INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO PROMOÇÃO OFICIAL SUPERIOR
2016/2017

TII

MODELO DE GOVERNAÇÃO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO NA DEFESA NACIONAL

Ricardo José Santos Veloso
PRIMEIRO-TENENTE EN-AEL

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

MODELO DE GOVERNAÇÃO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO NA DEFESA NACIONAL

PRIMEIRO-TENENTE, EN-AEL Ricardo José Santos Veloso

Trabalho de Investigação Individual do CPOS-M 2016/2017

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

MODELO DE GOVERNAÇÃO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO NA DEFESA NACIONAL

PRIMEIRO-TENENTE, EN-AEL Ricardo José Santos Veloso

Trabalho de Investigação Individual do CPOS-M 2016/2017

Orientador: COMODORO, EMA
Rui Manuel Alves Francisco

Pedrouços 2017

Declaração de compromisso Antiplágio

Eu, **Ricardo José Santos Veloso,** declaro por minha honra que o documento intitulado **Modelo de Governação das TIC na Defesa Nacional** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **CPOS-M 2016/2017** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.
Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços**, 19** de **junho** de **2017**

Ricardo José Santos Veloso
Primeiro-Tenente

Agradecimentos

Em primeiro lugar quero agradecer à minha mulher Dóris por todo o apoio que me prestou. As longas discussões deram origem a muitos contributos. A dois foi muito mais fácil.

Em segundo lugar um especial agradecimento à minha filha Mariana, que se privou do meu tempo para fazer aquilo que mais gosta, brincar com o pai.

Aos meus pais, quero agradecer por todo o apoio que me deram, sempre disponíveis para passear com a neta sempre que o trabalho mais o exigia.

Gostaria de expressar a minha gratidão para o meu orientador, Sr. Comodoro Alves Francisco, pela sua disponibilidade, experiência, conhecimento, e sobretudo pela forma como me apoiou.

Gostaria de agradecer ao Sr. contra-almirante Gameiro Marques e ao Sr. coronel Rosa Salvado pela disponibilidade demonstrada em fornecer toda a sua experiencia obtida na Secretaria-Geral e visão para o futuro das TIC na DN.

Ao Sr. coronel Pinho Viana agradeço todos os esclarecimentos fornecidos e pela forma paciente como deu respostas às minhas questões.

Ao Sr. capitão-de-mar-e-guerra Ferreira de Sousa e ao Sr. capitão-de-fragata Penim Garcia, não podia deixar de agradecer pelo apoio prestado.

Índice

Índice de Anexos

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

O Ministério da Defesa Nacional (MDN), assim como a restante Administração Pública (AP), é uma organização complexa, composta por múltiplos organismos com competências descentralizadas na área das Tecnologias da Informação e Comunicação (TIC), que foram desenvolvidas ao longo do tempo, sem qualquer tipo de estratégia delineada.

Neste trabalho será apresentada uma proposta de modelo de governação para as TIC da Defesa Nacional, que resulta de uma análise do estado da arte da governação das TIC no MDN, nomeadamente o Sistema Integrado de Gestão da Defesa Nacional (SIGDN), de uma análise dos modelos de governação dos Ministérios da Defesa da Holanda e Alemanha e por fim uma síntese dos princípios a serem adotados pelo modelo de governação, baseados na *framework* COBIT5.

A governação das TIC na Defesa Nacional terá de implementar uma estratégia alinhada com a estratégia global para Administração Pública, assim como garantir uma racionalização e otimização dos investimentos nas Tecnologias de Informação e Comunicação específicas do Ministério.

O modelo proposto prevê a criação de dois órgãos de governação, composto por representantes de todos os organismos do MDN, de forma a garantir o alinhamento estratégico para as TIC dentro do MDN.

Palavras-chave

Governação, Ministério da Defesa, Tecnologias de Informação, SIGDN, COBIT, Sistemas de Informação.

Abstract

The Portuguese Ministry of Defence (MoD), as well as the rest of the Public Administration, is a complex organization, composed by multiple organizations with decentralized Information and Communication Technologies (ICT) skills, which have been developed over time, without any kind of outlined strategy.

This research will present an IT governance model proposal for MoD, which results on the analysis of state of the art of MoD's IT governance model, namely the Sistema Integrado de Gestão da Defesa Nacional (SIGDN), an analysis of the IT Governance models of the Netherlands and Germany MoD and finally a synthesis of the principles to be adopted by the governance model, based on the COBIT5 framework.

The MoD's IT governance model will have to implement a strategy aligned with the Public Administration general strategy, as well as to ensure the MoD's IT investments rationalization and optimization.

The proposed model stipulates the creation of two governance structures, composed by representatives from all the MDN agencies, in order to ensure the IT strategic alignment within MoD.

Keywords

Governance, Ministry of Defense, Information Technologies, SIGDN, COBIT, Information Systems.

Lista de abreviaturas, siglas e acrónimos

AMN	Autoridade Marítima Nacional
AAN	Autoridade Aeronáutica Nacional
AMA	Agência para a Modernização Administrativa
AP	Administração Pública
BoD	*Board of Directors*
CDD	Centro de Dados da Defesa
CDT	Comissão de Direção Técnica
CEGER	Centro de Gestão da Rede Informática do Governo
CIT	C*yber/Information Technology*
CISO	*Chief Information Security Officer*
COBIT	*Control Objectives for Information and Related Technologies*
CPASI	Comissão de Politicas e Auditoria do Sistema de Informação da Defesa Nacional
CPHM	Comissão Portuguesa de História Militar
CTIC	Conselho para as Tecnologias de Informação e Comunicação na Administração Pública
DGPDN	Direção-Geral de Política de Defesa Nacional
DGRDN	Direção-Geral de Recursos da Defesa Nacional
DMO	*Defense Materiel Organisation*
DN	Defesa Nacional
DSSI	Direção de Serviços dos Sistemas de Informação
EMGFA	Estado-Maior General das Forças Armadas
ERP	*Enterprise Resource Planning*
ESPAP	Entidade de Serviços Partilhados da Administração Pública
FFAA	Forças Armadas
FMoD	*Federal Ministry of Defence*
GPTIC	Grupo de Projeto para as Tecnologias de Informação e Comunicação
HFAR	Hospital das Forças Armadas
IDN	Instituto da Defesa Nacional
IASFA	Instituto de Ação Social das Forças Armadas
IESM	Instituto de Estudos Superiores Militares
IGDN	Inspeção-Geral da Defesa Nacional

ISACA	*Information Systems Audit and Control Association*
IT	*Information Technology*
LO	Lei Orgânica
MDN	Ministério da Defesa Nacional
MDH	Ministério da Defesa da Holandês
MoD	*Ministry of Defence*
QC	Questão Central
QD	Questão Derivada
PAS	Plano de Ação Setorial
PGETIC	Plano Global Estratégico para a Racionalização e Redução de Custos com as Tecnologias de Informação e de Comunicação
PJM	Policia Judiciaria Militar
QUAR	Quadro de Avaliação e Responsabilização
RCA	Reunião da Comissão de Acompanhamento
RCM	Resolução do Conselho de Ministros
SAP	*Systeme, Anwendungen und Produkte*
SASPF	*Standard Application Software Product Families*
SG	Secretaria-Geral
SI	Sistema de Informação
SICA	Sistemas de Informação e Comunicação Automatizados
SICOM	Sistema Integrado de Comunicações Militares
SIGDN	Sistema Integrado de Gestão da Defesa Nacional
STI	Superintendência das Tecnologias de Informação
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação

Introdução

O desenvolvimento dos Sistemas de Informação (SI) e Tecnologias de Informação e Comunicações (TIC), nas entidades do Ministério da Defesa Nacional (MDN), caracteriza-se pela forma autónoma e independente como tem vindo a ocorrer. Estes sistemas têm vindo a ser desenvolvidos mediante necessidades e especificidades próprias, orçamentos e recursos humanos atribuídos para garantir todo o seu ciclo de vida[1].

Em 2002 um estudo concluiu que apesar da existência de um Sistema Integrado de Comunicações Militares[2] (SICOM), as redes de dados eram autónomas e sem qualquer interligação física. Os SI/TIC não apresentavam qualquer integração e interoperabilidade entre os diferentes ramos das Forças Armadas (FFAA), o Estado-Maior-General das Forças Armadas (EMGFA) e os Serviços Centrais (GPTIC, 2012).

