos de governação. Como avalia a maturidade deste processo na sua organização?

0	A organização TI não está efetivamente implementada para atingir os objetivos de negócio da organização	
1	Embora haja um uma compreensão implícita da necessidade de uma organização das TI, as funções e responsabilidades não estão formalizadas nem implementadas. As atividades das TI são reativas, e só são envolvidas nas últimas fases dos projetos realizados pela organização.	
2	A necessidade de uma organização TI é compreendida mas as decisões estão dependentes das perícias e conhecimentos de indivíduos chave. As funções TI estão organizadas para responder taticamente às necessidades dos utilizadores e às relações com os fornecedores.	
3	Estão definidas as funções que devem ser executadas pelo pessoal das TI e as que devem ser executadas pelos utilizadores. Os requisitos e perícias do pessoal das TI estão definidos e estabelecidos. As funções e responsabilidades das TI estão formalizadas e implementadas.	
4	A organização TI responde proactivamente à mudança e inclui as funções necessárias para satisfazer os requisitos de negócio da organização. A estrutura organizacional TI reflete as necessidades de negócio através do fornecimento de serviços alinhados com os processos estratégicos de negócio da organização, em vez de se limitar ao fornecimento de tecnologias isoladas.	
5	A tecnologia é usada extensivamente para assistir na monotorização do desempenho dos processos e da organização das TI. Está implementado um processo de evolução continua.	

5. **Gerir o investimento nas TI**

O processo " Gerir o investimento nas TI" satisfaz o requisito de negócio das TI que consiste em melhorar continuamente o custo-eficiência das TI e a sua contribuição para a rentabilidade do negocio, através de serviços padronizados e integrados que satisfazem os utilizadores. Como avalia a maturidade deste processo na sua organização?

0	Não é reconhecida a importância da seleção e do financiamento do investimento nas TI. Não é efetuado um rastreio ou monotorização dos gastos e investimentos nas TI	
1	A alocação da responsabilidade na seleção dos investimentos e o próprio financiamento das TI é feito numa base *ad hoc* e utilizando documentação informal. As decisões de financiamento são direcionadas para o nível operacional e são reativas.	
2	Existe uma compreensão implícita para a necessidade de selecionar o investimento nas TI, mas a sua observância está dependente do individuo. As decisões de financiamento são feitas ao nível tático e são reativas.	
3	Estão definidos e documentados os processos para o investimento e financiamento, que cobrem as questões tecnológicas e os elementos chave do negócio. O orçamento das TI está alinhado com a estratégia das TI e com os planos de negócio	
4	A responsabilidade para a seleção do investimento nas TI está atribuída a um individuo específico. É efetuada uma análise formal dos custos diretos e indiretos das operações existentes, dos investimentos propostos e dos custos totais do ciclo de vida. Os benefícios e retornos são calculados em termos financeiros e não-financeiros	
5	O processo de gestão do investimento é continuamente melhorado com base nas lições aprendidas e é feito a partir da análise da eficiência do investimento corrente. É incorporada na decisão dos investimentos uma análise de custos e benefícios do ciclo de vida.	

6. **Comunicar a direção e os objetivos da gestão**

O processo " Comunicar a direção e os objetivos da gestão" satisfaz os requisitos de negócio das TI que consiste em providenciar informação precisa e em tempo para os serviços das TI, riscos associados e responsabilidades correntes e futuras. Como avalia a maturidade deste processo na sua organização?

0	A gestão não estabeleceu um ambiente de controlo positivo das TI. Não é reconhecida a necessidade de estabelecer um conjunto de políticas, planos e procedimentos	
1	A gestão é reativa na abordagem dos requisitos do ambiente de controlo da informação. As políticas, procedimentos e padrões são desenvolvidos e comunicados numa base *ad hoc*. Os processos de desenvolvimento, comunicação e conformidade são informais e inconsistentes.	
2	As práticas são largamente informais. A qualidade é reconhecida como uma filosofia desejável mas as práticas são deixadas à descrição dos gestores individuais.	
3	Está desenvolvido, documentado e disseminado um ambiente completo de gestão de qualidade e de controlo da informação e que inclui um quadro para as políticas, planos e procedimentos. Embora esteja desenvolvido um quadro de políticas e procedimentos de controlo, a monitorização da sua observância é inconsistente. Estão padronizadas e formalizadas as técnicas que promovem a consciencialização da segurança.	
4	Está implementado um ambiente de controlo proactivo, o qual inclui um compromisso com a qualidade e uma consciencialização da segurança das TI. Está desenvolvido, mantido e disseminado um conjunto de políticas, planos e procedimentos que estão em consonância com as boas práticas internas.	
5	O ambiente de controlo da informação está alinhado com o quadro de gestão estratégica e com a visão e está constantemente a ser revisto, atualizado e continuamente melhorado. A monitorização, a autoavaliação e a verificação da observância são universais na organização.	

7. **Gerir os recursos humanos das TI**

O processo "gerir os recursos humanos das TI" satisfaz os requisitos de negócio das TI que consiste em adquirir pessoal competente e motivado para criar e fornecer serviços TI. Como avalia a maturidade deste processo na sua organização?

0	Não é reconhecida a importância de alinhar a gestão dos recursos humanos das TI com o processo de planeamento tecnológico da organização.	
1	A organização reconhece a necessidade da gestão dos recursos humanos das TI, mas o processo é informal e reativo.	
2	A contratação e gestão do pessoal das TI é focado no nível tático, orientada pala necessidade específicas do projeto, em vez de um entendimento equilibrado da disponibilidade de staff com competências quer internamente como externamente.	
3	Existe um processo definido e documentado para a gestão dos recursos humanos das TI. Está implementado um plano com uma aproximação estratégica para a gestão dos recursos humanos das TI. Está implementado um programa de rotação, desenhado para expandir as perícias de gestão tecnológica e de negócio.	
4	A responsabilidade pelo desenvolvimento e manutenção de um plano de gestão dos recursos humanos responsivo à mudança, está atribuída a um único individuo ou grupo com as perícias necessárias para desenvolver e manter esse mesmo plano. A gestão dos recursos humanos das TI é proactiva, tendo em conta o desenvolvimento da carreira do pessoal envolvido.	
5	A gestão dos recursos humanos TI está integrada com o planeamento tecnológico, assegurando o desenvolvimento otimizado e o uso das perícias TI disponíveis. São desenvolvidos programas de treino para todos os produtos e padrões tecnológicos antes de serem introduzidos na organização	

8. **Gerir a qualidade**

O processo "Gerir a qualidade" satisfaz os requisitos de negócio das TI que consiste em assegurar um melhoramento contínuo e mensurável da qualidade dos serviços fornecidos pelas TI. Como avalia a maturidade deste processo na sua organização?

0	A organização não tem implementado um processo de planeamento com um sistema de gestão de qualidade e com um sistema de desenvolvimento de ciclo de vida.	
1	Os gestores fazem julgamentos informais no que concerne à qualidade.	
2	As atividades do sistema de gestão de qualidade que ocorrem estão focadas nos processos dos projetos TI e não nos processos de toda a organização.	
3	Está definido um sistema de gestão de qualidade que está disseminado por toda a organização que envolve a gestão das TI e os utilizadores finais. Estão a emergir práticas e ferramentas comuns para a gestão da qualidade. São planeados e conduzidos ocasionalmente questionários de qualidade.	
4	O sistema de gestão de qualidade está aplicado a todos os processos. Está implementado e bem estruturado um programa para medir a qualidade. Os gestores TI estão a construir um conhecimento básico para medir qualidade.	
5	Os processos do sistema de gestão de qualidade são flexíveis e adaptáveis à mudança do ambiente das TI. O conhecimento base para medir a qualidade está imbuído das boas práticas externas. Os questionários de satisfação são um processo corrente, que depois de analisados, leva a que sejam implementadas ações de melhoramento.	

9. **Avaliar e gerir os riscos dasTI**

O processo "Avaliar e gerir os riscos das TI" que satisfaz os requisitos de negócio das TI que consiste em analisar e disseminar os riscos das TI e o seu potencial impacto nos objetivos e processos de negocio. Como avalia a maturidade deste processo na sua organização?

0	A avaliação dos riscos dos processos e decisões de negócio não correm na organização.	
1	Os riscos são considerados mas numa base ad hoc. Os riscos que afetam as operações diárias são raramente discutidas nas reuniões de gestão. Quando os riscos são considerados, a sua mitigação é inconsistente.	
2	A avaliação do risco existe, mas é implementada à descrição dos gestores de projeto.	
3	A gestão do risco segue um processo definido que está documentado. Está instituído um processo para mitigar os riscos quando estes são identificados.	
4	A avaliação e a gestão do risco são procedimentos padrão na organização. O risco é avaliado e mitigado ao nível do projeto individual e também regularmente no que respeita à operação das TI no geral. T Os gestores TI desenvolvem medidas padronizadas para avaliarem o risco e definem os rácios risco/retorno.	
5	Os processos de obtenção, análise e comunicação dos dados da gestão do risco estão maioritariamente automatizados. A gestão do risco está verdadeiramente integrada em todos os processos de negócio e das operações TI, é bem aceite e envolve extensivamente os utilizadores dos serviços das TI.	

10. **Gerir os projetos**

O processo "gerir os projetos" que satisfaz os requisitos de negócio das TI, que consiste em assegurar o fornecimento dos resultados dos projetos nos prazos, qualidade, orçamento acordados. Como avalia a maturidade deste processo na sua organização?

0	As técnicas de gestão de projeto não são usadas e a organização não considera os impactos do negócio associado com as falhas de gestão e com o desenvolvimento do projeto.	
1	A definição dos projetos das TI e as decisões críticas da gestão dos projetos são feitas sem envolvimento da gestão ou dos utilizadores. Não existe uma organização clara dentro das TI para a gestão de projetos. O tempo gasto nos projetos e nas despesas não são monitorizadas nem comparadas com o orçamento.	
2	A organização está num processo de desenvolver e utilizar algumas técnicas e métodos à medida que vai executando os projetos. Estão desenvolvidas orientações iniciais para muitos aspetos da gestão de projeto, mas a sua implementação é deixada à descrição do gestor de projeto.	
3	Os processos de gestão dos projetos das TI e a sua metodologia estão estabelecidos e disseminados. Os projetos das TI estão definidos com objetivos técnicos e de negócio. Está implementado um gabinete de gestão de projeto e as suas funções e responsabilidades definidas. Os projetos das TI são monitorizados com passos, prazos, orçamento e avaliação de desempenho definidos.	
4	A gestão do projeto é medida e avaliada por toda a organização e não só nas TI. Estão estabelecidos critérios de avaliação para cada passo do projeto. O valor e o risco são medidos e geridos antes, durante e depois da conclusão dos projetos. Cada vez mais os projetos levam em conta os objetivos da organização em vez de levarem em conta apenas os objetivos específicos das TI.	
5	Está implementada, em funcionamento e integrada na cultura da organização, uma metodologia de programa e projeto de ciclo de vida total. O planeamento de programas e projetos ao longo de toda a organização asseguram que os recursos TI estão a ser bem utilizados para apoiar as iniciativas estratégicas.	

Parte II – Obter e Implementar

11. Identificar soluções automatizadas

O processo "Identificar soluções automatizadas" que satisfaz os requisitos de negócio das TI que consiste na tradução de requisitos funcionais e de controlo do negócio em soluções automatizadas eficientes e efetivas. Como avalia a maturidade deste processo na sua organização?

0	A organização não requere a identificação de requisitos funcionais e de controlo do negócio para o desenvolvimento, implementação ou modificação de soluções tais como sistemas, serviços, infraestruturas, *software* e dados. A organização não está atenta às soluções tecnológicas disponíveis e potencialmente relevantes para o negócio.	
1	O *staff* reúne-se informalmente para discutir as necessidades, e por vezes os requisitos são documentados. As soluções são identificadas individualmente, através de uma procura limitada ou em resposta a ofertas dos fornecedores.	
2	As soluções são identificadas informalmente baseadas na experiencia interna e no conhecimento da função TI. O sucesso de cada projeto depende das perícias de alguns indivíduos chave. A qualidade da documentação e da tomada de decisão varia consideravelmente.	
3	A determinação das soluções TI é feita avaliando as alternativas em função dos requisitos de negócio ou dos utilizadores, oportunidades tecnológicas, viabilidade económica, avaliação de risco e outros fatores.	
4	A documentação dos projetos é de boa qualidade, e cada fase é devidamente aprovada. São consideradas soluções alternativas, incluindo a análise de custos e benefícios. A metodologia está claramente definida, geralmente compreendida e mensurável.	
5	A metodologia de aquisição e implementação tem a flexibilidade para projetos de pequena e grande dimensão. A própria metodologia produz documentação numa esturra pré-definida que faz com que a produção e manutenção sejam eficientes. São normalmente identificadas oportunidades para utilizar tecnologia para ganhar vantagem competitiva e aumentar a eficiência.	

12. **<u>Adquirir e manter aplicações de software</u>**

O processo "Adquirir e manter aplicações de software" satisfaz os requisitos de negócio das TI que consiste em alinhar as aplicações disponíveis com os requisitos de negócio, em tempo e com custos razoáveis. Como avalia a maturidade deste processo na sua organização?

0	Não existe um processo para desenhar e especificar as aplicações. Tipicamente, as aplicações são obtidas baseadas nas ofertas dos fornecedores, conhecimento da marca ou familiarização do *staff* das TI com um determinado produto, com pouca ou nenhuma consideração dos requisitos atuais.	
1	O processo de aquisição e manutenção de aplicações software varia de projeto para projeto.	
2	A razão de sucesso com as aplicações depende grandemente dos níveis de experiencia e das perícias existentes no *staff* das TI. A manutenção é usualmente problemática e sofre quando o conhecimento interno na organização é perdido.	
3	Existe um processo claro e definido para a aquisição e manutenção de aplicações de *software*. Este processo é alinhado com a estratégia das TI e do negócio. As metodologias são geralmente inflexíveis e dificilmente aplicáveis em todos os casos, pelo que alguns passos são omissos.	
4	Existe uma metodologia formal e bem compreendida que inclui um desenho e processos específicos, critérios para aquisição, um processo para teste e requisitos definidos para documentação.	
5	A aquisição é baseada em componentes com aplicações padronizadas, pré-definidas e alinhadas com as necessidades do negócio. A aquisição e a metodologia de manutenção são bastante avançadas, permitindo ter uma grande capacidade de resposta e flexibilidade às mudanças dos requisitos de negócio.	