Segundo Gorgulho (2007), o panorama das TIC na Defesa, à data do trabalho de investigação, caracterizava-se pela existência de sistemas e serviços com características e finalidades semelhantes (como por exemplo o correio eletrónico, *intranet*, comunicações de voz), mas que funcionavam de forma isolada dentro de cada Ramo das FFAA. Foi também identificado pelo autor que a política de exploração dos recursos informacionais (TIC) na Defesa não era realizado de forma integrada.

Em 2013 um trabalho de investigação no Instituto de Estudos Superiores Militares (IESM), identificou, de entre outras, as seguintes vulnerabilidades no MDN (Seuanes, 2013):

- Inexistência de um modelo de governação que defina os níveis de responsabilidade e os mecanismos de controlo;
- As competências atribuídas à Secretaria-Geral (SG) não estão implementadas;
- Os sistemas comuns não são geridos de forma centralizada;

Face ao exposto, verificou-se a necessidade de propor um modelo de governação das TIC para o MDN, de forma transversal para o EMGFA e os três Ramos das FFAA, para todos os organismos que pertencem aos Serviços Centrais, para o Instituto de Ação Social das Forças Armadas (IASFA), para Autoridade Marítima Nacional (AMN), para a Autoridade Aeronáutica Nacional (AAN) e para Comissão Portuguesa de História Militar (CPHM), que garanta:

[1] Conceção, planeamento, especificação, desenvolvimento, instalação, exploração, manutenção e abate

[2] Sistemas de comunicações operacionais das Forças Armadas

- A satisfação das suas atuais necessidades operacionais (eficácia), através de uma maior interoperabilidade intra-ministerial, integrando sistemas e explorando transversalmente sistemas de gestão comum;
- A exploração eficiente dos recursos informacionais, nomeadamente através ganhos de sinergia entre todas as entidades, a racionalização de recursos e a redução de custos.

O objeto da investigação deste trabalho é a governação das TIC na Defesa Nacional (DN).

O modelo de governação a propor aplica-se aos SI/TIC de gestão comuns aos organismos da DN, devendo garantir a articulação com os SI/TIC de cariz operacional/militar específicos dos Ramos, os quais são governados pelos órgãos de governação respetivos.

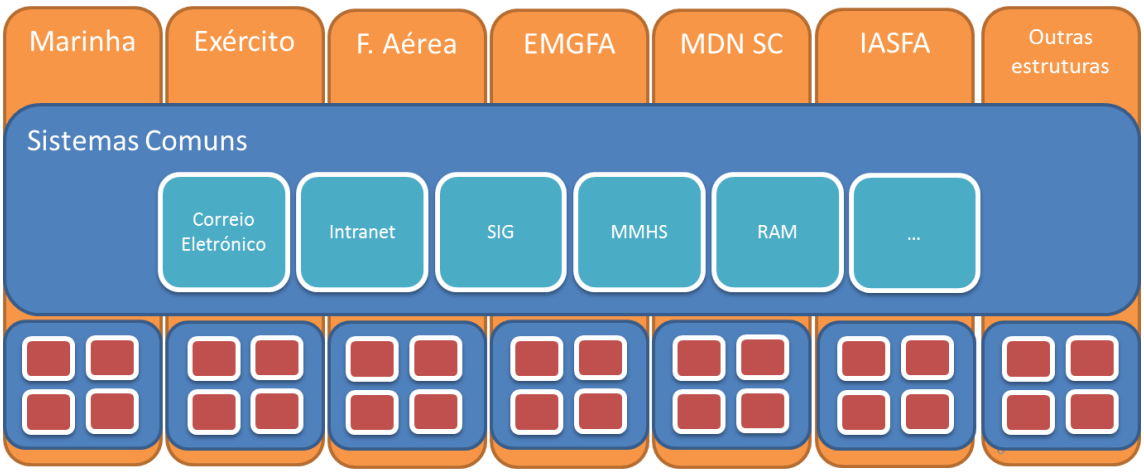


Figura 1 – Exemplos de potenciais Sistemas de Informação de gestão Comuns na DN

Fonte: (autor, 2016)

O Objetivo Geral (OG) deste trabalho de investigação consiste em propor um modelo de governação que implemente um conjunto de medidas de governação otimizada e racionalizada das TIC na DN.

Tendo como origem o OG, são propostos os seguintes Objetivos Específicos (OE):

OE1: Analisar a situação de governação das TIC na DN

OE2: Analisar modelos de governação aplicados em países selecionados (Holanda, Alemanha)

OE3: Sintetizar os princípios a serem adotados pelo modelo de governação

Tendo em conta o enunciado do tema, o objeto da investigação e os objetivos (geral e específicos) é formulada a seguinte questão central (QC):

"Que modelo de governação TIC é o mais adequado para a DN?"

A resposta à questão central será dada através da procura de respostas às seguintes questões derivadas (QD):

QD1: Como se carateriza a situação de governação TIC na DN?

QD2: Como estão implementados os modelos de governação TIC em países de referência?

QD3: Que princípios devem ser adotados pelo modelo de governação TIC?

O trabalho de investigação foi desenvolvido seguindo as "Orientações Metodológicas para a Elaboração de Trabalhos de Investigação" (IESM, 2015).

A investigação desenvolveu-se recorrendo a uma estratégia qualitativa e método indutivo, com base num Estudo de Caso, que utilizou como base de observação o modelo de governação das TIC dos Ministérios da Defesa da Holanda e Alemanha. Realizou-se posteriormente uma análise dos princípios a adotar pelo modelo de governação, com base numa *framework*[3] de referência nesta área do conhecimento, e proposto (em anexo) um modelo que melhor se adeque à realidade portuguesa.

Este trabalho está organizado em quatro capítulos, iniciando-se com uma breve introdução, seguido do desenvolvimento e finalmente as conclusões.

A seguir à presente introdução será apresentado o que constou do processo de revisão da literatura, com a descrição dos conceitos estruturantes da investigação. Neste capítulo será utilizado como método de recolha de dados a pesquisa bibliográfica.

No segundo capítulo será descrito o estado atual da governação das TIC na DN e analisado em mais detalhe a governação no projeto Sistema Integrado de Gestão da Defesa Nacional (SIGDN). Este capítulo encontra-se alinhado com o OE 1 e serão obtidas respostas à QD 1. Este capítulo terá como método de recolha de dados a pesquisa bibliográfica e entrevistas.

O capítulo seguinte encontra-se alinhado com o OE 2 e pretende analisar modelos de governação das TIC no Ministério da Defesa da Holanda e da Alemanha e tem como objetivo obter respostas à QD 2. Serão aplicados, neste capítulo, os métodos de recolha de dados a pesquisa bibliográfica e a observação de dados.

No quarto capítulo serão sintetizados os princípios a serem adotados pelo modelo de governação. Este capítulo encontra-se alinhado com o OE 3 e serão obtidas respostas à QD 3. Neste capítulo, os métodos de recolha de dados que serão aplicados são a pesquisa bibliográfica.

[3] Conjunto de conceitos e boas praticas utilizados para resolver um problema num domínio específico.

As conclusões serão compostas por um sumário das grandes linhas do procedimento metodológico, avaliação dos resultados obtidos, contributos, recomendações e identificação de linhas de investigação futuras.

No Apêndice A será apresentado o modelo de governação proposto.

1. Aspetos essenciais da Investigação

Neste capítulo será contextualizado o problema da investigação e descritos os conceitos estruturantes para a investigação.

1.1. Contexto

Em 2011 o Estado Português assume compromissos com o Fundo Monetário Internacional, Banco Central Europeu e Comissão Europeia, a fim de reduzir os custos de forma transversal na Administração Publica (AP), incluindo nas TIC. Neste sentido foi constituído o Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC), "que funciona na dependência do membro do Governo responsável pela área da modernização administrativa" (Presidência do Concelho de Ministros, 2011).

No final de 2011, o GPTIC elaborou o Plano Global Estratégico de Racionalização e Redução de Custos nas TIC, na Administração Pública (PGETIC), que pretende potenciar a eficiência e a eficácia de operação ao menor custo possível. (GPTIC, 2011).

No PGETIC foram propostas 25 medidas de racionalização das TIC de acordo com os seguintes eixos de atuação:

- Melhoria dos mecanismos de governabilidade;
- Redução de custos;
- Utilização das TIC para potenciar a mudança e a modernização administrativa;
- Implementação de soluções TIC comuns;
- Estímulo ao crescimento económico.

A Resolução do Conselho de Ministros nº 12/2012, de 07 de fevereiro determinou que todos os ministérios deverão apresentar os respetivos planos de ação sectoriais (PAS) de racionalização das TIC, identificando, com prazos e responsáveis, as iniciativas e projetos de índole sectorial, que contribuam para o referencial de redução de custos e melhoria dos serviços públicos. No final de 2012 o MDN apresentou o PAS de racionalização das TIC no MDN, no qual foram apresentadas vinte medidas de ação que se encontram alinhadas com o PGETIC, sendo a Medida 1 "Governação das TIC no MDN", que desde a sua ultima atualização, em junho de 2015, ainda se encontra com uma taxa de execução de 0% (GPTIC, 2012).

A 03 de junho de 2016, foi publicada uma Resolução do Conselho de Ministros (RCM) n.º 33/2016, de 3 de junho, que determinou a constituição do grupo de projeto denominado Conselho para as Tecnologias de Informação e Comunicação na

Administração Pública (CTIC), que funciona na dependência do Primeiro-Ministro (Diário da Republica, 2016) .

Esta RCM veio definir um novo modelo de governação para as TIC na Administração Pública (AP), aberto à sociedade e ajustado aos objetivos do Governo, abrindo portas à definição de uma estratégia transversal para as TIC (Diário da Republica, 2016).

Ao CTIC foram delegadas as seguintes competências:

a) "Apreciar e aprovar a estratégia TIC, incluindo os planos de ação dos departamentos governamentais, doravante abreviadamente designados por «Planos Setoriais TIC», tendo em conta o Programa do Governo e os objetivos do programa SIMPLEX; (Diário da Republica, 2016)"
b) "Aprovar decisões de carácter programático relacionadas com a definição e execução da estratégia TIC; (Diário da Republica, 2016)"
c) "Aprovar a definição das metas anuais e plurianuais no âmbito da estratégia TIC, e avaliar a sua execução. (Diário da Republica, 2016)"

O CTIC é a "estrutura de coordenação responsável por operacionalizar a estratégia e o plano de ação global para as TIC na AP" (Diário da Republica, 2016)".

Foram definidos os seguintes objetivos para o CTIC:

a) "Promover o estudo das TIC na AP, incluindo a análise dos sistemas de informação e das estruturas organizacionais; (Diário da Republica, 2016)"
b) "Estudar e elaborar a estratégia e o plano de ação para as TIC na AP, doravante abreviadamente designada por «estratégia TIC»; (Diário da Republica, 2016)"
c) "Implementar as medidas contidas na estratégia TIC que lhe caiba realizar diretamente; (Diário da Republica, 2016)"
d) "Acompanhar e monitorizar a implementação das medidas que fiquem a cargo de outras entidades, incluindo as medidas constantes dos planos setoriais TIC, e monitorizar a integração e o alinhamento dos planos de ação setoriais com a estratégia TIC; (Diário da Republica, 2016)"
e) "Propor as metas e objetivos anuais para a execução das iniciatias e medidas governativas, em articulação com a proposta de Lei do Orçamento do Estado, assim como as metas plurianuais de médio e longo prazo. (Diário da Republica, 2016)"

O CTIC integra na sua estrutura organizacional o Comité Técnico, que é composto pela Agência para a Modernização Administrativa (AMA), que dirige, o Centro de Gestão da Rede Informática do Governo (CEGER), a Entidade de Serviços Partilhados da Administração Pública. I.P. (ESPAP) e um Representante Ministerial de cada área do Governo; e o Conselho Consultivo.

Como consequência em 02 de março de 2017 o Conselho de Ministros aprovou a Estratégia TIC 2020 e os respetivos planos setoriais apresentados pelos CTIC (Conselho de Ministros, 2017). O MDN passou, desde esta data, a garantir um alinhamento Estratégico com estes dois documentos para a área das TIC.

1.2. **Base conceptual**

De acordo com a revisão da literatura efetuada, apresentam-se os seguintes conceitos estruturantes.

As TIC são "um conjunto de artefactos tecnológicos (…), que facilitam e aumentam as capacidades individuais e coletivas na comunicação, na recolha, no tratamento, na preservação de informação e no suporte às ações que desencadeamos em consequência das decisões que tomamos, nos diversos contextos em que nos situamos ao longo do tempo". (GPTIC, 2011)

Sobre a Gestão é possível encontrar um elevado número de definições. De acordo com Henry Fayol, gerir é prever e planear, organizar, comandar, coordenar e controlar (Murugan, 2007).

A Infraestrutura (TIC) consiste num conjunto de equipamentos e sistemas de *software* que são necessários para a operação de uma empresa ou organização (Laudon & Laudon, 2012).

O SI pode ser definido como um conjunto de componentes inter-relacionados que recebem, processam, armazenam e distribuem informações para apoiar a tomada de decisão, a coordenação e o controlo numa organização (Laudon & Laudon, 2012).

Governação das TIC consiste na determinação das regras, responsabilidades, por parte dos decisores, para garantir o correto comportamento na utilização das TIC na organização (Weill & Ross, 2013). A governação deverá garantir o alinhamento estratégico das TIC ao negócio; a gestão e manutenção das infraestruturas e serviços; e garantir a correta utilização das tecnologias.

Existe uma lista diversa de *frameworks* e normas que definem boas práticas para a Governação das TIC, contudo será utilizado como referência o *Control Objectives for*

Information and Related Technologies (COBIT), atualmente na versão 5, que foi desenvolvido com base em diversos padrões e modelos de referência, conforme apresentado na Figura 2.

O COBIT, desenvolvido pela *Information Systems Audit and Control Association* (ISACA), tem como objetivo principal disponibilizar um modelo de referência para governação e gestão das TIC. Este modelo diferencia, desde logo, a Governação da Gestão.

"A governação garante que as necessidades, as condições e as opções das Partes Interessadas (*stakeholders*) sejam avaliadas a fim de determinar objetivos da organização acordados e equilibrados; definindo a direção através da priorização e tomada de decisão; e monitorizando o desempenho e a conformidade com a direção e os objetivos estabelecidos" (ISACA, 2012).

"A gestão é responsável pelo planeamento, desenvolvimento, execução e monitorização das atividades em consonância com a direção estratégica estabelecida pelo órgão de governação a fim de atingir os objetivos da organização " (ISACA, 2012).

Face ao exposto importa concluir que enquanto a gestão controla tarefas operacionais, a governação controla a gestão.

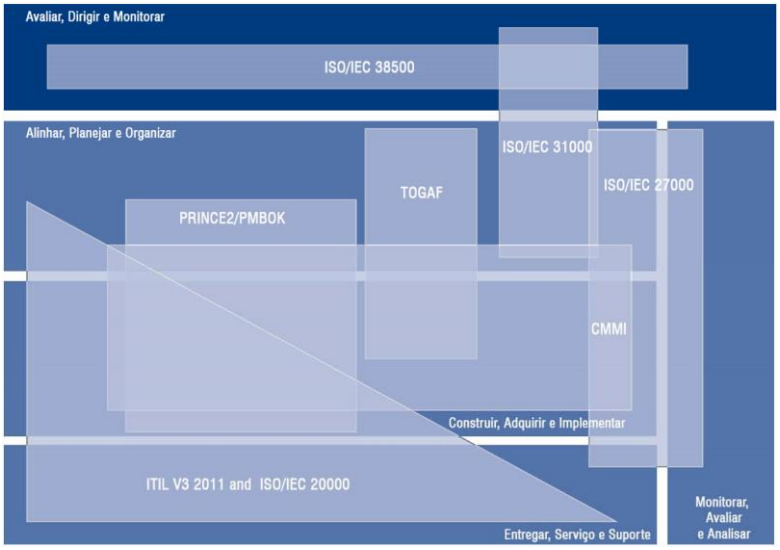


Figura 2 – Relação entre o modelo COBIT 5 e outras normas e padrões

Fonte: (ISACA, 2012)

2. Definição do atual Estado da Governação das Tecnologias de Informação no Ministério da Defesa Nacional

Neste capítulo será descrito o estado atual da governação das TIC no MDN, com especial enfoque no Sistema Integrado de Gestão da DN, face à sua dimensão, estado atual de maturação e importância no MDN.