13. **Adquirir e manter infraestruturas tecnológicas**

O processo "Adquirir e manter infraestruturas tecnológicas" satisfaz os requisitos de negócio das TI que consiste em adquirir e manter um infraestrutura das TI padronizada e integrada. Como avalia a maturidade deste processo na sua organização?

0	A gestão de uma infraestrutura tecnológica não é reconhecida como um assunto importante para ser abordado.	
1	São feitas mudanças na infraestrutura para cada aplicação nova mas sem um plano global. As atividades de manutenção reagem às necessidades de curto prazo.	
2	A aquisição e manutenção de uma infraestrutura das TI não é baseada em nenhuma estratégia definida e não considera as aplicações de negócio que precisam de ser apoiadas.	
3	Existe um processo definido, claro e geralmente compreendido para adquirir e manter infraestruturas das TI. O processo apoia as necessidades das aplicações críticas de negócio e está alinhado com a estratégia das TI e do negócio, mas não é consistentemente aplicado. A manutenção é planeada, agendada e coordenada.	
4	O processo de aquisição e manutenção de infraestruturas está desenvolvido a um nível que trabalha bem para a maioria das situações, é seguido consistentemente e é focado na reutilização. A infraestrutura tecnológica apoia adequadamente as aplicações de negócio. O processo é bem organizado e proactivo.	
5	O processo de aquisição e manutenção das infraestruturas tecnológicas é proactivo e alinhado com as aplicações críticas do negócio e com a arquitetura tecnológica. A infraestrutura TI é vista como um facilitador chave para alavancar o uso das TI.	

14. **Facilitar a operação e o uso**

O processo "Facilitar a operação e o uso" satisfaz os requisitos de negócio das TI que consiste em assegurar a satisfação dos utilizadores com ofertas de serviço, níveis de serviço e integrando sem problemas a tecnologia e as aplicações nos processos de negócio. Como avalia a maturidade deste processo na sua organização?

0	Não existe implementado um processo relacionado com a produção de documentação do utilizador, manuais de operação e material de treino. O único material existente é aquele que foi fornecido com a compra dos produtos.	
1	A documentação é ocasionalmente produzida e é distribuída inconsistentemente a grupos limitados. Muita da documentação e muitos dos procedimentos estão desatualizados.	
2	Não existe uma aproximação uniforme ao desenvolvimento de procedimentos do utilizador e de operação. O material de treino é produzido por indivíduos ou por equipas de projeto, e a qualidade depende dos indivíduos envolvidos.	
3	Existe um quadro claramente definido, aceite e compreendido para a documentação do utilizador, os manuais de operação e o material de treino. Os procedimentos são armazenados e mantidos numa biblioteca formal e podem ser acedidos por qualquer individuo que necessite de os conhecer.	
4	Os procedimentos e material de treino estão integrados de modo a incluir interdependências e interfaces. Os comentários dos utilizadores relacionados com a documentação e treino são coligidos e avaliados como parte de um processo de melhoramento. A documentação e o material de treino, são usados com um nível de confiança e disponibilidade elevados.	
5	A documentação e o material de treino é atualizado para refletir as mudanças organizacionais, operacionais e de s*oftware*. O desenvolvimento de documentação, do material de treino e o fornecimento de programas de treino estão completamente integrados com o negócio e com as definições de processos de negócio, suportando os requisitos de toda a organização e não só os procedimentos orientados para as TI.	

15. **Obter recursos das TI**

O processo "Obter recursos das TI" satisfaz o requisito de negócio das TI que consiste em melhorar o custo-eficácia e contribuir para a rentabilidade do negócio. Como avalia a maturidade deste processo na sua organização?

0	Não existe implementado um processo definido de obter recursos das TI.	
1	Existe apenas uma relação *ad hoc* entre as aquisições da organização, processos de gestão dos contratos e as TI.	
2	Os processos de aquisição são utilizados maioritariamente para projetos de grande dimensão e visibilidade.	
3	As políticas e procedimentos são orientados pelo processo de aquisição global da organização. A aquisição das TI está largamente integrada com os sistemas de aquisição da organização. Existem padrões para a aquisição dos recursos das TI.	
4	A aquisição das TI está completamente integrada com os sistemas de aquisição de toda a organização. São tomadas medidas de aferição na gestão das aquisições e dos contratos relevantes para as TI.	
5	A gestão assegura a aplicação de políticas e procedimentos na aquisição das TI. Estão implementadas medidas de aferição na gestão das aquisições e dos contratos das TI mais relevantes para a organização. As relações com os fornecedores e parceiros são geridas estrategicamente.	

16. **Gerir as mudanças**

O processo "gerir as mudanças" satisfaz os requisitos de negócio das TI que consiste em responder aos requisitos de negócio em linha com a estratégia de negócio da organização, e ao mesmo tempo reduzir os defeitos das soluções e serviços fornecidos. Como avalia a maturidade deste processo na sua organização?

0	Não existe um processo definido da gestão da mudança, podendo as mudanças serem feitas sem nenhum controlo.	
1	Não existe e se existe é de fraca qualidade, documentação das mudanças efetuadas, e a configuração da documentação é incompleta e falível. É provável ocorrerem erros em conjunto com interrupções no ambiente de produção causadas por uma fraca gestão da mudança.	
2	Existe implementado um processo informal de gestão da mudança e a maioria das mudanças seguem essa aproximação, mas no entanto não é estruturada, é rudimentar e susceptivel ao erro.	
3	Existe implementado um processo de gestão da mudança formal, que inclui a caracterização, priorização, procedimentos de emergência e autorização da mudança, e a sua observância começa a emergir. Estão implementadas soluções alternativas e os processos são muitas vezes ignorados. As análises do impacto das mudanças TI nas operações do negócio começam a ser formalizadas para apoiar lançamentos planeados de novas aplicações e tecnologias.	
4	O processo é eficiente e efetivo, mas depende consideravelmente de procedimentos e controlos manuais para assegurar que a qualidade seja atingida. Todas as mudanças são sujeitas a planeamento e avaliação de impacto de modo a minimizar a ocorrência de prolemas futuros. Está implementado um processo de aprovação para as mudanças.	
5	O processo de revisão reflete a monitorização do resultado. A gestão da mudança TI está integrada com a gestão da mudança do negócio para assegurar que que as TI sejam um facilitador para o aumento da produtividade e para a criação de novas oportunidades de negócio para a organização.	

17. **Instalar e acreditar as soluções e as mudanças**

O processo "Instalar e acreditar as soluções e as mudanças" satisfaz o requisito de negócio das TI que consiste em implementar sistemas novos ou modificados que trabalhem sem problemas de maior após a sua instalação. Como avalia a maturidade deste processo na sua organização?

0	Existe a falta de um processo de instalação e de acreditação formal, e nem os gestores superiores nem os membros do *staff* das TI reconhece a necessidade de verificar que as soluções estão adaptadas à sua finalidade.	
1	Em alguns projetos são efetuados testes, mas a iniciativa para testar é deixada às equipas do projeto, e as aproximações tomadas variam bastante. A acreditação formal e a sua assinatura são raras ou não existentes	
2	Existe alguma consistência nas aproximações aos testes e à acreditação, mas não são baseadas em nenhuma metodologia. São as equipas de desenvolvimento que normalmente decidem que tipo de teste devem efetuar. Não existe um processo de aprovação formal.	
3	Os processos de instalação e acreditação estão integrados nos ciclos de vida dos sistemas e até certo nível, automatizados. A qualidade dos sistemas a entrar em produção é inconsistente com os novos sistemas, e geram com alguma frequência problemas de pós-implementação.	
4	A qualidade dos sistemas a entrar em produção é satisfatória com níveis aceitáveis de problemas pós-instalação. O processo de automatização é feito sem critério e dependente do projeto. A gestão pode estar satisfeita com o atual nível de eficiência, apesar da falta de avaliação após a implementação. O sistema de teste reflete adequadamente o ambiente de operação.	
5	Os processos de instalação e de acreditação estão completamente integrados no ciclo de vida dos sistemas e automatizados quando apropriados, facilitando o treino, teste e transição para o ambiente de produção. Os ambientes de teste estão bem desenvolvidos, os registos dos problemas e processos de resolução de falhas asseguram uma transição eficiente e efetiva para o ambiente de produção.	

Parte III – Fornecer e Apoiar

18. Definir e gerir níveis de serviço

O processo "Definir e gerir níveis de serviço" satisfaz o requisito de negócio das TI que consiste em assegurar o alinhamento dos serviços chave das TI com a estratégia de negócio. Como avalia a maturidade deste processo na sua organização?

0	A gestão não reconhece a necessidade dum processo para definir níveis de serviço. As responsabilidades para os monitorizar não estão atribuídas.	
1	Existe a consciência da necessidade de gerir os níveis de serviço, mas o processo é informal e reativo. A responsabilidade para definir e gerir serviços não está definida.	
2	Existem níveis de serviço acordados, mas eles são informais e não revistos. Os relatórios de níveis de serviço são incompletos e podem ser irrelevantes ou enganosos para os clientes. Os relatórios de níveis de serviço estão dependentes das perícias e iniciativas dos gestores individuais.	
3	Serviços e níveis de serviço estão definidos, documentados e acordados usando um processo padrão. As deficiências nos níveis de serviço estão identificadas, mas os procedimentos para as resolver são informais.	
4	Os níveis de serviço são cada vez mais definidos na fase de definição de requisitos do sistema e incorporadas no desenho da aplicação e nos ambientes operacionais. A satisfação do cliente é rotineiramente medida e avaliada. Os critérios para a definição de níveis de serviço baseiam-se no nível de importância do negócio e incluem disponibilidade, confiabilidade, desempenho, capacidade de crescimento, apoio ao utilizador, planeamento contínuo e considerações de segurança. Quando os níveis de serviço não são atingidos, são analisadas as causas para que isso não acontecesse.	
5	Os níveis de serviço são continuamente reavaliados para garantir o alinhamento dos objetivos TI com os objetivos do negócio, enquanto beneficiam da tecnologia, incluindo a razão custo-benefício. Os níveis de satisfação do cliente são continuamente monitorizados e geridos. A gestão de TI tem os recursos e as responsabilidades necessárias para atingir as metas dos níveis de serviço.	

19. Gerir os serviços de terceiros

O processo "Gerir os serviços de terceiros" satisfaz o requisito de negócio das TI que consiste em assegurar o fornecimento de serviços satisfatórios por terceiros, assegurando a transparência no que respeita a benefícios, custos e riscos. Como avalia a maturidade deste processo na sua organização?

0	As responsabilidades não estão definidas. Não existem políticas e procedimentos formais no que diz respeito aos contratos com terceiros. Não existem atividades de medição nem a apresentação de relatórios por parte dos terceiros.	
1	Não existem termos de acordo padrão com os prestadores de serviços. A medição dos serviços prestados é informal e reativa.	
2	O processo para a supervisão dos prestadores de serviços, riscos associados e a entrega de serviços é informal. É utilizado um contrato assinado com termos e condicões (por exemplo a descrição dos serviços prestados).	
3	Existem procedimentos bem documentados para a governação dos serviços de terceiros, com processos claros para controlar e negociar com os fornecedores.	
4	As qualificações do fornecedor, os riscos e as capacidades são verificadas continuamente. Os requisitos do serviço estão definidos e ligados aos objetivos de negócio. Existe um processo para analisar se o desempenho de serviço está conforme os termos contratuais, fornecendo informações para avaliar os serviços de terceiros atuais e futuros.	
5	A evidência de conformidade do contrato face aos requisitos operacionais, legais e de controlo é monitorizada e as soluções corretivas são impostas. O terceiro está sujeito a uma revisão independente periódica e o *feedback* sobre o desempenho é fornecido e utilizado para melhorar a prestação de serviços.	

20. Gerir desempenho e capacidade

O processo "Gerir desempenho e capacidade" satisfaz o requisito de negócio das TI que consiste em otimizar o desempenho da infraestrutura TI, recursos e capacidades em resposta às necessidades de negócio. Como avalia a maturidade deste processo na sua organização?

0	A Gestão não reconhece que processos de negócio chave podem exigir altos níveis de desempenho das TI ou que a necessidade global do negócio para serviços das TI pode exceder a capacidade. Não existe nenhum processo de planeamento de capacidades.	
1	Os utilizadores procuram soluções alternativas para as restrições de capacidade e desempenho. As medidas tomadas para gerir o desempenho e as capacidades são tipicamente reativas. O processo de planeamento das capacidades e do desempenho é informal.	
2	As necessidades de desempenho são geralmente identificadas com base nas avaliações de sistemas individuais e no conhecimento das equipes de projeto e apoio. Algumas ferramentas individuais podem ser usadas para diagnosticar problemas de desempenho e capacidade, mas a consistência dos resultados depende da especialização dos indivíduos-chave. Problemas de disponibilidade podem ocorrer de forma inesperada e aleatória e levam bastante tempo a diagnosticar e corrigir.	
3	Os desempenhos futuros e os requisitos de capacidade são modelados seguindo um processo definido. Os relatórios são produzidos dando estatísticas de desempenho.	
4	As questões de capacidade e desempenho insuficientes são tratadas de acordo com procedimentos definidos e normalizados. São usadas ferramentas automatizadas para monitorizar recursos específicos, como espaço em disco, redes, servidores e *gateways* de rede. Em geral os utilizadores estão satisfeitos com a atual capacidade de serviço e poderão exigir novos e melhores níveis de disponibilidade.	
5	A infraestrutura das TI e os requisitos do negócio estão sujeitos a revisões periódicas para assegurar que a capacidade ideal é alcançada com o menor custo possível. Ferramentas para monitorizar os recursos críticos das TI são normalizadas, usadas em todas as plataformas e estão ligadas a um sistema de gestão de incidentes de toda a organização.	

21. **<u>Assegurar um serviço continuo</u>**

O processo "Assegurar um serviço contínuo" satisfaz o requisito de negócio das TI que consiste em assegurar um impacto no negócio mínimo no caso de uma interrupção do serviço TI. Como avalia a maturidade deste processo na sua organização?

0	Não existe nenhuma compreensão dos riscos, vulnerabilidades e ameaças para as operações das TI ou o impacto para o negócio em caso de perda de serviços de TI. A gestão não sente necessidade de ter em atenção a continuidade do serviço.	
1	O foco de atenção da gestão no serviço contínuo está mais virado para os recursos de infraestrutura, e não aos serviços das TI. Os utilizadores implementam soluções alternativas em resposta aos problemas. A resposta para grandes perturbações é reativa e mal preparada.	
2	Os relatórios sobre a disponibilidade do sistema são esporádicos, podem ser incompletos e não têm em conta o impacto sobre o negócio. Não existe nenhum plano de continuidade documentado, embora haja compromisso de disponibilidade de serviço contínuo e os seus principais princípios são conhecidos.	
3	O plano de continuidade das TI é documentado e é baseado na criticidade do sistema e no impacto na organização. Existem relatórios periódicos dos testes ao serviço contínuo. Os indivíduos tomam a iniciativa de seguir as normas e de obter formação para lidar com incidentes graves ou mesmo com um desastre.	
4	As atividades de manutenção são baseadas nos resultados de testes no serviço contínuo, nas boas práticas internas e nas mudanças do ambiente das TI e do negócio. São recolhidos dados estruturados sobre serviço contínuo, analisados, relatados e tomadas as ações devidas.	
5	O plano de continuidade das TI é integrado com os planos de continuidade do negócio e é rotineiramente atualizado. O requisito de manter um serviço contínuo é assegurado pelos vendedores e principais fornecedores. Existe uma verificação global do plano de continuidade e os seus resultados são utilizados para atualizar o plano.	

22. **Assegurar os sistemas de segurança**

O processo "Assegurar os sistemas de segurança" satisfaz o requisito de negócio das TI que consiste em manter a integridade da informação e processamento das infraestruturas e em minimizar o impacto das vulnerabilidades na segurança e dos incidentes. Como avalia a maturidade deste processo na sua organização?

0	A organização não reconhece a necessidade de segurança nas TI.	
1	A segurança das TI é abordada de forma reativa. A segurança das TI não é medida. As falhas detetadas procuram atribuir a culpa a alguém, porque as responsabilidades não são claras.	
2	Embora as informações relevantes a segurança sejam produzidas por sistemas, não é analisada. Os serviços de terceiros podem não abordar as necessidades específicas de segurança da organização. As políticas de segurança estão a ser desenvolvidas, mas as perícias e as ferramentas são insuficientes.	
3	As responsabilidades em matéria de segurança das TI estão atribuídas e entendidas, mas não são consistentemente aplicadas. Existe um plano de segurança TI e soluções de segurança impulsionados pela análise de risco.	
4	A análise de risco e o impacto na segurança das TI é consistentemente realizada. A identificação dos utilizadores, autenticação e autorização estão padronizados. São feitos testes de segurança usando processos padrão e formalizados, levando à melhoria dos níveis de segurança. Os processos de segurança das TI são coordenados com a função de segurança de toda a organização. Os relatórios de segurança das TI estão ligados aos objetivos de negócio.	
5	Os incidentes de segurança são prontamente abordados com procedimentos de resposta a incidentes formalizados e apoiados em ferramentas automatizadas. São realizadas aferições periódicas à segurança para avaliar a eficácia da implementação do plano de segurança. As informações sobre ameaças e vulnerabilidades são sistematicamente coligidas e analisadas.	

23. **Identificar e alocar custos**

O processo "identificar e alocar custos" satisfaz o requisito de negócio das TI que consiste em assegurar a transparência e a compreensão dos custos TI, e em melhorar o custo-eficácia através do uso bem informado dos serviços TI. Como avalia a maturidade deste processo na sua organização?

0	Não existe um processo reconhecido para identificar e distribuir custos no que diz respeito ao fornecimento de serviços de informação. A organização não reconhece a necessidade de contabilizar os custos e não gera nenhuma discussão sobre o assunto.	
1	Existe um entendimento generalizado dos custos totais de serviços de informação, mas não existe nenhuma identificação dos custos por utilizador, cliente, departamento, grupos de utilizadores, funções de serviço, projetos ou produtos finais. Praticamente não existe nenhuma monitorização de custos, mas apenas um relatório de custos agregados a ser entregue a gestão.	
2	A distribuição de custos baseia-se na suposição do custo informal ou rudimentar (por exemplo, custos de hardware), e praticamente não existe nenhuma ligação a medidas de criação de valor. Não existe nenhuma formação ou comunicação sobre o procedimento padrão para a identificação e distribuição de custos.	
3	Está definido um processo para relacionar os custos de TI com os serviços prestados aos utilizadores.	
4	São identificados custos diretos e indiretos e são transmitidos à gestão e utilizadores do processo de negócio, de uma forma atempada e automatizada. Os relatórios do custo dos serviços de informação estão ligados aos objetivos da organização e SLAs e são monitorizados.	
5	Os custos são identificados como itens cobráveis que poderiam apoiar um sistema de cobrança aos utilizadores com base nos serviços prestados. O acompanhamento e a avaliação dos custos dos serviços são usados para otimizar as despesas na obtenção dos recursos das TI. Os relatórios dos custos do serviço de informação fornecem um aviso antecipado para uma possível alteração dos requisitos de negócios.	

24. **Educar e treinar os utilizadores**

O processo "Formar e treinar os utilizadores" satisfaz o requisito de negócio das TI que consiste em usar de uma maneira eficaz e eficiente soluções tecnológicas e aplicações que asseguram que os utilizadores cumprem as politicas e procedimentos. Como avalia a maturidade deste processo na sua organização?

0	Não existe um programa de formação e treino. A organização não reconhece a necessidade de abordar as questões relacionadas com a formação, não existindo nenhuma discussão sobre o assunto.	
1	Na ausência dum programa organizado, os funcionários identificam e participam em cursos de formação por sua conta própria.	
2	Existe a consciência da necessidade dum programa de treino e educação e para os processos associados em toda a organização. Não está definido um programa de formação e treino e estas atividades, executadas de forma não sistemática, dependem fortemente, e variam substancialmente, de acordo com os formadores.	
3	Está instituído e disseminado um programa de treino e formação em que os colaboradores e gestores identificam e documentam as necessidades de formação. Os processos de treino e formação são padronizados e documentados.	
4	Existe um programa abrangente de treino e formação com resultados mensuráveis. O treino e formação são componentes que fazem parte da carreira do individuo. A gestão apoia e participa em sessões de treino e educação. Os processos estão constantemente a ser melhorados levando em conta as melhores práticas internas.	
5	O treino e formação providenciada resultam numa melhoria do desempenho individual. O treino e formação são componentes críticos da carreira do individuo. São disponibilizados orçamentos, recursos, instalações e instrutores suficientes para os programas de treino e formação. Os processos são refinados e melhorados, aproveitando as melhores práticas externas e modelos de maturidade usando uma aferição com outras organizações.	

25. **Gerir o serviço de apoio e incidentes**

O processo "Gerir o serviço de apoio e incidentes" satisfaz o requisito de negócio das TI que consiste em permitir o uso efetivo dos sistemas TI pela realização de consultas e questionários ao utilizador e análise e resolução de incidentes TI. Como avalia a maturidade deste processo na sua organização?

0	Não existe apoio para solucionar problemas e dúvidas do utilizador. Não existe um processo de gestão de incidentes. A organização não reconhece a necessidade de abordar esta questão.	
1	Não existe nenhum processo normalizado, sendo apenas fornecido um apoio reativo. A gestão não monitoriza as questões do utilizador, os incidentes ou as tendências.	
2	Está disponível uma assistência informal, que consiste numa rede de indivíduos com bons conhecimentos. Estes indivíduos têm algumas ferramentas comuns disponíveis para auxiliar na resolução de incidentes.	
3	Os procedimentos estão padronizados e documentados, e a formação é informal. É deixada à descrição do individuo a obtenção de formação e o cumprimento das normas. As perguntas frequentes (FAQs) e as diretrizes de utilizador estão criadas, mas indivíduos terão de as procurar e podem não segui-las. A resposta em tempo útil para questões e incidentes não é medida, e os incidentes podem ficar sem ser resolvidos. Os utilizadores recebem uma comunicação clara sobre onde e como relatar problemas e incidentes.	
4	Existe uma compreensão dos benefícios dum processo de gestão de incidentes em todos os níveis da organização, e a função de serviço de apoio está estabelecida em certas unidades organizacionais. As responsabilidades são claras, e a eficácia é monitorizada. O pessoal do serviço de apoio é treinado e os processos são melhorados através da utilização de software específico para cada tarefa.	
5	O processo de gestão de incidentes e a função do serviço de apoio estão estabelecidos, bem organizados e assumem uma orientação de serviço ao cliente. As FAQs são bastante extensas e abrangentes e fazem uma parte integrante da base de conhecimento. Os processos foram refinados ao nível das melhores práticas da indústria, com base nos resultados da análise de indicadores de desempenho, melhoria contínua e aferição com outras organizações.	

26. **Gerir a configuração**

O processo "Gerir a configuração " satisfaz o requisito de negócio das TI que consiste em otimizar a infraestrutura TI, recursos e capacidades e a responsabilidade pelos ativos TI. Como avalia a maturidade deste processo na sua organização?

0	A Gestão não tem a noção dos benefícios em ter um processo que é capaz de produzir relatórios e gerir a infraestrutura das TI, tanto para configurações de hardware ou como para software.	
1	As tarefas de gestão de configuração básica, tais como a manutenção de inventários de hardware e software, são realizadas de forma individual. Não estão definidas práticas padrão.	
2	A gestão está ciente da necessidade de controlar a configuração das TI e compreende os benefícios de uma configuração da informação precisa e completa, mas existe uma dependência implícita nos conhecimentos e na experiência dos técnicos. Não estão definidas práticas de trabalho padrão.	
3	Os procedimentos e práticas de trabalho estão documentados, normalizados e comunicados, mas a formação e aplicação das normas recai na vontade do indivíduo. Além disso, ferramentas semelhantes para gerir a configuração estão implementadas em várias plataformas.	
4	As normas e procedimentos são comunicados e incorporados na formação e os desvios são monitorizados, controlados e relatados. Os sistemas de gestão de configuração cobrem a maior parte dos ativos das TI e permitem uma gestão de lançamento e um controlo da distribuição adequados. As análises de exceção, bem como as verificações físicas, são consistentemente aplicadas e as suas causas investigadas.	
5	Todos os ativos das TI são geridos num sistema de gestão de configuração central que contém todas as informações necessárias sobre os componentes, suas inter-relações e eventos. Existe uma integração total de processos inter-relacionados, e os mesmos utilizam e atualizam os dados de configuração duma forma automatizada. São impostas regras para limitar a instalação de software não autorizado. A gestão prevê reparações e atualizações baseadas em relatórios de análise, fornecendo atualizações programadas e capacidades de tecnologia renovada.	

27. **Gerir problemas**

O processo "Gerir problemas " satisfaz o requisito de negócio das TI que consiste em assegurar a satisfação dos utilizadores com o serviço oferecido e níveis de serviço e reduz os defeitos e a necessidade de refazer o trabalho. Como avalia a maturidade deste processo na sua organização?

0	Não existe consciência da necessidade de gerir problemas, pois não existe nenhuma diferenciação entre incidentes e problemas. Por isso não existe nenhuma tentativa para identificar a causa principal dos incidentes.	
1	O pessoal com o conhecimento chave presta assistência na resolução dos problemas relativos à sua área de atuação, mas a responsabilidade pela gestão dos problemas não está atribuída. As informações não são compartilhadas, resultando na criação de problemas adicionais e perda de tempo produtivo durante a procura de respostas.	
2	O processo de resolução evoluiu a um nível tal, que os indivíduos-chave são responsáveis por identificar e resolver os problemas. As informações são compartilhadas entre funcionários duma maneira informal e reativa. O nível de serviço para a comunidade de utilizadores varia e é dificultado pelos conhecimentos insuficientemente estruturados disponíveis ao gestor do problema.	
3	A resolução dos problemas e os processos de agravamento estão normalizados. O registo e acompanhamento dos problemas e as suas resoluções estão descentralizados e fragmentados dentro de uma equipa de resposta que usa as ferramentas disponíveis. As informações são compartilhadas entre o pessoal envolvido de forma proactiva e formal. A revisão por parte da gestão dos incidentes, da análise da identificação dos problemas e a sua resolução é limitada e informal.	
4	Os métodos e os procedimentos estão documentados, comunicados e medidos pela eficácia. A maioria dos problemas são identificados, registados e relatados, e a sua resolução iniciada. Os conhecimentos e competências são cultivados, mantidos e desenvolvidos para níveis mais elevados, pois a função é vista como um ativo e o principal contribuidor para a realização dos objetivos das TI e para a melhoria dos serviços.	
5	Os problemas são antecipados e evitados. O conhecimento sobre padrões de problemas do passado e do futuro é mantido através de contactos regulares com os fornecedores e especialistas. A maioria dos sistemas estão equipados com mecanismos automáticos de deteção e alerta, que são continuamente controlados e avaliados.	

28. **Gerir dados**

O processo "Gerir dados " satisfaz o requisito de negócio das TI que consiste em otimizar o uso da informação e que a informação está disponível quando requerida. Como avalia a maturidade deste processo na sua organização?

0	Os dados não são reconhecidos como ativos e recursos corporativos. Não está identificado um responsável pelos dados nem atribuída responsabilidade individual para a gestão dos mesmos. A segurança e a qualidade dos dados é pobre ou inexistente.	
1	Existe uma abordagem *ad hoc* para a especificação de requisitos de segurança e para a gestão de dados, mas não existem procedimentos de comunicação formal. Não ocorre nenhuma formação específica na gestão de dados. A responsabilidade pela gestão de dados não é clara.	
2	Começa a existir uma responsabilização pelos dados nos níveis superiores da gestão. Os requisitos de segurança para a gestão dos dados são documentados por indivíduos-chave. As responsabilidades para a gestão de dados são atribuídas informalmente a pessoal chave das TI.	
3	A responsabilidade pelos dados está atribuída à entidade que controla a integridade e a segurança. Os procedimentos de gestão de dados estão formalizados dentro das TI, e algumas ferramentas de backup/restauração e eliminação de equipamentos são utilizadas.	
4	A responsabilidade pela propriedade dos dados e a sua gestão está claramente definida, atribuída e comunicada por toda a organização. Os procedimentos são formalizados e amplamente conhecidos, e o conhecimento é compartilhado. Os objetivos e indicadores de desempenho são acordados com os clientes e monitorizados através dum processo bem definido. Existe formação para os membros da equipa de gestão de dados.	
5	Os requisitos e necessidades futuras são explorados de forma pró-ativa. As responsabilidades para a propriedade dos dados e a gestão dos mesmos são claramente estabelecidas, amplamente conhecidas em toda a organização e atualizadas em tempo útil. São utilizadas ferramentas sofisticadas com grande automatização para a gestão de dados. As oportunidades de melhoria são exploradas constantemente.	