2.1. Organização do Ministério da DN

De acordo com a sua Lei Orgânica (LO) o Ministério da Defesa Nacional é o departamento governamental que tem por missão a preparação e execução da política de DN e das FFAA.

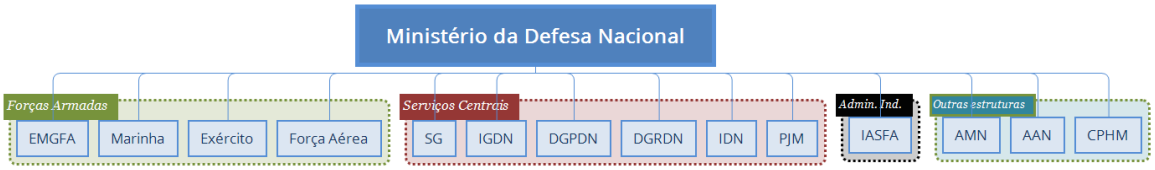


Figura 3 – Organização do MDN

Fonte: (autor, 2016)

Encontram-se na dependência direta do Estado, através do MDN, as FFAA, na qual se incluem o Estado-Maior-General das Forças Armadas e os três ramos das FFAA – Marinha, Exército e Força Aérea.

Na sua dependência, o MDN, integra também os Serviços Centrais nos quais se incluem a Secretaria-Geral (SG), a Inspeção-Geral da Defesa Nacional (IGDN), a Direção-Geral de Política de Defesa Nacional (DGPDN), a Direção-Geral de Recursos da Defesa Nacional (DGRDN), o Instituto da Defesa Nacional (IDN) e a Policia Judiciária Militar (PJM).

O IASFA é um organismo que se encontra sob a administração indireta do Estado, designadamente sob superintendência e tutela do Ministro da Defesa Nacional.

A AMN e a AAN, são organismos com competências no exercício da autoridade nos espaços marítimo e aéreo, respetivamente, sob observância das orientações definidas pelo MDN. A CPHM é um organismo que se encontra na direta dependência do MDN, com relevantes serviços prestados em prol da promoção da cultura e da história militar portuguesas (Diário da República, 1998).

Em 2014, no âmbito da Reforma "Defesa 2020", o MDN sofreu uma revisão da sua LO, passando a SG a ter a atribuição de: "Implementar (...) uma política integradora para toda a área dos sistemas de informação e tecnologias de informação e comunicação no universo da Defesa Nacional (DN), incluindo a gestão da informação para apoio à tomada

de decisão, competindo-lhe coordenar os SI/TIC e administrar os SI/TIC de natureza comum, (…)*"* (Diário da República, 2014).

Na dependência da SG encontra-se a Direção de Serviços dos Sistemas de Informação (DSSI), a quem compete, entre outros, a governação dos SI da DN (Anexo A — Competências da Direção de Serviços dos Sistemas de Informação); e o Centro de Dados da Defesa (CDD), a quem compete, entre outros, gerir as TIC de todos os organismos da defesa (Anexo B — Competências do Centro de Dados da Defesa).

A DSSI é o organismo do MDN que tem por missão "assegurar a gestão global do Sistema Integrado de Gestão da Defesa Nacional, (…)". (Salvado, s.d.)

O SIGDN é um SI de gestão comum na DN, que se encontra em exploração quer pelos Serviços Centrais do MDN, quer pelas FFAA.

2.2. **Sistema Integrado de Gestão da Defesa Nacional**

O SIGDN é um sistema *Enterprise Resource Planning*[4] (ERP), cujas caraterísticas visavam estabelecer procedimentos normalizados e possibilitar o exercício das atividades no âmbito do planeamento e gestão dos recursos financeiros e orçamentais, logísticos e humanos, no MDN, de forma a maximizar a sua eficiência e eficácia.

2.2.1. Enquadramento

O projeto que deu origem ao SIGDN iniciou-se em 2004, após um despacho do Ministro de Estado e da Defesa Nacional, que em 2002 determinou a uniformização das plataformas de gestão financeira das FFAA e Serviços Centrais do MDN. (Silva, 2011).

Dada a dimensão e transversalidade do projeto foi considerado fundamental definir um modelo de governação para envolver as diferentes entidades do MDN no processo de decisão relacionado com o desenvolvimento e exploração do sistema, e efetuar uma gestão centralizada e coordenada de defesa (Inspeção-Geral da Defesa Nacional, 2016). Para isso foi criada uma entidade gestora para a área dos SI/TIC no MDN, que atualmente está atribuída a incumbência à DSSI e que se encontra na dependência da Secretaria-Geral, conforme apresentado na Figura 4.

[4] Sistema de informação que integra os dados e os processos de negócio (finanças, contabilidade, recursos humanos, fabricação, marketing, vendas, compras) de uma organização num único sistema. (Laudon & Laudon, 2012, p.81)

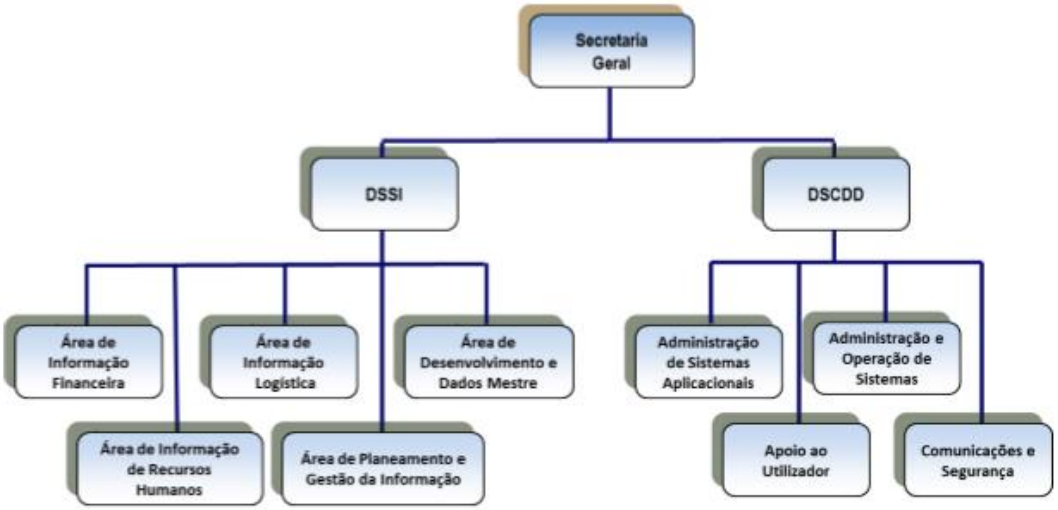


Figura 4 – Organização SIGDN da Secretaria-Geral do MDN

Fonte: (Salvado, s.d.)

2.2.2. Organização

As organizações hierárquicas são compostas por diferentes níveis, do ponto de vista funcional e do ponto de vista do tipo de decisão, conforme apresentado na Figura 5.

No nível da gestão sénior as decisões são caracterizadas como decisões estratégicas de longo prazo. A este nível são definidos os objetivos, missão e direção do negócio da organização e analisado o seu desempenho financeiro.

No nível de gestão intermédia executam-se os planos e os programas, que permitam atingir o cumprimento dos objetivos estratégicos definidos pela gestão sénior.

A gestão operacional está focada nas atividades diárias e na forma com as decisões do nível intermédio são cumpridas (Laudon & Laudon, 2012).

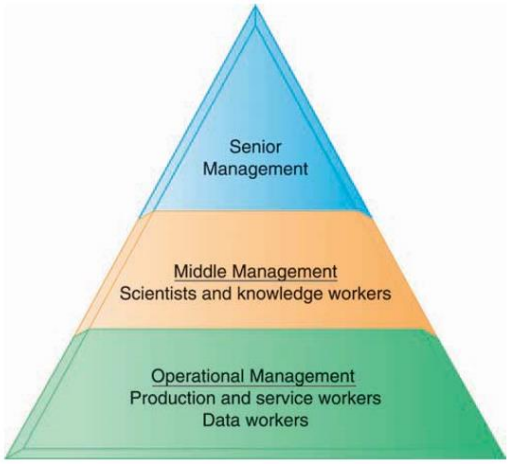


Figura 5 –Níveis das organizações

Fonte: (Laudon & Laudon, 2012)

A estrutura de coordenação do SIGDN é uma estrutura hierárquica, composta pelos diferentes níveis organizacionais e com diferentes níveis de decisão. Na Figura 6 apresenta-se a estrutura de coordenação geral do SIGDN.

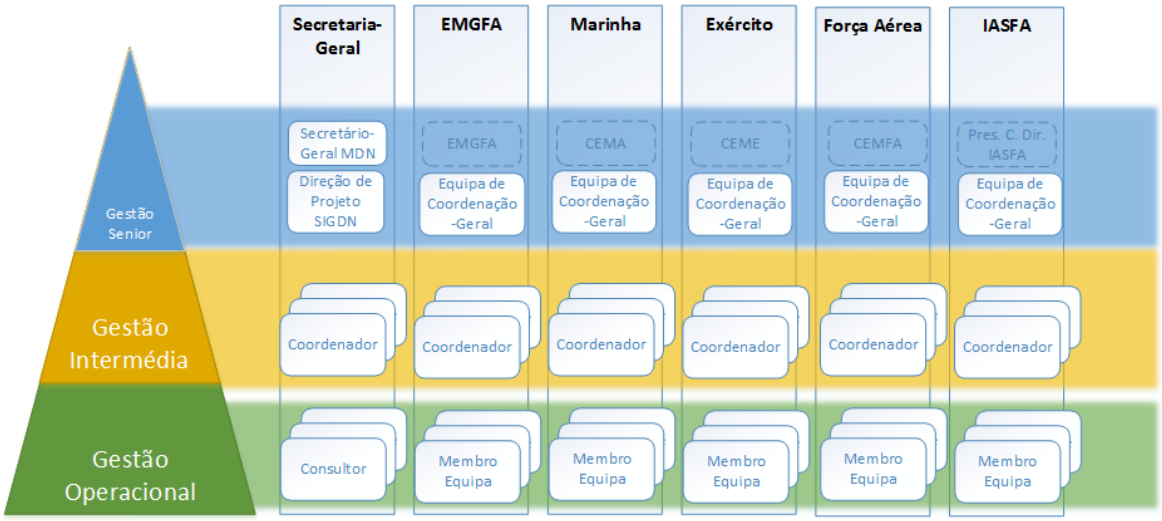


Figura 6 – Estrutura de coordenação do SIGDN

Fonte: (autor, 2017)

Na Secretaria-Geral, ao nível de gestão de topo, o *Sponsor* [5] do projeto é o Secretário-Geral e a Direção do SIGDN é composta pelo Secretário-Geral Adjunto (diretor) e pelo Diretor da DSSI (diretor adjunto), Diretor do CDD e por um representante externo da empresa subcontratada pela Secretaria-Geral para desenvolvimento e manutenção do SIGDN.

A este nível estão definidos três níveis de decisão:

- A Comissão de Políticas e Auditoria do Sistema de Informação da Defesa Nacional (CPASI);
- A Comissão de Acompanhamento do SIG;
- *O steering committee*[6].

A CPASI destina-se a elaborar e propor orientações para a integração dos SI/TIC da DN. É dirigida pelo Secretário-Geral do MDN e reúne com representantes do EMGFA e dos Ramos. Esta comissão está suspensa desde 2009 (Ministério da Defesa Nacional, 2013).

[5] Indivíduo, ou grupo, dentro da organização que desenvolve o projeto, que assegura a atribuição de recursos financeiros para o projeto (Miguel, 2010) .

[6] Grupo de planeamento estratégico de uma organização, responsável pelo desenvolvimento do plano estratégico e pela aprovação e definição da necessidade de criação de novos sistemas (Laudon & Laudon, 2012).

Tabela 1 – Reuniões de Coordenação SIGDN

Nivel Organiz.	Reuniões	Participantes	Periodicidade
Sénior	CPASI	Secretário-Geral, Secretário-Geral Adjunto, Representante do CEMGFA e dos Ramos	Não definida
	Steering	Secretário-Geral, Secretário-Geral Adjunto, Dir. DSSI, Dir. CDD, Representante(s) Empresa(s), Representantes das àreas Funcionais do SIGDN	Mensal
	Comissão de Acompanhamento	Secretário-Geral Adjunto, Dir. DSSI, Dir. CDD, Representante(s) Empresa(s), Representante do CEMGFA, dos Ramos e IASFA, Representantes das àreas Funcionais do SIGDN	Mensal
Intermédia	Auditorias Externas	Coordenadores da àrea Funcional do SIGDN	Não definida
	Planeamento	Coordenadores da àrea Funcional do SIGDN	Não definida

Fonte: (Pinho, 2017)

A Comissão de Acompanhamento (CA) do SIGDN, constituída pelos participantes descritos na Tabela 1, é o orgão consultivo para a direção e controlo do SIGDN, ao qual compete:

- "Monitorizar a execução dos projetos em tempo, custo e qualidade garantindo o seu alinhamento com os objetivos inicialmente definidos;"
- "Assegurar o enquadramento do programa com os objetivos estratégicos da organização;"
- "Garantir que o projeto tem recursos necessários;"
- "Validar cada uma das fases do projeto;"

A CA é presidida pelo Secretário-Geral Adjunto (Diretor do SIGDN) e reúne com representantes de todas as entidades que utilizam o SIGDN (Coordenadores do SIGDN), assim como a Direção Executiva do SIGDN, no qual se incluem o Dir. DSSI (Diretor-Adjunto) e coordenadores técnicos das Áreas Funcionais do SIGDN (Ministério da Defesa Nacional, 2013).

O *Steering Committee* é o orgão responsável pela validação da execução dos contratos externos para o desenvolvimento e manutenção do SIGDN. A reuniões são lideradas pelo Secretário-Geral, e são compostas pela Direção do Programa ao nível do MDN e por representantes das empresas contratadas para o efeito. As reuniões servem essencialmente para a coordenação entre a SG e a empresa (Ministério da Defesa Nacional, 2013).

Adicionalmente, no âmbito da DSSI (gestão intermédia), estão definidos dois níveis de decisão:

- Auditorias Externas;
- Reuniões de Planeamento.

As Auditorias Externas realizam-se sempre que é identificada, pelas entidades responsáveis, a necessidade de validar os procedimentos adotados ou os resultados apresentados. Estas auditorias são realizadas pela IGDN desde 2009.

As reuniões de planeamento são realizadas em conjunto com os coordenadores internos e elementos-chave do SIGDN. São realizadas atividades de planeamento das actividades e relatórios mensais. A reuniões são realizadas com os coordenadores das restantes entidades, sempre que surge a necessidade de serem tomadas decisões no âmbito das Áreas Funcionais do SIGDN, nomeadamente na definição de especificações técnicas de novos processos e nos testes finais de aceitação das soluções desenvolvidas.

2.2.3. Planeamento

O planeamento das Atividades do SIGDN, a médio prazo ("*Roadmap* para os SI/TIC"), estabelece objetivos estratégicos com uma validade de cinco anos, alinhados com a Lei de Programação Militar, estando prevista a sua revisão a cada três anos (Ministério da Defesa Nacional, 2013).