29. Gerir o ambiente físico

O processo "Gerir o ambiente físico" satisfaz o requisito de negócio das TI que consiste em proteger os componentes do computador e os dados do negócio e em minimizar o risco de disrupção do negócio. Como avalia a maturidade deste processo na sua organização?

0	Não existe consciência da necessidade de proteger as instalações ou o investimento em recursos de computação. Os fatores ambientais, incluindo a proteção contra incêndios, poeira, eletricidade e o calor e humidade em excesso, não são nem monitorizados nem controlados.	
1	A gestão das instalações e equipamentos é feita de acordo com as competências e perícias de indivíduos-chave. O pessoal pode movimentar-se dentro das instalações sem restrição. A gestão não monitoriza os controlos ambientais das instalações ou o movimento de pessoal.	
2	Os procedimentos de manutenção das instalações não estão bem documentados e dependem de boas práticas de alguns indivíduos.	
3	Os controlos ambientais, a manutenção preventiva e a segurança física são itens que constam no orçamento aprovado pela administração. As restrições de acesso são aplicadas, sendo apenas permitido o acesso às instalações de computação por pessoal autorizado.	
4	Os requisitos ambientais e de segurança física estão documentados e o acesso é estritamente controlado e monitorizado. Os membros da equipa responsável pelas instalações têm treino sobre situações de emergência, bem como nas práticas de saúde e segurança. A administração monitoriza a eficácia dos controlos e a observância dos padrões estabelecidos. A administração estabeleceu métricas e objetivos para medir a gestão do ambiente computacional.	
5	Os padrões são definidos para todas as instalações, incluindo a escolha do local, a construção, a guarda, a segurança pessoal, os sistemas mecânicos e elétricos e a proteção contra fatores ambientais (p. ex., incêndio, inundações). Todas as instalações são inventariadas e classificadas de acordo com o processo de gestão de risco em curso na organização. O acesso é estritamente controlado e feito numa base de necessidade de trabalho, é monitorizado continuamente, e todos os visitantes são sempre acompanhados. O ambiente é monitorizado e controlado por meio de equipamento especializado, e as salas de equipamentos deixaram de ter necessidade de ser guarnecidas. Os objetivos são continuamente medidos e avaliados.	

30. **Gerir as operações**

O processo "Gerir as operações" satisfaz o requisito de negócio das TI que consiste em manter a integridade dos dados e em assegurar que a infraestrutura TI pode resistir e recuperar da ocorrência de erros e falhas. Como avalia a maturidade deste processo na sua organização?

0	A organização não dedica nem tempo nem recursos para a criação de atividades de operações e de apoio básico das TI.	
1	São estabelecidos alguns procedimentos padrão, e as atividades de operações são reativas. A maioria dos processos operacionais são programados informalmente, e o processamento dos pedidos é feito sem validação prévia. Os computadores, os sistemas e as aplicações que apoiam os processos de negócio são frequentemente interrompidos, atrasados ou estão indisponíveis.	
2	O orçamento disponível para as ferramentas é distribuído caso a caso. As operações de apoio são informais e intuitivas. Existe uma grande dependência nas competências e perícias dos indivíduos. As instruções sobre o que fazer, quando e em que ordem não estão documentados.	
3	Os recursos são alocados e existe algum treino «on-job». As funções repetitivas estão definidas formalmente, normalizadas, documentadas e comunicadas. Os eventos e os resultados das tarefas finalizadas são registados, com uma comunicação limitada à gestão. Os contratos de manutenção e de prestação de serviço com os fornecedores são informais.	
4	O planeamento e as tarefas estão documentados e comunicados, tanto internamente, para a função de TI como para os clientes do negócio. É possível medir e monitorizar as atividades diárias através de protocolos de desempenho normalizados e níveis de serviço estabelecidos. A gestão monitoriza o uso de recursos de computação e a realização do trabalho ou tarefas atribuídas. São estabelecidos acordos formais de manutenção e de serviços com os fornecedores.	
5	Os processos operacionais de gestão das TI são padronizados e documentados com base no conhecimento e são sujeitos a uma melhoria contínua. Os processos automatizados que apoiam os sistemas funcionam perfeitamente e contribuem para um ambiente estável. Todos os problemas e falhas são analisados para identificar a sua causa. São realizadas reuniões frequentes com a gestão das mudanças que asseguram a inclusão em tempo das mudanças no agendamento da produção.	

Parte IV – Monitorizar e Avaliar

31. Monitorizar e avaliar o desempenho das TI

O processo de "Monitorizar e avaliar o desempenho das TI" satisfaz os requisitos de negócio das TI no que respeita à transparência e compreensão dos custos TI, benefícios, estratégias, politicas e níveis de serviço de acordo com os requisitos de governação. Como avalia a maturidade deste processo na sua organização?

0	A organização não tem um processo de monitorização implementado. As TI não fazem monitorização independente dos projetos ou dos processos. Não estão disponíveis relatórios uteis, atempados e precisos. A necessidade de compreender claramente os objetivos dos processos não é reconhecida.	
1	A monitorização está implementada e as métricas são escolhidas caso a caso, de acordo com as necessidades dos processos e dos projetos específicos das TI. A monitorização é geralmente implementada reactivamente para responder a um acidente que tenha causado alguma perda ou embaraço para a organização.	
2	A interpretação dos resultados monitorizados é baseada nas perícias de indivíduos chave. São escolhidas e implementadas ferramentas limitadas para a recolha de informação, mas não existe uma aproximação planeada.	
3	Está desenvolvido um conhecimento base formalizado do histórico do desempenho. A avaliação ainda é efetuada ao nível dos projetos e processos TI individuais e não está integrada em todos os projetos. Estão definidos medições de desempenho TI, medições não financeiras, medições estratégicas, medições de satisfação do utilizador e medições de níveis de serviço. Está definido um enquadramento para medir o desempenho.	
4	Existe uma integração das métricas ao longo de todos os projetos e processos TI. A gestão é capaz de avaliar o desempenho, baseado em critérios aprovados. A medição da função TI está alinhada com os objetivos de toda a organização.	
5	Todos os processos de monitorização estão otimizados e apoiam os objetivos de toda a organização. São usadas como rotina, métricas orientadas pelo negócio para medir o desempenho, que estão integradas nos quadros de avaliação estratégico, tais como o *balanced scorecard*. Os processos de monitorização estão consistentes com os planos de melhoria dos processos da organização.	

32. Monitorizar o controlo interno

O processo "Monitorizar e avaliar o controlo interno" que satisfaz os requisitos de negócio das TI que consiste em proteger a obtenção dos objetivos das TI, obedecendo às leis e regulamentos relacionados com as TI. Como avalia a maturidade deste processo na sua organização?

0	A organização tem falta de procedimentos para monitorizar a eficiência dos controlos internos. Não estão implementados métodos de reportar a gestão do controlo interno. Não existe consciência da necessidade de segurança operacional TI ou de assegurar um controlo interno.	
1	São aplicadas perícias individuais para avaliar o controlo interno, mas sem nenhum critério. A gestão TI não atribuiu formalmente a responsabilidade para monitorizar a eficiência dos controlos internos.	
2	A avaliação do controlo interno está dependente num conjunto de perícias de indivíduos chave. Começam a ser usadas metodologias e ferramentas para monitorizar controlos internos, mas sem um plano. Fatores de risco específico para o ambiente TI são identificados com base em perícias individuais.	
3	As políticas e procedimentos são desenvolvidos para avaliar e comunicar as atividades de monitorização do controlo interno. São usadas políticas de avaliação de risco dos processos TI dentro de um quadro de controlo desenvolvido especificamente para a organização TI. Estão definidas politicas de mitigação e de processos de risco especifico.	
4	A organização estabelece níveis de tolerância para o processo de controlo interno das TI. São implementadas ferramentas para padronizar as avaliações e detetar automaticamente exceções de controlo. Está estabelecida formalmente uma função de controlo interna TI, com indivíduos especializados e certificados utilizando um quadro de controlo formal endossado pela gestão de nível superior.	
5	A gestão implementa em toda a organização um programa de melhoria contínua que leva em conta as lições aprendidas e as boas práticas da indústria para a monitorização do controlo interno. A organização utiliza ferramentas integradas e atualizadas, quando apropriado, que permite uma avaliação efetiva dos controlos críticos das TI e uma rápida deteção de incidentes de monitorização de controlo.	

33. **Assegurar a observância dos requisitos externos**

O processo "Assegurar a observância dos requisitos externos" satisfaz os requisitos de negócio das TI que consiste em garantir o cumprimento das leis, regulamentos e requisitos contratuais. Como avalia a maturidade deste processo na sua organização?

0	Existe pouca consciência dos requisitos externos que afetam as TI, sem nenhum processo que assegure o cumprimento dos requisitos contratuais, legais e regulatórios	
1	Existe consciência que a observância dos requisitos contratuais, legais e regulatórios tem impacto na organização. São seguidos processos informais para manter a observância, mas só quando essa necessidade surge em novos projetos ou em resposta a auditorias.	
2	Onde a observância é um requisito recorrente, tais como nos regulamentos financeiros ou legislação de privacidade, são desenvolvidos procedimentos individuais de observância e são seguidos numa base anual. No entanto, não existe uma abordagem padronizada. Existe uma confiança elevada no conhecimento e responsabilidades dos indivíduos, e os erros provavelmente acontecerão.	
3	O controlo efetuado é muito limitado e existem requisitos de observância que nunca foram analisados. Existem contratos padronizados e processos legais para minimizar os riscos associados com a responsabilidade contratual.	
4	Está implementado um mecanismo para monitorizar o não cumprimento dos requisitos externos fazer cumprir as práticas internas e implementar ações corretivas. As questões de não cumprimento são analisadas para encontrar as causas, com o objetivo de encontrar soluções sustentáveis.	
5	A organização toma parte em discussões com grupos regulatórios e de indústria para compreender e influenciar os requisitos externos que a afetam. Estão desenvolvidas boas práticas que asseguram a observância dos requisitos externos, com muito pequenas exceções. Existe um sistema de rastreio central aplicável a toda a organização, que permite medir e melhorar a qualidade e a efetividade do processo de monitorização do cumprimento.	

34. **<u>Providenciar governação das TI</u>**

O processo "providenciar governação das TI " satisfaz os requisitos de negócio das TI em integrar a governação TI com os objetivos da governação da organização e cumprir com as leis e regulamentos. Como avalia a maturidade deste processo na sua organização?

0	Existe uma falta de conhecimento do processo de governação TI. A organização não reconhece que seja um assunto a abordar.	
1	A abordagem da gestão é reativa, e só existe uma comunicação esporádica e inconsistente sobre o assunto. A gestão apenas tem uma indicação aproximada de como as TI contribuem para o desempenho do negócio. A gestão apenas responde reactivamente a incidentes que tenham causado alguma perda ou embaraço para a organização.	
2	As atividades de governação das TI e os indicadores de desempenho, nos quais se incluem os processos de planeamento, fornecimento e monitorização das TI, estão em desenvolvimento. Estão identificados alguns processos das TI para serem melhorados, mas são baseados em decisões individuais. A Os processos, ferramentas e métricas para medir a governação TI são limitadas e podem não estar a ser usadas na sua capacidade máxima devido à falta perícias nessa funcionalidade.	
3	Está definido e documentado um patamar para os indicadores de governação TI onde estão definidas e documentadas ligações entre as medidas de sucesso e os indicadores de desempenho. Os procedimentos são padronizados e documentados. Estão identificadas ferramentas para apoiar a supervisão da governação das TI.	
4	As responsabilidades são claras e o dono do processo está estabelecido. Os processos das TI e os processos da governação das TI estão alinhados e integrados com a estratégia do negócio e das TI. A evolução dos processos TI é baseada primariamente numa compreensão quantitativa, e é possível monitorizar e medir a observância com os procedimentos e métricas do processo. Os indicadores de desempenho sobre todas as atividades de governação são registados e rastreados levando à melhoria da organização.	
5	A implementação de políticas das TI, levam a que a organização, as pessoas e os processos se adaptem facilmente e apoiem totalmente os requisitos de governação das TI. Todos os problemas e desvios são analisados para determinar as suas causas e são rapidamente identificadas e iniciadas as ações necessárias. As TI são usadas de uma maneira extensiva, integrada e otimizada para automatizar o fluxo de trabalho e disponibiliza ferramentas para melhorar a qualidade e efetividade. São	

	usados peritos externos e aferição com outras organizações para aconselhamento. A governação das TI e a governação da organização estão estrategicamente ligadas, alavancando os recursos financeiros, humanos e tecnológicos para aumentar a vantagem competitiva da organização.	

Parte V – Redação Livre

1) Quais os cinco processos, daqueles indicados anteriormente, que considera críticos na sua organização e porquê?

2) Como avalia o estado atual das TI na defesa, como definiria o estado desejado e que linhas de ação considera mais importantes numa eventual reorganização?

Apêndice 4 - Interpretação dos dados do questionário da Avaliação da Maturidade da Gestão e Controlo dos Processos das TI

O COBIT, do ITGI, é uma moldura de apoio à governança das TI que compreende um modelo de maturidade da gestão e controlo dos processos das TI. Neste modelo são definidos 34 processos, agrupados segundo 4 domínios distintos, cuja maturidade é estabelecida por um de seis níveis possíveis.

A metodologia adotada para realizar a avaliação do estado atual das TI consiste assim na autoavaliação de cada uma das entidades referidas através deste questionário, que se baseia no modelo de maturidade do COBIT.

Face à natureza das respostas, e reconhecendo que existem alguns valores espúrios em alguns dos vetores de análise, foi criado um fator de ponderação, baseado na moda, mediana e média, que melhor represente a natureza dos dados.

Da leitura conjunta dos valores obtidos nos questionários dos processos de cada domínio, modelados na tabela 3 e resumidos nos gráficos que se seguem, com a explanação do correspondente nível de maturidade e daquele que pretendemos atingir, permitiu obter as vulnerabilidades e potencialidades do atual modelo que passaremos a elencar. Seguidamente através de uma análise SWOT pretende-se identificar as linhas de ação que conduzirão ao novo modelo a propor.

Por uma questão de comodidade na leitura, as tabelas, que originalmente deveriam estar dimensionadas de zero a cinco, foram adaptadas aos valores obtidos.

Tabela 3 – Avaliação da Maturidade da Gestão e Controlo dos Processos das TI

Fonte (Autor, 2013)

Nº	Descrição	valor	moda	mediana	media	MDN	EMGFA	Marinha	Exército	FA
Parte I – Planear e Organizar										
1	Definir um planeamento estratégico das TI	3	3	3	3,4	3	3	4	3	4
2	Definir uma arquitetura de informação	3	3	3	3,4	3	4	3	4	3
3	Determinar uma direção tecnológica	4	4	4	3,8	3	4	3	4	5
4	Definir Processos TI eorganização	3	3	3	3,4	3	4	3	4	3
5	Gerir o investimento nas TI	3	3	3,5	3,6	3	4	3	3	5
6	Comunicar a direção e os objetivos da gestão	3	3	3	3	3	3	3	2	4
7	Gerir os recursos humanos das TI	2	2	2	2,6	2	2	1	3	5
8	Gerir a qualidade	2	-	2	2,2	3	3	1	2	2
9	Avaliar e gerir os riscos dasTI	2	2	2	2,4	2	2	2	3	3
10	Gerir os projetos	4	4	4	3,6	2	3	4	4	5
Parte II – Obter e Implementar										
11	Identificar soluções automatizadas	3	4	4	3,6	3	4	3	4	4
12	Adquirir e manter aplicações de software	3	3	3	3,4	3	3	3	4	4
13	Adquirir e manter infraestruturas tecnológicas	4	4	4	4	3	5	3	4	5
14	Facilitar a operação e o uso	2	2	2	2,8	2	3	2	2	5
15	Obter recursos das TI	4	4	4	3,8	3	4	4	4	4
16	Gerir as mudanças	2	-	3	2,8	2	4	2	3	3
17	Instalar e acreditar as soluções e as mudanças	4	4	4	3,6	3	4	3	4	4
Parte III – Fornecer e Apoiar										
18	Definir e gerir níveis de serviço	3	-	3,2	3,25	4	3	2	3	4
19	Gerir os serviços a terceiros	2	-	3	2,75	2	4	2	4	3
20	Gerir desempenho e capacidade	3	-	3,2	3,25	3	4	2	3	4
21	Assegurar um serviço continuo	3	4	3,4	3,25	2	4	3	4	4
22	Assegurar os sistemas de segurança	3	4	3,6	3,25	2	4	3	5	4
23	Identificar e alocar custos	2	-	3	2,75	2	4	2	4	3
24	Educar e treinar os utilizadores	3	-	3,6	3,5	2	3	4	4	5
25	Gerir o serviço de apoio e incidentes	3	4	3,6	3,5	4	3	3	4	4
26	Gerir a configuração	2	-	3,4	3,25	2	4	2	4	5
27	Gerir problemas	3	4	3,4	3,25	2	4	3	4	4
28	Gerir dados	3	3	3,4	3,25	3	4	3	4	3
29	Gerir o ambiente físico	4	5	3,8	3,75	3	5	2	4	5
30	Gerir as operações	3	-	4	3,75	3	5	3	5	4
Parte IV – Monitorizar e Avaliar										
31	Monitorizar e avaliar o desempenho das TI	2	-	3	2,8	2	4	2	3	3
32	Monitorizar o controlo interno	3	3	3	2,8	1	3	3	4	3
33	Assegurar a observância dos requisitos externos	3	-	4	3,8	3	4	3	5	4
34	Providenciar governação das TI	3	3	3	3,4	3	4	3	4	3

1. Planear e organizar

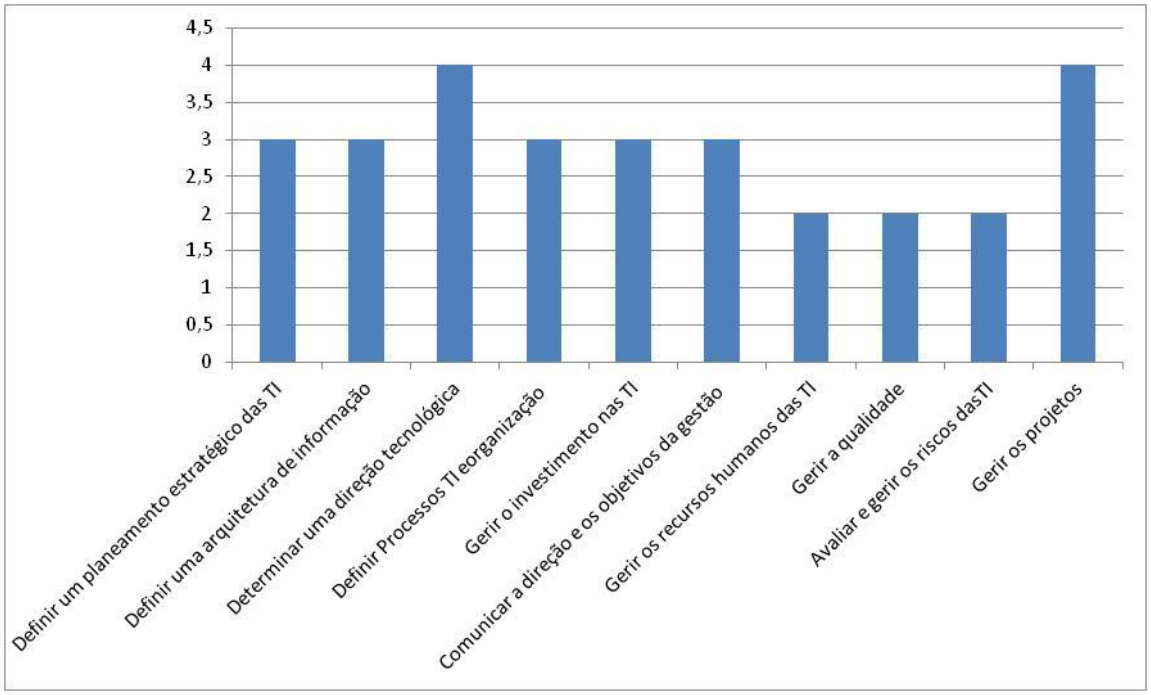


Gráfico 1 – Processos relacionados com o planeamento e organização

Fonte: (Autor, 2013)

Embora esteja definido quando e como deve ser feito o planeamento estratégico e nele estejam aclarados, de forma consistente, os riscos que a organização está disposta a correr (P), a implementação dos processos é deixada ao critério dos gestores TI (V). O planeamento estratégico não reflete, quer o valor acrescentado, quer as mudanças de tecnologia e os desenvolvimentos estratégicos da DN (V).

Estão desenvolvidas políticas básicas da arquitetura da informação, incluindo alguns requisitos estratégicos (P), mas a observância dessas políticas, padrões e ferramentas não está consistentemente implementada (V). Esta arquitetura da informação começa a estar assente em ferramentas automatizadas (P), mas ainda não reflete os requisitos de negócio (V). Os processos e regras encontram-se dependentes do *software* fornecido pelos fornecedores, não levando em consideração a informação não tradicional nos processos, organização e sistemas (V).

O planeamento tecnológico não está orientado pelos padrões e desenvolvimentos internacionais e da indústria, sendo, pelo contrário, guiado por fornecedores chave, apesar do desenvolvimento tecnológico, a longo prazo, ser consistente com as orientações da organização (V). Por outro lado, a aplicação do plano tecnológico é inconsistente, não exis-

tindo processos que analisem qual o impacto das alterações tecnológicas no negócio da DN (V). A função TI tem uma organização estabelecida, documentada e alinhada com a estratégia das TI (P), mas não é flexível e adaptativa (V). Quer as funções a ser executadas pelo pessoal das TI, quer as que competem aos utilizadores, encontram-se definidas (P). Os requisitos e perícias do pessoal das TI estão definidos e estabelecidos (P). As funções e responsabilidades das TI estão formalizadas e implementadas (P), não estando, no entanto, implementado um processo de evolução continua (V).

Estão definidos e documentados os processos para o investimento e financiamento, que cobrem as questões tecnológicas e os elementos chave do negócio, assumindo a sua aprovação um cariz formal (P). No entanto, não são usadas as boas práticas da indústria para avaliar os custos e para aumentar a eficiência dos investimentos (V). O pessoal das TI tem as perícias necessárias para desenvolver um orçamento das TI e para recomendar os investimentos nas TI apropriadas (P). As decisões de investimento não incorporam as tendências de melhoramento preço/eficiência, nem uma análise de custos e benefícios ao longo do ciclo de vida (V).

Está desenvolvido, documentado e disseminado um ambiente completo de gestão de qualidade e de controlo da informação, que inclui um quadro para as políticas, planos e procedimentos (P), mas a monitorização da sua observância é inconsistente (V). Estão padronizadas e formalizadas as técnicas que promovem a consciencialização da segurança (P). Está estabelecido um programa que define e monitoriza as atividades do sistema de gestão de qualidade dentro das TI (P), embora as suas atividades estejam focadas nos processos dos projetos TI individuais e não nos processos de toda a organização (V).

Apesar de existir avaliação do risco (P), esta é implementada à descrição dos gestores de projeto que, normalmente, apenas a aplicam a projetos de grande envergadura ou na resposta a problemas (V). Os processos de mitigação do risco começam a ser implementados, mas apenas onde estes estejam identificados (V).

Os processos de gestão dos projetos das TI e a sua metodologia estão estabelecidos e disseminados (P), mas as atividades a desenvolver após a implementação do sistema, embora definidas, não são aplicadas por todos os gestores da organização (V).

2. Obter e Implementar

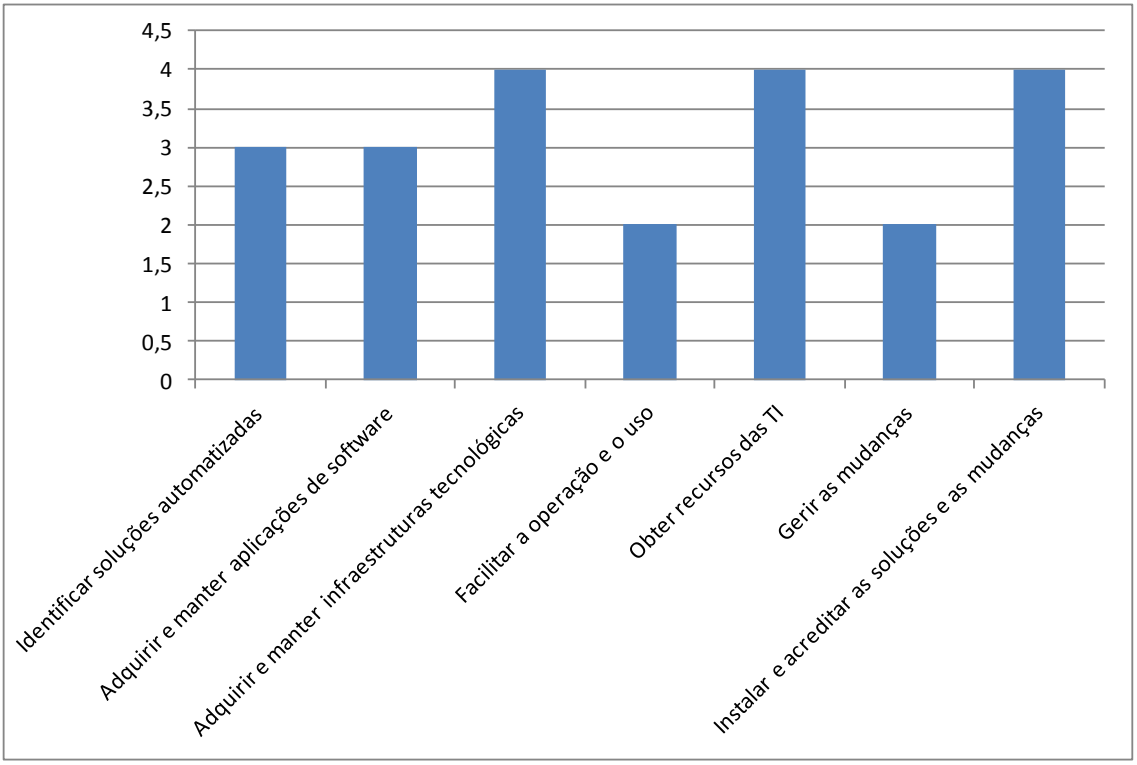


Gráfico 2 – Processos relacionados com a aquisição e implementação

Fonte: (Autor, 2013)

A determinação das soluções TI é feita por avaliação das alternativas, em função dos requisitos de negócio ou dos utilizadores, oportunidades tecnológicas, viabilidade económica e avaliação de risco (P). No entanto, apenas em alguns projetos as decisões são tomadas de forma individual pelas diversas entidades da Defesa (V). As soluções TI são aprovadas sem levar em conta tecnologias alternativas ou requisitos funcionais de negócio (V). A organização tenta, de forma consistente, aplicar processos documentados aos diferentes projetos e aplicações (P), mas as metodologias, sendo inflexíveis e de difícil aplicação a todos os casos, dá azo a que alguns passos sejam omissos (V).

O processo para adquirir e manter as infraestruturas das TI apoia as necessidades das aplicações críticas e está alinhado com a estratégia das TI e do negócio (P), mas não é consistentemente aplicado (V). Não existe uma aproximação uniforme ao desenvolvimento de procedimentos do utilizador e de operação (V). Os procedimentos e a qualidade do apoio ao utilizador variam numa escala que vai de fraca a muito boa, com muita pouca consistência e integração ao longo da organização (V). A aquisição de recursos TI está completamente integrada com os sistemas de aquisição de toda a organização (P). Está

implementado um processo de gestão da mudança formal, que inclui a caracterização, priorização, procedimentos de emergência e autorização da mudança (P), mas os processos, sendo muitas vezes ignorados, potenciam o erro e as mudanças não autorizadas (V).