A avaliação da concretização dos objetivos é realizada através da definição de metas estabelecidas no documento Quadro de Avaliação e Responsabilização (QUAR). Este documento, de caráter anual, estabelece (entre outros):

- "Os objetivos estratégicos plurianuais determinados superiormente;"
- "Os objetivos anualmente fixados e, em regra hierarquizados;"
- "Os indicadores de desempenho e respetivas fontes de verificação;"
- "O grau de realização de resultados obtidos na prossecução de objetivos;"
- "A identificação dos desvios e, sinteticamente, as respetivas causas;"
- "A avaliação final do desempenho do serviços;"

O Plano de Atividades a curto prazo, aprovado anualmente, define (entre outros):

- "Missão, Visão e Competências da Unidade Orgânica;"
- "Alinhamento dos Objetivos da estrutura orgânica com a SG;"
- "Quadro de Objetivos e de Indicadores;"
- "Mapa de pessoal proposto;"
- "Quadro Atividades-colaborador;"
- "Fichas de Formação;"

O plano de Atividades é complementado com um plano de projeto, que define as tarefas a curto prazo no âmbito do programa SIGDN, e está alinhado com o QUAR. É desta forma que todas as atividades são controladas de forma contínua.

2.2.4. Controlo

Decorrente das atividades de controlo e gestão do SIGDN são elaborados e mantidos atualizados os seguintes documentos:

- Controlo de Pontos em Aberto – lista de problemas, necessidades de correção ou melhoramento, que são identificados, tratados, avaliados, validados e planeados, no âmbito das reuniões de *steering*, para futuro desenvolvimento.
- Relatórios de Atividades - relatórios mensais que identificam a taxa de execução das tarefas, permitindo desta forma alimentar os indicadores de gestão do SIGDN.
- Gestão de Riscos, Controlo de Qualidade e Gestão da Mudança – A gestão de riscos é realizado em sede da reuniões de *steering* e identifica uma lista de riscos, a sua criticidade e as repetivas medidas de mitigação ou planos de contingência. A gestão da qualidade é realizado através de um plano que estabelece os objetivos de qualidade e respetivas medidas a tomar. A gestão da mudança é concretizada através de ações de formação que visam preparar os utilizadores do SIGDN para a entrada de novos processos e soluções tecnológicas.

2.2.5. Formação

A formação realizada no âmbito do SIGDN tem várias vertentes, realizando-se para isso as seguintes atividades:

- Formação consultores internos – formação especifica em modulos SAP[7], complementado com *on-job training*[8], realizada pelos consultores internos menos experientes;
- *Workshops* funcionais – ações de formação ministradas aos utilizadores finais e elementos-chave, com o objetivo de demonstrar novas funcionalidades do sistema;
- Formação de formadores e preparação de manuais – formação ministrada aos formadores dos Ramos das FFAA, com o objetivo de integrar novos módulos nas suas estruturas de formação;
- Formação de utilizadores finais – Formação especifica das funcionaildades do sistema (processos SAP) aos utilizadores finais.

2.2.6. Restantes SI

Na SG existem atualmente outros projetos em desenvolvimento, fora do âmbito do SIGDN, a saber, Federação de Identidades, Federação do *Service Desk*[9], Rede de Bibliotecas, Portal RHV e EDOCLINK, estando a sua gestão a cargo do CDD (Salvado, 2017). Estes são os projetos que dada a sua aplicabilidade de forma transversal no MDN estão a ser geridos pela SG.

Desde 2013 as Reuniões da Comissão de Acompanhamento (RCA), passaram a incluir outros projetos para além do SIGDN, nomeadamente os acima referidos. Desta forma a SG otimizou a CA, passando esta a coordenar nas suas reuniões os vários projetos desenvolvidos na SG (Francisco, 2017) .

2.3. **Síntese Conclusiva**

O MDN desde 2004, quando iniciou o Projeto SIGDN, implementou uma organização que tinha como objetivo garantir o desenvolvimento de um SI que servisse de forma transversal as diversas entidades do MDN. Esta organização desenvolveu-se até consolidar um modelo de governação.

Nos últimos quatro anos, iniciaram-se novos projetos, que se encontram fora do âmbito do SIGDN e que têm como objetivo dotar as entidades do estado da exploração de novos serviços de interesse comum. A SG decidiu utilizar a organização do SIGDN, nomeadamente as reuniões da Comissão de Acompanhamento, para desenvolver atividades de gestão dos projetos.

[7] *Systeme, Anwendungen und Produkte* – Software de gestão de empresas
[8] Forma de treino realizado no local de trabalho, através da observação e execução de tarefas.
[9] O *Service Desk* é uma função primária de apoio centralizado ao utilizador no âmbito das TIC

Desta forma é possível responder à QD1, caraterizando o SIGDN como único SI que foi desenvolvido recorrendo a um modelo de governação. Os restantes SI/TIC de gestão comum da DN não estão a ser geridos, desenvolvidos, nem explorados no âmbito de um modelo de governação.

3. Modelos de governação de Tecnologias de Informação e Comunicação

Neste capítulo vão analisar-se os modelos de governação da Defesa da Holanda e da Alemanha. Estes países caraterizam-se por uma governação das TIC da Defesa centralizada nos respetivos Ministérios da Defesa.

3.1. Holanda

O Ministério da Defesa da Holandês (MDH) compreende o *Central Staff*, que elabora a politica da Defesa, os quatro serviços das Forças Armadas, que garantem a prontidão do pessoal e do material militar, o *Support Command* e o *Defense Materiel Organisation* (DMO), que fornece produtos e serviços. O *Minister of Defence* é responsável máximo da Organização. O *Secretary-General* é responsável pelas funções de liderança da componente civil. O *Chief of Defence* é responsável pela preparação e execução das operações realizadas pelos serviços das forças armadas (Government of the Netherlands, 2017).