3. Fornecer e apoiar

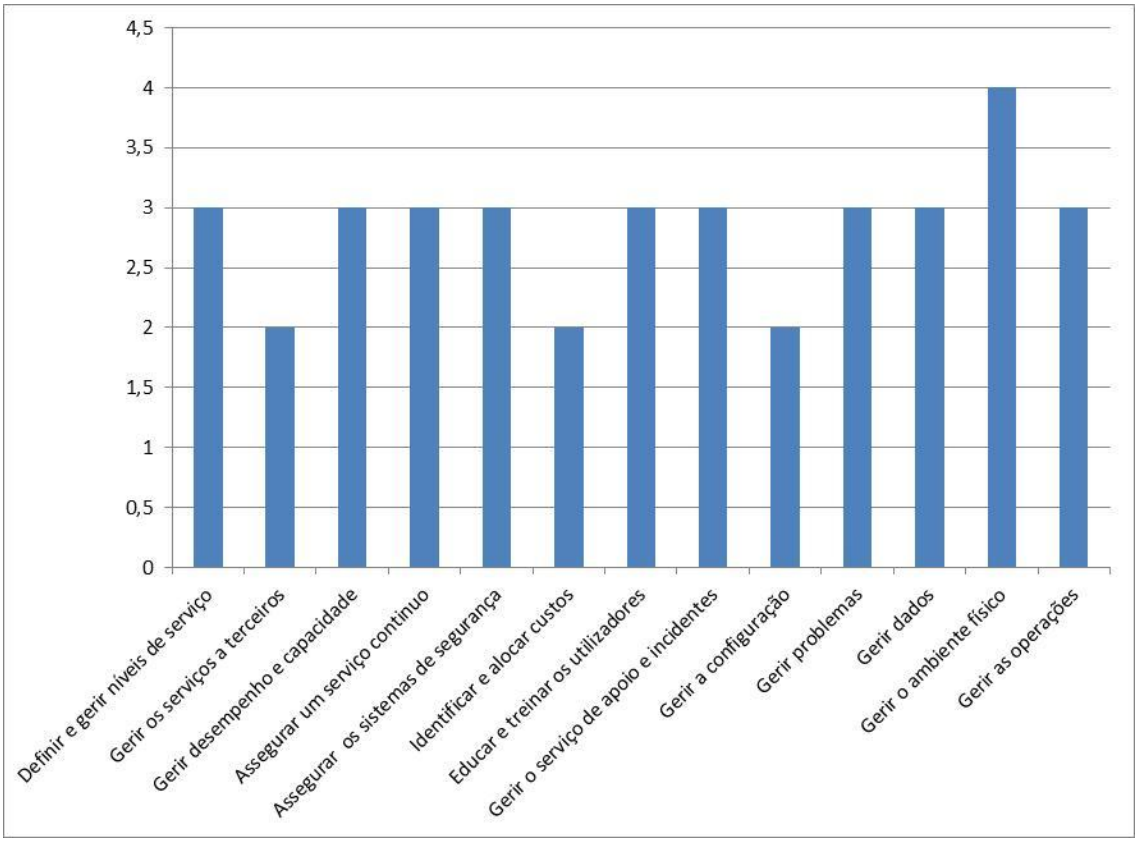


Gráfico 3 – Processos relacionados com o Fornecimento e Apoio

Fonte: (Autor, 2013)

As responsabilidades para gerir os níveis de serviço estão bem definidas (P), mas com autoridade discricionária, nem sempre contribuindo para as necessidades de negócio (V). As deficiências nos níveis de serviço estão identificadas, mas os procedimentos para as resolver são informais (V). O processo para a supervisão dos prestadores de serviços, riscos associados e entrega de serviços é informal, não apoiando os objetivos de negócio (V). Os requisitos de desempenho e de capacidades estão definidos para todo o ciclo de vida do sistema, com requisitos e métricas de avaliação (P), subsistindo, no entanto, problemas relacionados com o desempenho e com as capacidades que podem criar, nos utilizadores, algum ceticismo em relação à capacidade do serviço (V).

O plano de serviço contínuo das TI está implementado e documentado, com as responsabilidades claramente definidas e atribuídas (P). A área funcional das TI segue as

normas e tem formação suficiente para lidar com incidentes graves e com a recuperação de desastres (P). Os procedimentos de segurança são definidos e alinhados com a política de segurança da TI, com as responsabilidades atribuídas (P), mas não contêm um claro enfoque no negócio e os testes efetuados são *Ad hoc* (V). Está disponível treino na segurança das TI (P), apesar de ser informalmente programado e gerido (V). Embora haja uma consciência generalizada da necessidade de identificar os custos, a sua distribuição baseia-se na suposição do custo informal ou rudimentar (por exemplo, custos de hardware), não se identificando praticamente nenhuma ligação a medidas de criação de valor (V).

Os processos de distribuição de custos são repetitivos (V). Não existe nenhuma formação ou comunicação sobre o procedimento padrão para a identificação e distribuição de custos (V). A responsabilidade por coligir ou distribuir os custos não está atribuída (V). Os processos de treino e educação são padronizados e documentados com recursos alocados para apoiar os respetivos programas (P), mas a análise da ocorrência de problemas no treino e na educação só é realizada ocasionalmente (V).

Os procedimentos de serviço de apoio e de gestão de incidentes estão padronizados e documentados (P), mas a formação é informal e deixada à descrição do individuo (V). As questões e incidentes são controlados de forma manual e monitorizados individualmente (P), não existindo um sistema de comunicação formal (V). A resposta em tempo útil para questões e incidentes não é medida, podendo os incidentes ficar sem resolução (V). O controlo da configuração das TI está dependente do conhecimento e experiência dos técnicos, com as ferramentas que gerem a configuração a diferirem entre plataformas (V).

O conteúdo dos dados de configuração é limitado, não sendo usado por processos inter-relacionados, tais como a gestão de alterações e a gestão de problemas (V). A resolução dos problemas e os processos de agravamento estão normalizados (P), mas o registo e acompanhamento dos problemas e as suas resoluções estão descentralizados e fragmentados (V). Os desvios das normas estabelecidas ou padrões são susceptíveis de não serem detetados e a sua resolução é limitada e informal (V).

A responsabilidade pela gestão de dados encontra-se atribuída, com os procedimentos de gestão de dados formalizados e com recurso à utilização de ferramentas de backup/restauração e eliminação de equipamentos (P). A necessidade de gestão das operações de computadores é compreendida e aceite dentro da organização (P). Os recursos são alocados e existe algum treino «*on-job*» (P).

4. Monitorizar e Avaliar

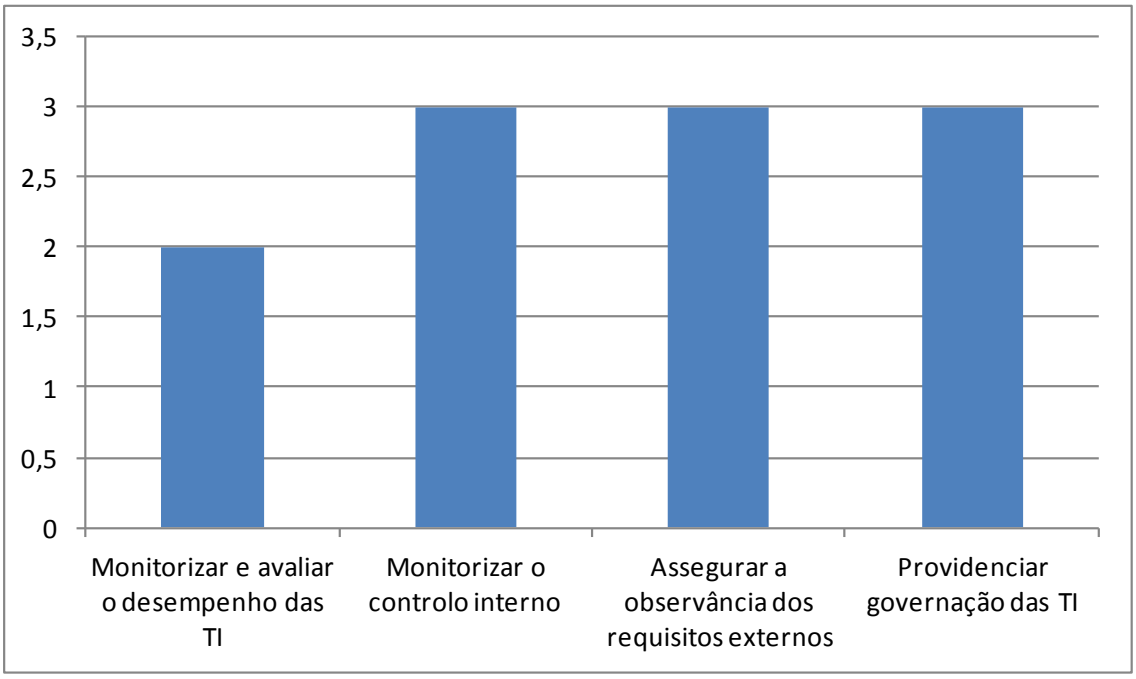


Gráfico 4 – Processos relacionados com o Monitorizar e Avaliar

Fonte: (Autor, 2013)

Estão identificadas medidas básicas a serem objeto de monitorização, com métodos e técnicas de recolha e avaliação (P), mas os processos não são adotados em toda a organização (V). A interpretação dos resultados monitorizados é baseada nas perícias de indivíduos chave (V). A gestão apoia e institui a monitorização para efeitos de controlo interno (P). São usadas políticas de avaliação de risco dos processos TI dentro de um quadro de controlo desenvolvido, especificamente, para a organização TI (P). Estão definidas políticas de mitigação e de processos de risco específico (P). São desenvolvidas politicas, planos e procedimentos, documentadas e comunicadas para assegurar a observância das obrigações contratuais, regulatórias e legais (P), embora algumas não sejam seguidas e outras possam estar desatualizadas ou a sua implementação possa ser impraticável (V). Está definido e documentado um patamar para os indicadores de governação TI, onde estão definidas e documentadas ligações entre as medidas de sucesso e os indicadores de desempenho (P). Os procedimentos estão padronizados e documentados (P). Os processos de governação podem ser monitorizados, mas não existe um mecanismo para detetar os desvios (V).

Apêndice 5 - Análise SWOT às TI da Defesa Nacional

Efetuada a análise do ambiente interno através do questionário baseado na metodologia COBIT, e deduzidas as conclusões da Auditoria às TI da DN foram identificadas as Potencialidades e as Vulnerabilidades que lhes são inerentes. De seguida procedeu-se à análise do ambiente externo através da análise da Resolução de Conselho de Ministros n.º 46/2011, de 14 de novembro e do Despacho n.º 149/2012, de 12 de junho do MDN, entre outras contribuições, de onde foram deduzidas as Oportunidade e os Desafios. Uma vez identificados os fatores procedeu-se à criação da matriz SWOT segundo a metodologia apresentada na Tabela 4.

Tabela 4 - Estrutura da matriz SWOT

Ambiente Interno / Ambiente Externo.	**P**otencialidades	**V**ulnerabilidades
Oportunidades	**(OP)** Linha de acção que emprega as **P**otencialidades para explorar as **O**portunidades	**(OV)** Linha de acção que explora **O**portunidades para corrigir as **V**ulnerabilidades
Desafios	**(AP)** Linha de acção que emprega as **P**otencialidades para evitar (ou minimizar) as **A**meaças	**(AV)** Linha de acção que corrige as **V**ulnerabilidades para superar as **A**meaças

Nas páginas seguintes apresentam-se as matrizes representando a análise efetuada nos ambientes interno e externo segundo os moldes descritos anteriormente, e das quais foram deduzidas as linhas de ação estruturais e ao nível dos processos que vão contribuir para a edificação do modelo de organizacional a propor.

Tabela 5– Matriz SWOT das TI da DN

Ambiente Interno / **Ambiente Externo**	**Potencialidades**	**Vulnerabilidades**
	O SIG em exploração nas áreas logísticas e financeiras constitui uma boa prática de racionalização de recursos. Os Ramos têm as perícias necessárias para a execução do planeamento estratégico. A arquitetura da informação reflete os requisitos estratégicos. A função TI tem uma organização estabelecida, documentada e alinhada com a estratégia das TI. Estão definidas as funções que devem ser executadas pelo pessoal das TI e utilizadores. As funções e responsabilidades das TI estão formalizadas e implementadas. Os processos para o investimento e financiamento de tecnologia estão formalizados. A área funcional das TI têm as perícias necessárias para recomendar os investimentos nas TI. Está implementado um processo de gestão de qualidade e de controlo da informação. Os processos de gestão dos projetos das TI e a sua metodologia estão estabelecidos e disseminados. A determinação das soluções TI é feita por avaliação das alternativas, em função dos requisitos de negócio ou dos utilizadores, oportunidades tecnológicas, viabilidade económica e avaliação de risco. O processo para adquirir e manter as infraestruturas das TI apoia as necessidades das aplicações críticas e está alinhado com a estratégia das TI e do negócio. A aquisição de recursos TI está completamente integrada com os sistemas de aquisição de toda a organização. Está implementado um processo de gestão da mudança formal, que inclui a caracterização, priorização, procedimentos de emergência e autorização da mudança. As responsabilidades para gerir os níveis de serviço estão bem definidas.	Inexistência de um plano estratégico de médio e longo prazo. Inexistência de um modelo de governação que defina os níveis de responsabilidade e os mecanismos de controlo. As competências atribuídas à SG não estão implementadas. Os sistemas comuns não são geridos de forma centralizada. O planeamento estratégico é deixado ao critério dos gestores. Planeamento estratégico não reflete, quer o valor acrescentado, quer as mudanças de tecnologia e os desenvolvimentos estratégicos da DN. Não está implementada a observância das políticas da arquitetura da informação. As ferramentas automatizadas não refletem os requisitos de negócio da DN O planeamento tecnológico não está orientado pelos padrões e desenvolvimentos internacionais e da indústria nem leva em conta o impacto das alterações tecnológicas. A organização da função TI não é flexível nem adaptativa Não é utilizado um método de avaliação de custos para aumentar a eficiência dos investimentos Os investimentos não incorporam uma análise custos e benefícios ao longo do ciclo de vida. A avaliação do risco é feita ao critério dos gestores e apenas é aplicável em projetos de grande envergadura. Processos de aquisição descentralizados potenciam a aquisição de ferramentas redundantes. Processo de aquisição das TI descentralizado dificulta a interoperabilidade. As soluções TI são aprovadas sem levar em conta tecnologias alternativas ou requisitos funcionais de negócio. Não existe uma aproximação uniforme ao desenvolvimento de procedimentos do utilizador e de operação Os procedimentos do apoio ao utilizador têm muita pouca

	Os requisitos de desempenho e de capacidades estão definidos para todo o ciclo de vida do sistema, com requisitos e métricas de avaliação. O plano de serviço contínuo das TI está implementado e documentado, com as responsabilidades claramente definidas e atribuídas. A área funcional das TI segue as normas e tem formação suficiente para lidar com incidentes graves e com a recuperação de desastres. Os procedimentos de segurança são definidos e alinhados com a política de segurança da TI, com as responsabilidades atribuídas. Está disponível treino na segurança das TI. Os processos de treino e educação estão padronizados e documentados com recursos alocados para apoiar os respetivos programas. Os procedimentos de serviço de apoio e de gestão de incidentes estão padronizados e documentados. As questões e incidentes são controlados de forma manual e monitorizados individualmente. A resolução dos problemas e os processos de agravamento estão normalizados. A responsabilidade pela gestão de dados encontra-se atribuída, com os procedimentos de gestão de dados formalizados e com recurso à utilização de ferramentas de backup/restauração e eliminação de equipamentos A necessidade de gestão das operações de computadores é compreendida e aceite dentro da organização. Os recursos são alocados e existe algum treino «*on-job*». Estão identificadas medidas básicas a serem objeto de monitorização, com métodos e técnicas de recolha e avaliação. A gestão apoia e institui a monitorização para efeitos de controlo interno. São usadas políticas de avaliação de risco dos processos TI dentro de um quadro de controlo desenvolvido, especificamente, para a organização TI Estão definidas políticas de mitigação e de processos de risco específico- São desenvolvidas politicas, planos e procedimentos, documentadas e comunicadas para assegurar a observância das obriga-	consistência e integração ao longo da organização. Os processos de gestão da mudança são por vezes ignorados potenciando o erro e as mudanças não autorizadas. As deficiências nos níveis de serviço estão identificadas, mas os procedimentos para as resolver são informais O processo para a supervisão dos prestadores de serviços, riscos associados e entrega de serviços é informal, não apoiando os objetivos de negócio. Os procedimentos de segurança não contêm um claro enfoque no negócio e os testes efetuados são *Ad hoc* O treino na segurança das TI é programado e gerido informalmente. A identificação do custo baseia-se no custo informal ou rudimentar (por exemplo, custos de hardware), não se identificando nenhuma ligação a medidas de criação de valor. Os processos de distribuição de custos são repetitivos. Não existe nenhuma formação ou comunicação sobre o procedimento padrão para a identificação e distribuição de custos. A responsabilidade por coligir ou distribuir os custos não está atribuída. A análise da ocorrência de problemas no treino e na educação só é realizada ocasionalmente. A formação em gestão de incidentes é informal e deixada à descrição do individuo. A resposta em tempo útil para questões e incidentes não é medida, podendo os incidentes ficar sem resolução. O controlo da configuração das TI está dependente do conhecimento e experiência dos técnicos, com as ferramentas que gerem a configuração a diferirem entre plataforma. O conteúdo dos dados de configuração é limitado, não sendo usado por processos inter-relacionados, tais como a gestão de alterações e a gestão de problemas. O registo e acompanhamento dos problemas e as suas resoluções estão descentralizados e fragmentados. Os desvios das normas estabelecidas ou padrões são susceptíveis de não serem detetados e a sua resolução é limitada e informal. A monitorização do processo da gestão da qualidade é inconsistente e está focada nos projetos TI individuais.

	ções contratuais, regulatórias e legais. Está definido e documentado um patamar para os indicadores de governação TI, onde estão definidas e documentadas ligações entre as medidas de sucesso e os indicadores de desempenho. Os procedimentos estão padronizados e documentados.	A interpretação dos resultados monitorizados é baseada nas perícias de indivíduos chave. Os processos de governação podem ser monitorizados, mas não existe um mecanismo
Oportunidades	**Linhas de ação estratégica que empregam as Potencialidades para explorar as Oportunidades**	**Linhas de ação estratégica que exploram as Oportunidades para corrigir as Vulnerabilidades**
O governo deliberou que cada ministério identifique um organismo responsável pela coordenação das áreas das TI e interlocutor único nessa área. O PGETIC estipula que cada ministério deverá elaborar a sua estratégia setorial, em cumprimento dos vetores estratégicos delineados. O PGETIC preconiza "um modelo que permita gerir de forma holística as TIem que esteja definida a autoridade e responsabilidade pela elaboração e implementação de políticas e normas que visem o alinhamento dos objetivos estratégicos das TI com os objetivos de negócio, tendo como referência três pilares: a Gestão da informação, os Sistemas TI e a Segurança da Informação. O GPTIC preconiza uma efetiva centralização da gestão das TI, ao nível da aquisição e gestão do ciclo de vida de todas as infraestruturas, comunicações e SI[13], em cada ministério. O GPTIC advoga a implementação de uma metodologia de avaliação dos projetos e investimentos em TI de modo a garantir o retorno do investimento, numa ótica custo-benefício, e a evita dar a existência de redundâncias. Potenciar a interoperabilidade na AP, privilegiando o uso de uma plataforma central que concentre as redes dos diversos ministérios. Incrementar a partilha das estruturas de direção	Potenciar as valências e perícias dos Ramos ao nível da arquitetura de informação para edificar uma arquitetura comum na DN. Disseminar as orientações e os objetivos da gestão, através informação precisa e em tempo. Estabelecer procedimentos, políticas e padrões para a aquisição e contratos de recursos das TI. Assegurar a aplicação de políticas e procedimentos na aquisição das TI. Estabelecer processos de instalação e de acreditação integrados no ciclo de vida dos sistemas e automatizados, que facilitem o treino, o teste e a operação. Avaliar o desempenho como parte de um processo de melhoria contínua. Estabelecer uma organização de gestão de incidentes e de função do serviço de apoio que assumam uma orientação de serviço ao cliente. Estabelecer regras para limitar a instalação de software não autorizado. Gerir os dados de modo a otimizar o uso da informação e que esta esteja disponível quando requerida. Gerir as operações de modo a manter a integridade dos dados e em assegurar que a infraestrutura TI pode resistir e recuperar da ocorrência de erros e falhas.	Estabelecer uma organização ao nível estratégico que garanta a governação das TI de uma forma coerente e holística e que sustente a estratégia da organização. Estabelecer uma organização ao nível executivo que monitorize a governação das TI Estabelecer uma organização responsável pela formulação e implementação da estratégia das TI Efetuar um planeamento estratégico de longo prazo, ao nível da DN que sustente e complemente a estratégia da organização e os requisitos de governação e que leve em conta a risco e o valor acrescentado. Gerir os recursos humanos das TI da DN, garantindo que os Ramos aloquem pessoal competente e motivado para criar e fornecer serviços TI Desenvolver programas de treino para todos os produtos e padrões tecnológicos antes de serem introduzidos na organização. Estabelecer um sistema de gestão de qualidade, flexível e adaptável à mudança do ambiente das TI. Produzir documentação do utilizador e operacional que assegure a satisfação dos utilizadores. Definir e gerir níveis de serviço que alinhem os serviços chave das TI com a estratégia de negócio. Otimizar o desempenho da infraestrutura TI, recursos e capacidades em resposta às necessidades de negócio. Realizar análises de tendência de modo a detetar qualquer problema de desempenho resultantes de um maior volume de

[13] Agregando a manutenção e desenvolvimento de todas as aplicações verticais do ministério.

e de comando e controlo do ministério e das FFAA. Incrementar, coordenar e explorar as sinergias entre as diferentes estruturas, numa lógica de partilha de recursos e boas práticas, que vise a racionalização do que é comum, uniformizando e padronizando procedimentos e processos, mas salvaguardando as especificidades de cada Ramo.		negócio, que permita o planeamento e a prevenção de problemas inesperados. Implementar métricas para avaliar a capacidade e o desempenho das TI afinadas por medidas de sucesso e indicadores de desempenho para todos os processos de negócios importantes Assegurar que o impacto no negócio mínimo no caso de uma interrupção do serviço TI. Garantir que não ocorrerá um desastre ou um incidente importante resultante de um único ponto de falha do fornecimento do serviço. Manter a integridade da informação e processamento das infraestruturas e minimizar o impacto das vulnerabilidades na segurança, integrando as funções de segurança com as aplicações desde o início do projeto. Elaborar um plano de segurança que incorpore os requisitos de segurança das TI, realizando aferições periódicas à segurança para avaliar a eficácia da implementação do plano. Avaliar as métricas resultantes das avaliações de segurança de modo a ajustar o plano de segurança num processo contínuo de melhoria. Assegurar que os utilizadores cumprem as politica e procedimentos de modo a usar de uma maneira efetiva e eficiente as soluções tecnológicas e as aplicações . Gerir os ativos das TI num sistema de gestão de configuração central que contenha todas as informações necessárias sobre os componentes, suas inter-relações e eventos de modo a otimizar a infraestrutura TI, recursos e capacidades.
Desafios	**Linhas de ação estratégica que empregam as Potencialidades para lidar com os desafios**	**Linhas de ação estratégica que corrige as Vulnerabilidades para lidar com os desafios**
Racionalização da utilização das tecnologias de informação (TI) na administração central, através da implementação de serviços partilhados e da redução do número de entidades TI em ministérios ou outras entidades públicas. O orçamento disponibilizado para a área das TI tem vindo a sofrer um decréscimo ao longo dos últimos 4 anos, correspondendo a uma redução de despesa com as TI de 33%, desde 2010. Acomete à Agência para a Modernidade	Edificar uma estrutura de gestão de projetos responsável pelos programas das capacidades ao longo do ciclo de vida total. Implementar uma metodologia de gestão de projetos de ciclo de vida total, que assegure o cumprimento dos prazos, a qualidade e o orçamento acordado. Implementar medidas de aferição na gestão das aquisições e dos contratos das TI mais relevantes para a DN Monitorizar e avaliar o controlo interno de modo a proteger a obtenção dos objetivos das TI, obedecendo às leis e regulamentos.	Gerir o investimento nas TI da DN de modo melhorar continuamente o custo-eficiência das TI. Implementar processos de gestão do risco automatizados em toda a organização Garantir que as decisões operacionais e de investimento de grande dimensão são feitas levando em conta o plano de gestão do risco e que são avaliadas continuamente as estratégias de mitigação do risco. Implementar uma metodologia de aquisição e implementa-

(AMA) a responsabilidade pelo "processo de avaliação prévia, obrigatório e vinculativo, dos investimentos especialmente relevantes com a aquisição de bens e serviços no âmbito das TIC.	Assegurar a observância dos requisitos externos que consiste em garantir o cumprimento das leis, regulamentos e requisitos contratuais. Implementar políticas das TI, que levem a organização, as pessoas e os processos adaptarem-se facilmente e apoiarem os requisitos de governação das TI	ção, que traduza os requisitos funcionais e de controlo em soluções automatizadas e eficientes. Implementar um mecanismo que detete e atue caso as soluções TI sejam aprovadas sem levar em conta tecnologias alternativas ou requisitos funcionais de negócio. Implementar um processo de aquisição e manutenção de aplicações de software que alinhe as aplicações disponíveis com os requisitos de negócio, em tempo e com custos razoáveis. Implementar um processo de aquisição e manutenção das infraestruturas tecnológicas que privilegie a redução do custos . Implementar processos de gestão da mudança que reflitam a monitorização do resultado e que detetem *software* não licenciado ou não autorizado. Assegurar o fornecimento de serviços TI aos Ramos assegurando a transparência no que respeita a benefícios, custos e riscos. Monitorizar os processos de aquisição e de supervisão do serviço de terceiros com base em métricas. Identificar e alocar custos de modo a assegurar a transparência e a compreensão dos custos TI, e em melhorar o custo-eficiência através do uso bem informado dos serviços TI. Identificar e alocar custos de modo a assegurar a transparência e a compreensão dos custos TI, e em melhorar o custo-eficiência através do uso bem informado dos serviços TI. Otimizar as despesas na obtenção dos recursos das TI através do acompanhamento e a avaliação dos custos dos serviços. Garantir que são disponibilizados orçamentos, recursos, instalações e instrutores suficientes para os programas de treino e educação. Estabelecer um plano a longo prazo sobre a necessidade de instalações para apoiar o ambiente de computação da organização, que inclua escolha do local, a construção, a guarda, a segurança pessoal, os sistemas mecânicos e elétricos e a proteção contra fatores ambientais. Monitorizar e avaliar o desempenho das TI no que respeita à transparência e compreensão dos custos TI, benefícios estratégias, politicas e níveis de serviço de acordo com os requisitos de governação.

Apêndice 6 – Valorização dos critérios de Avaliação

Para avaliar qual o modelo organizacional das TI que melhor se adequa à DN, torna-se necessário confrontar os modelos concetuais inferidos no capítulo 4 com os critérios de avaliação deduzidos no capítulo 3. Para o efeito, recorreu-se à ferramenta Microsoft Project Server 2010, embebida no Enterprise Project Manager, que tem como principal função a gestão de projetos. A metodologia do Microsoft Project Server 2010 assenta na hierarquização de critérios, através da análise do grau de importância com que cada um contribui para o projeto.

No âmbito deste trabalho, na primeira fase, pretendeu-se estabelecer uma hierarquização do grau de importância que cada modelo (centralizado, hibrido e descentralizado) atribuiu a cada critério (eficácia, eficiência, governação, segurança de informação e risco de transição), quando confrontados entre si, cujo resultado se apresenta na Figura 16.

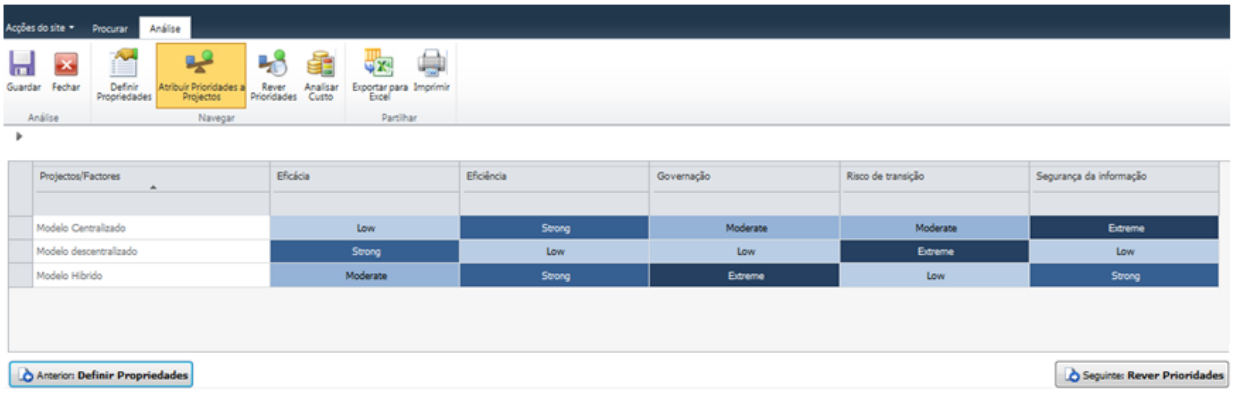


Figura 15 – Critérios vs Modelos Conceptuais

Com os valores introduzidos, o Microsoft Project Server 2010 através de calculações internas vai hierarquizar o grau de importância que cada critério para a identificação do modelo, verificando de seguida a consistência dos valores atribuídos. Da Figura 17 podemos deduzir que a governação é o critério que maior importância para a escolha do modelo organizacional das TI da DN. Para que a análise seja coerente o grau de consistência obtido terá que ser superior a 90%. Na análise efetuada, foi obtida uma consistência de 91,56%, a qual confere credibilidade aos pesos atribuídos.