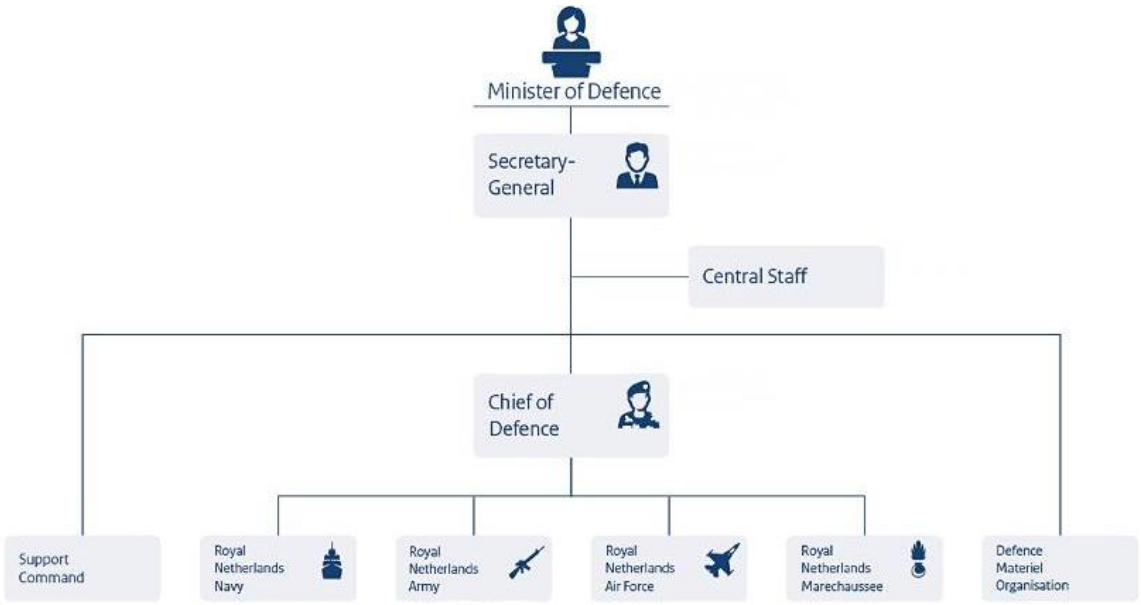


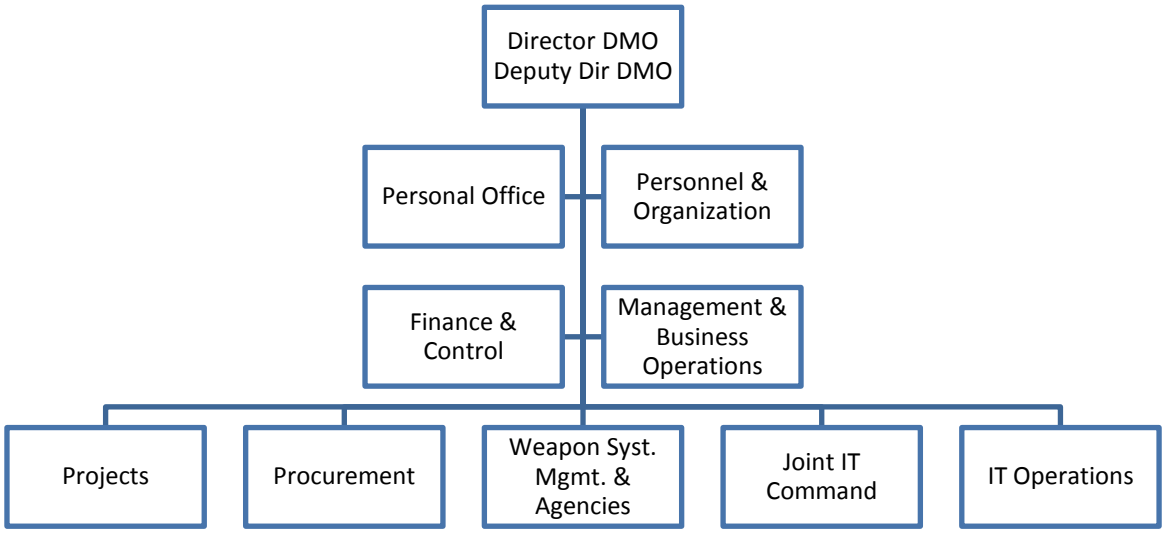
Figura 7 – Organização do Ministério da Defesa Holandês

Fonte: (Government of the Netherlands, 2017)

O MDH centralizou as TIC no DMO, atribuindo aos comandos operacionais (serviços) competências limitadas ao nível das TIC, apenas as necessárias para o suporte básico diário ao utilizador e suporte em combate.

Este organismo tem três principais atividades: Projetos e Compras; Sistemas de Armas e Agências; Marketing e Venda. No final de 2016 tinha em curso cerca de 273 projetos na área das TIC, orçamentados num total de mil milhões de euros.

Os recursos humanos no DMO são aproximadamente 4100 pessoas, composto por um quadro de civis e militares.



.

Figura 8 – Organização do DMO

Fonte: adaptado pelo autor (Lambrichs, 2016)

O MDH tem implementado um modelo de governação baseado num modelo *Demand-CIO-Supply*, conforme apresentado na Figura 9.

Este modelo é caracterizado por separar os organismos que gerem as necessidades (*Demand*) daqueles que fornecem (*Supply*) os serviços TIC.

De acordo com Cecere, et al. este modelo apresenta as vantagens de um fornecimento flexível, uma especialização e uma melhor gestão dos vários fornecedores de serviços, contudo apresenta as desvantagens de reduzida responsabilização e maior sobrecarga dos fornecedores dos serviços (Cecere et al., 2008).

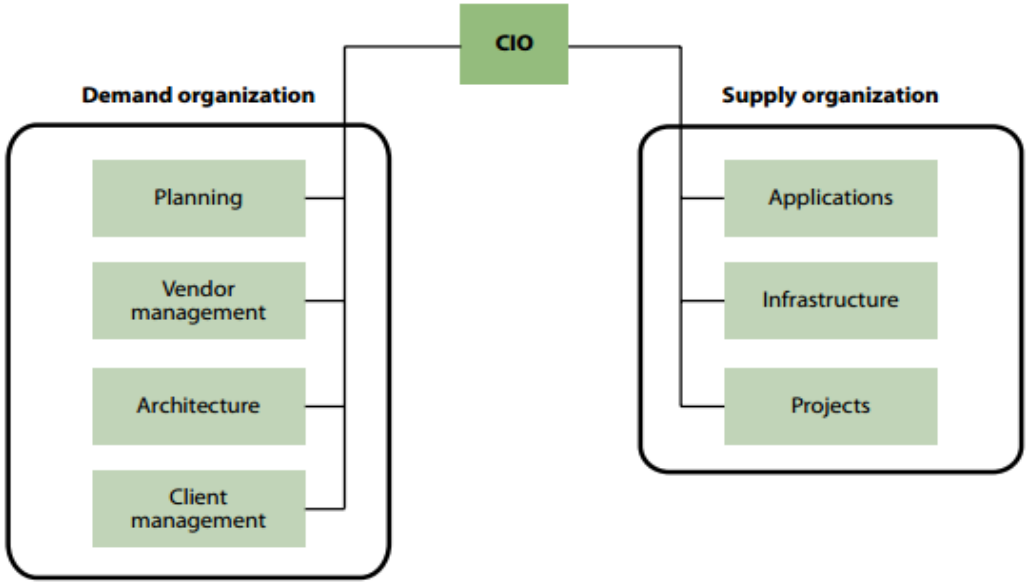


Figura 9 – Organograma tipo de uma Organização *Demand-CIO-Supply*

Fonte: (Cecere et al., 2008)

No MDH o responsável pelas necessidades é o *Defence Staff* (Diretor de Planos, em nome do Chefe de Defesa), o CIO[10] é o *Principal Directorate of Business Management* e o responsável pelo fornecimento é a DMO (*Joint IT Command*). As três organizações reúnem-se no *IT Governance Board* e presidente é o *Deputy Secretary-General*.

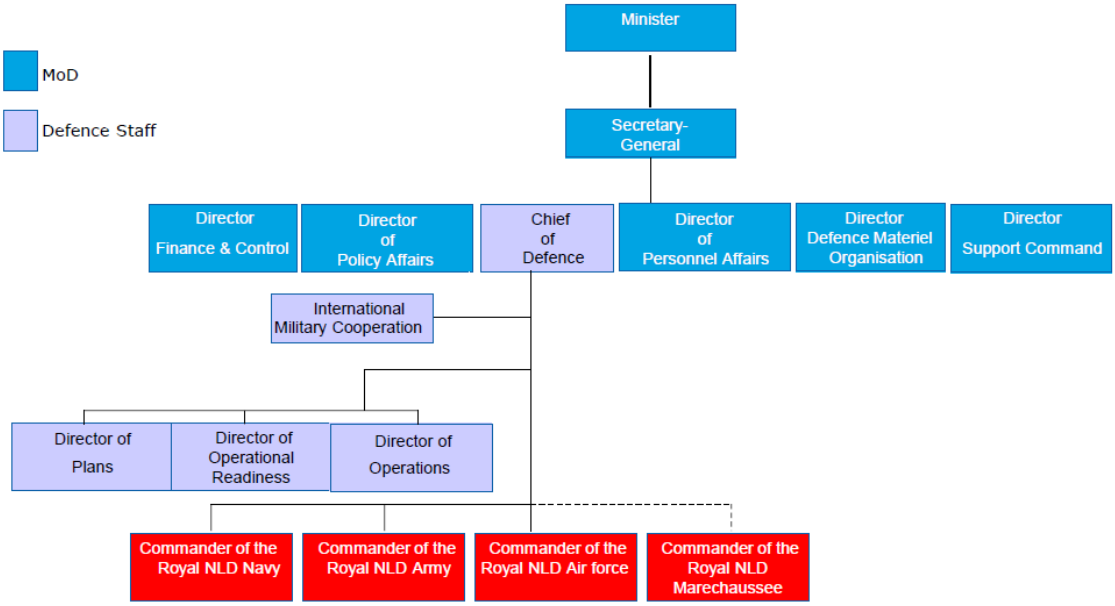


Figura 10 – Organograma do Ministério da Defesa Holandês

Fonte: (Ministry of Defense, 2017)

O *IT Governance Board*, é constituído pelo *Director of Plans*, *Principal Director of Business Management*, vice-Diretor do *DMO*, Diretor do *Joint IT Command*, vice-Diretor do *Finance and Control*, e os Vice-Chefe dos Serviços. O presidente deste Conselho é o *Deputy Secretary-General*. As decisões tomadas neste Conselho são posteriormente informadas ao *Council*.

O *IT Governance Board* tem como tarefas, ao nível da governação das TIC, a determinação das responsabilidades da governação, definição da visão e estratégia das TIC, definição da *enterprise architecture*[11], avaliação dos projetos estratégicos, gestão do portfólio de projetos e riscos. Todas as decisões estratégicas no âmbito das TIC são realizadas neste órgão de governação.