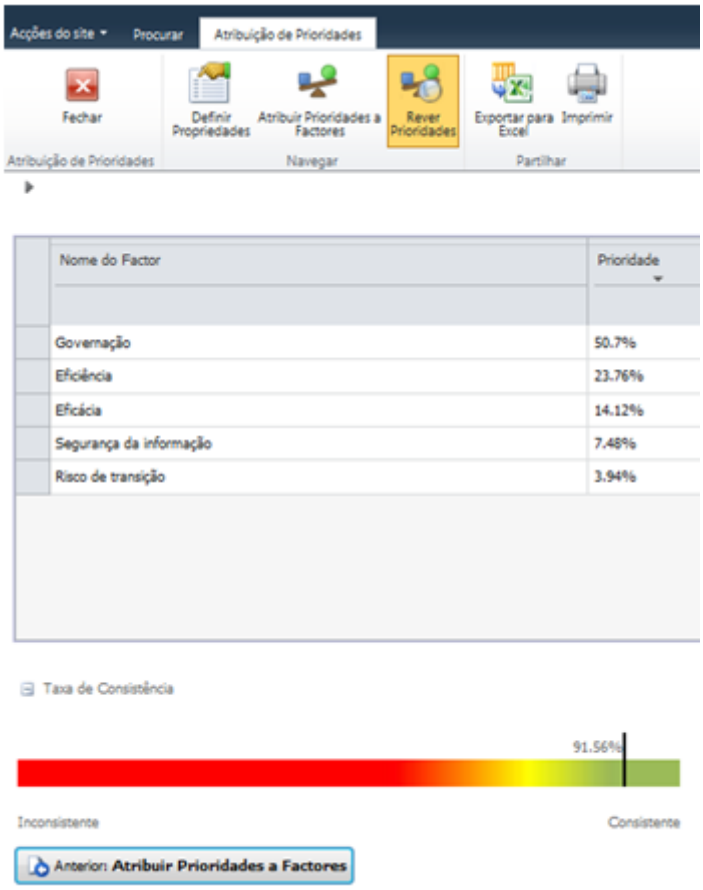
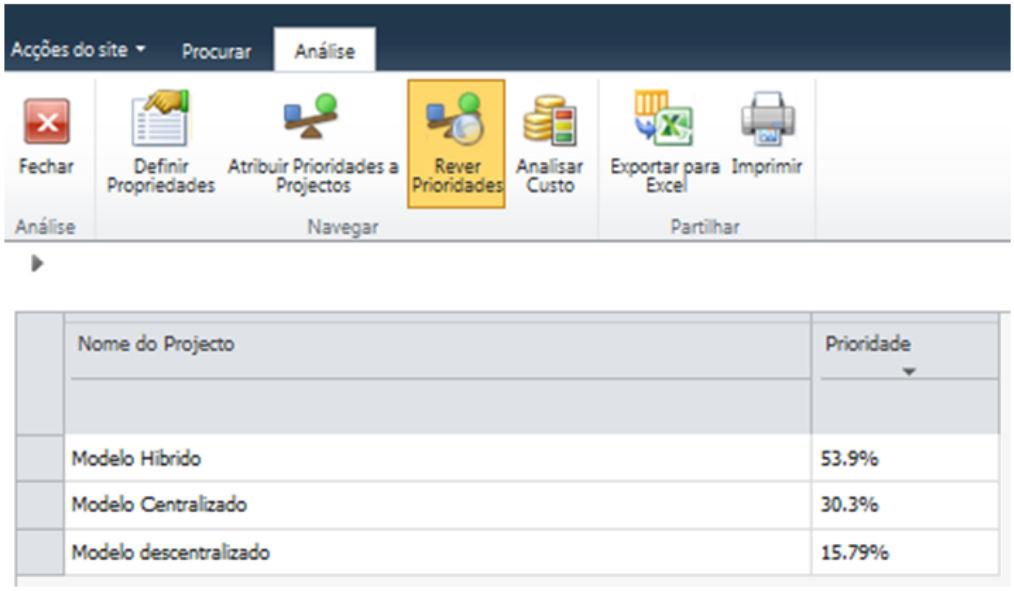


Figura 16 – Consistência das prioridades atribuídas

Do processo de comparação dos diferentes modelos sujeitos aos fatores acima enumerados decorreu a seleção do modelo híbrido como sendo aquele que melhor se adequa ao universo da Defesa.



Nome do Projecto	Prioridade
Modelo Híbrido	53.9%
Modelo Centralizado	30.3%
Modelo descentralizado	15.79%

Figura 17 – Resultados da análise do Project Server 2010

Apêndice 7 – Processos da estrutura a implementar nas TI da DN

No capítulo 4 deduziu-se a arquitetura de referência para as TI da DN. Neste apêndice pretende-se elencar em maior detalhe as funções a desempenhar por cada elemento da estrutura:

1. **Comité de Governação Estratégica**
   - Conduzir a governação das TI da Defesa em todas as suas vertentes de alto nível: Política, Estratégica, Arquitetónica, Interoperabilidade e Tecnológica.
   - Analisar e aprovar o quadro estratégico das TI na DN e o seu alinhamento com a estratégia, visão e processos de Defesa .
   - Tendo por base o quadro estratégico das TI da DN, estabelecer as políticas, princípios, orientações, prioridades, objetivos e riscos a mitigar para uma gestão eficaz e racional das TI na DN .
   - Aprovar as mudanças de direção tecnológicas e avaliar o potencial impacto no negócio da DN.
   - Aprovar o plano de segurança das TI.
   - Aprovar a arquitetura de informação que reflita todos requisitos de negócio da DN e que use as boas práticas da indústria.
   - Analisar e produzir orientações sobre o relatório de qualidade dos serviços TI e dos processos de aquisição TI, a ser submetido pelo CGExec.
   - Analisar e aprovar o relatório de contas TI.
   - Aprovar o orçamento TI da DN.

2. **Comité de Governação Executiva**

   O CGExec é apoiado pela estrutura do CIO na consecução dos trabalhos subjacentes às suas responsabilidades, listadas seguidamente:

   - Propor e implementar políticas TI, que levem a organização, as pessoas e os processos adaptarem-se facilmente e apoiarem os requisitos de governação das TI.

- Concretizar e submeter ao CGE o processo de planeamento estratégico a longo prazo, que leve em conta os objetivos estratégicos da DN e a sua eventual evolução, estabeleça considerações sobre o risco e valor acrescentado e reflita os desenvolvimentos tecnológicos.
- Disseminar as orientações e os objetivos da gestão, através de informação precisa e em tempo, que inclua os riscos associados e responsabilidades correntes e futuras, de modo a que o ambiente de controlo da informação esteja alinhado com o quadro de gestão estratégica e com a visão.
- Garantir que as decisões operacionais e de investimento de grande dimensão são feitas levando em conta o plano de gestão do risco e que são avaliadas continuamente as estratégias de mitigação do risco.
- Implementar um mecanismo que detete e atue no caso de soluções TI serem aprovadas sem que se tenha considerado tecnologias alternativas ou os próprios requisitos funcionais de negócio.
- Assegurar a aplicação de políticas e procedimentos na aquisição das TI.
- Avaliar o desempenho dos serviços das TI da DN, como parte de um processo de melhoria contínua.
- Monitorizar os processos de aquisição e de supervisão do serviço de terceiros com base em métricas.
- Desenvolver e implementar o plano de segurança das TI.
- Analisar a valorização dos custos para que estes sejam incorporados no processo do orçamento da organização.
- Monitorizar e avaliar o desempenho das TI no que respeita à transparência e compreensão dos custos TI, benefícios estratégicos, politicas e níveis de serviço de acordo com os requisitos de governação.
- Monitorizar e avaliar o controlo interno de modo a proteger a obtenção dos objetivos das TI, obedecendo às leis e regulamentos.
- Gerir os recursos humanos das TI da DN, garantindo que os Ramos aloquem pessoal competente e motivado para criar e fornecer serviços TI.
- Preparar os relatórios e documentação necessária submeter ao CGE.

3. CIO

(a) Divisão de Arquitetura Empresarial (DAE)

- Desenvolver e manter uma arquitetura de informação, robusta e responsiva e em contínua evolução, que reflita todos requisitos de negócio da DN e que use as boas práticas da indústria.
- Implementar uma metodologia de gestão de projetos de ciclo de vida total, que assegure o cumprimento dos prazos, a qualidade e o orçamento acordado.
- Implementar um processo de aquisição e manutenção de aplicações de *software* que alinhe as aplicações disponíveis com os requisitos de negócio, em tempo e com custos razoáveis.
- Implementar um processo de aquisição e manutenção das infraestruturas tecnológicas que privilegie a redução de custos através da racionalização e padronização dos componentes de infraestrutura e pelo uso da automatização.
- Implementar medidas de aferição na gestão das aquisições e dos contratos das TI mais relevantes para a DN.
- Estabelecer procedimentos, políticas e padrões para a aquisição e contratos de recursos das TI.
- Estabelecer processos de instalação e de acreditação integrados no ciclo de vida dos sistemas e automatizados, que facilitem o treino, o teste e a operação.

(b) Divisão de Desenvolvimento de Capacidades (DDC)

- Produzir um plano robusto de infraestruturas tecnológicas, orientado pelos padrões e desenvolvimentos internacionais e da indústria, que identifique as capacidades, recursos, sistemas de aplicações padronizadas, integradas e estáveis que vão ao encontro das necessidades correntes e futuras do negócio da DN.

- Implementar uma metodologia de aquisição e implementação, apoiada por bases de dados de conhecimentos internos e externos que traduza os requisitos funcionais e de controlo em soluções automatizadas e eficientes.
- Gerir o investimento nas TI da DN de modo a melhorar continuamente o custo-eficiência das TI através de serviços padronizados e integrados que satisfaçam os utilizadores, e que incorporem uma análise dos desenvolvimentos tecnológicos e uma análise de custos e benefícios do ciclo de vida.
- Produzir documentação do utilizador e operacional que assegure a satisfação dos utilizadores com ofertas de serviço, níveis de serviço, que integre a tecnologia e as aplicações nos processos de negócio e que reflita as mudanças organizacionais, operacionais e de *software.*
- Desenvolver programas de treino para todos os produtos e padrões tecnológicos antes de serem introduzidos na organização.
- Garantir que são disponibilizados orçamentos, recursos, instalações e instrutores suficientes para os programas de treino e educação.

(c) Divisão de operações e manutenção de capacidades (DOMC)

- Definir e gerir níveis de serviço que alinhem os serviços chave das TI com a estratégia de negócio.
- Assegurar o fornecimento de serviços TI aos Ramos assegurando a transparência no que respeita a benefícios, custos e riscos.
- Otimizar o desempenho da infraestrutura TI, recursos e capacidades em resposta às necessidades de negócio.
- Realizar análises de tendência de modo a detetar qualquer problema de desempenho resultantes de um maior volume de negócio, que permita o planeamento e a prevenção de problemas inesperados.
- Implementar métricas para avaliar a capacidade e o desempenho das TI afinadas por medidas de sucesso e indicadores de desempenho para todos os processos de negócios importantes.

- Assegurar que o impacto no negócio mínimo no caso de uma interrupção do serviço TI.
- Garantir que não ocorrerá um desastre ou um incidente importante resultante de um único ponto de falha do fornecimento do serviço.
- Manter a integridade da informação e processamento das infraestruturas e minimizar o impacto das vulnerabilidades na segurança, integrando as funções de segurança com as aplicações desde o início do projeto.
- Elaborar um plano de segurança que incorpore os requisitos de segurança das TI, realizando aferições periódicas à segurança para avaliar a eficácia da implementação do plano.
- Avaliar as métricas resultantes das avaliações de segurança de modo a ajustar o plano de segurança num processo contínuo de melhoria.
- Assegurar que os utilizadores cumprem as politica e procedimentos de modo a usar de uma maneira efetiva e eficiente as soluções tecnológicas e as aplicações.
- Estabelecer uma organização de gestão de incidentes e de função do serviço de apoio que assumam uma orientação de serviço ao cliente.
- Implementar processos que detetem *software* não licenciado ou não autorizado.
- Gerir os ativos das TI num sistema de gestão de configuração central que contenha todas as informações necessárias sobre os componentes, suas inter-relações e eventos de modo a otimizar a infraestrutura TI, recursos e capacidades.
- Estabelecer regras para limitar a instalação de *software* não autorizado.
- Gerir os dados de modo a otimizar o uso da informação e que esta esteja disponível quando requerida.
- Estabelecer um plano a longo prazo sobre a necessidade de instalações para apoiar o ambiente de computação da organização, que inclua escolha do local, a construção, a guarda, a segurança pessoal, os sistemas mecânicos e elétricos e a proteção contra fatores ambientais.

- Gerir as operações de modo a manter a integridade dos dados e em assegurar que a infraestrutura TI pode resistir e recuperar da ocorrência de erros e falhas.
- Assegurar a observância dos requisitos externos que consiste em garantir o cumprimento das leis, regulamentos e requisitos contratuais.

(d) Divisão de Apoio Logístico (DAL)

- Planear e executar o apoio logístico às TI.
- Preparar e conduzir os processos de contratualização TI.
- Preparar o orçamento TI e o relatório de execução orçamental.
- Identificar e alocar custos de modo a assegurar a transparência e a compreensão dos custos TI, e em melhorar o custo-eficiência através do uso bem informado dos serviços TI.
- Otimizar as despesas na obtenção dos recursos das TI através do acompanhamento e a avaliação dos custos dos serviços.

(e) Divisão de Gestão da Transição (DGT)

- Implementar processos de gestão da mudança que reflitam a monitorização do resultado.
- Estabelecer um sistema de gestão de qualidade, flexível e adaptável à mudança do ambiente das TI, que esteja integrado e implementado em todas as atividades e que contribua para um melhoramento contínuo e mensurável da qualidade dos serviços fornecidos pelas TI.
- Implementar processos de gestão do risco automatizados em toda a organização, que analisem e disseminem os riscos das TI e o seu potencial impacto nos objetivos e processos de negócio.