[10] O *Chief Information Officer* é o nome do cargo atribuído ao responsável máximo das TIC de uma organização/empresa.

[11] *Enterprise Architecture* aplica princípios e práticas de arquitetura para orientar as organizações através do negócio, informações, processos e mudanças necessárias a tecnologia para executar as suas estratégias (The Federation of Enterprise Architecture Professional Organizations, s.d.)

O CIO é responsável pelos regulamentos e normas, pelo estudo e avaliação de diferentes planos, nomeadamente o *Defence IT Plan*. Presta também a assessoria ao MDH no *Council*.

O *Council* é constituído pelo *Secretary-General*, que preside este conselho, *Director of Policy Affairs, Chief of Defense, Director of Finance & Control*.

O Plano Estratégico das TIC é um plano definido pelo MDH, a cada dois anos, que está incluído no processo de planeamento da Defesa. Este plano estratégico descreve a tradução dos requisitos do negócio para os requisitos TIC. Os requisitos são então traduzidos em projetos e geridos no âmbito de uma gestão de Portfólio[12]. Os projetos são priorizados e selecionados os que mais contribuem para os objetivos estabelecidos.

Face à sua relevância, os grandes projetos são controlados por uma *steering board*. A avaliação e monitorização dos projetos é da responsabilidade do *Director of Plans*, que é informado pelo DMO. Este processo realiza-se duas vezes por ano e como resultado são realizados os ajustes necessários aos projetos.

3.2. **Alemanha**

O *Federal Ministry of Defence* (FMoD) da Alemanha, sofreu uma restruturação em 2012, que visava a criação de órgãos transversais a toda a estrutura civil e militar, com o objetivo de otimizar recursos humanos e materiais, deixando para cada ramo específico o comando de decisão e controlo para aspetos mais operacionais (Maizière, 2013).

Em 2015, o Ministro da Defesa Alemão determinou a criação de um grupo de trabalho para desenvolver um conceito para a criação de um novo organismo, o *Directorate-General for Cyber/IT (CIT)***,** responsável pelas áreas *cyber*[13] e TIC (Bundesministerium der Verteidigung, 2016). Esta nova Direção-Geral foi criada em 2016 e prevê-se que esteja com a sua estrutura completa no final do primeiro semestre de 2017 (Bundesministerium der Verteidigung, 2016).

O Diretor-Geral CIT encontra-se na dependência direta do Secretário de Estado e é o CIO do FMoD, sendo ele responsável por todos os assuntos relacionados com *cyber/IT*, conforme apresentado na Figura 11. Com esta organização, pretendeu-se garantir que a modernização das CIT, bem como o uso, operação e proteção das TIC do FMoD são

[12] Gestão de portfólio é uma coleção de projetos ou programas e outros trabalhos que são agrupados para atender os objetivos estratégicos (Project Management Institute, 2013).

[13] "Espaço virtual é o novo meio de comunicação que surge da interconexão mundial dos computadores" (Lévy, 1999)

garantidos por uma única entidade, retirando essa competência das restantes Direções-Gerais (Bundesministerium der Verteidigung, 2016).

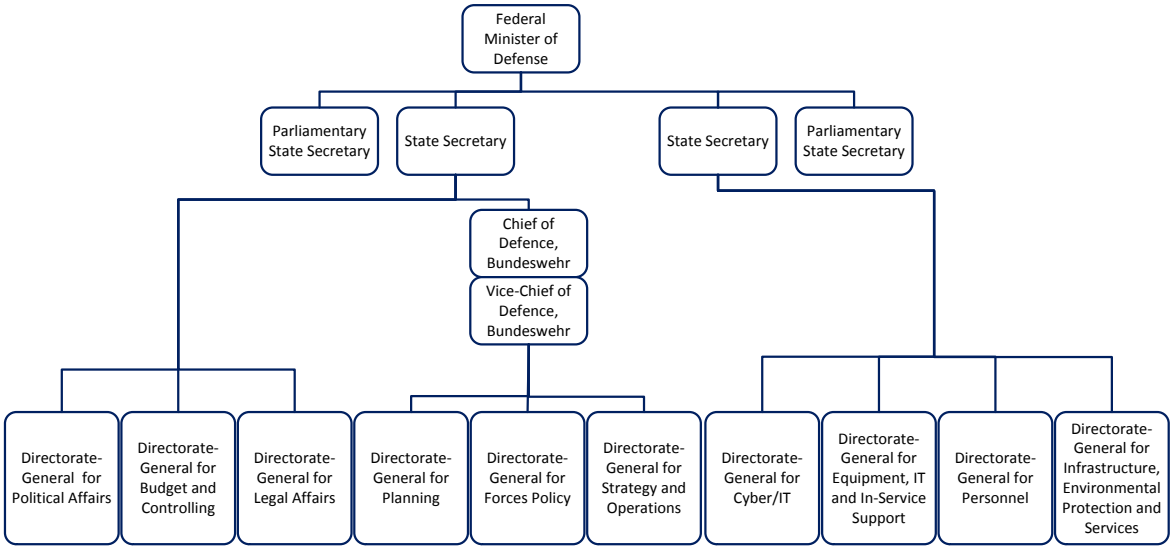


Figura 11 – Organização do FMoD

Fonte: adaptado pelo autor (Bundesministerium der Verteidigung, 2016)

O Diretor-Geral CIT tem as seguintes responsabilidades:

- Exercer o poder de decisão e a representação externa dos interesses nas matérias CIT da FMoD, a nível nacional e internacional;
- Assegurar utilização das TIC em conformidade com os objetivos políticos, estratégicos e operacionais do FMoD e de acordo com diretrizes do Governo Federal;
- Garantir o desenvolvimento futuro, bem como priorização dos requisitos dos utilizadores em matéria de CIT;
- Emitir orientações centrais para a normalização, conceção, desenvolvimento, instalação, monitorização, exploração e proteção das TIC na área de responsabilidade da FMoD;
- Controlar a implementação de arquiteturas e normas TIC, dos objetivos estratégicos e as decisões do *IT Council*;
- Reunir as necessidades (*demand*) TIC do FMoD e garantir a supervisão técnica a fornecedores internos de serviços TIC;
- Consolidar serviços TIC intraministeriais;
- Participar em iniciativas legislativas do FMoD que afetam as TIC em exploração na administração pública;

- Garantir a segurança da informação no FMoD através do *Chief Information Security Officer*[14] (CISO).

A Direcção-Geral do CIT baseia-se num modelo de *PLAN* - *BUILD* - *RUN* (planeamento, construção e execução).

Com base neste modelo, foram criadas duas divisões com as seguintes responsabilidades:

- Divisão CIT I concentra-se nas tarefas de *cyber* e governação das TIC (*PLAN*) subdivididas em:
  - Estratégia e Política - definição da política, estratégia, controlo e consolidação das TIC para o Governo Federal, assim como a coordenação com organismos nacionais e internacionais;
  - Gestão da Inovação – análise de necessidades financeiras futuras, identificação de objetivos a médio prazo, identificação da necessidade desenvolvimento de novas capacidades informáticas, gestão da inovação, investigação e tecnologia, nas TIC;
  - Gestão da Arquitetura *Cyber* / IT - desenvolvimento de uma arquitetura de CIT, bem como a definição de politicas e arquitetura de segurança das TIC, desenvolvimento conceptual da formação básica e avançada dos recursos humanos das TIC;
  - Administração Digital - gestão da informação, coordenação de inquéritos ao abrigo do *Freedom of Information Act*[15];
  - Assuntos de informação geográfica da *Bundeswehr*[16]- a coordenação e apoio aos Sistemas de Informação Geográfica da *Bundeswehr;*
- Divisão CIT II concentra-se na implementação (BUILD) e exploração (RUN). O CISO é o Chefe desta Divisão. As tarefas estão subdivididas em:
  - Desenvolvimento e exploração das TIC da *Bundeswehr* – definição da política e do controlo das TIC, garantia o apoio ao comando e controlo, coordenação dos requisitos para os prestadores de serviços

[14] Responsável máximo da organização, responsável por garantir a segurança das TIC.
[15] Lei que permite o acesso do público em geral aos dados detidos pelo governo nacional (Bundesministerium der Justiz und fur Verbraucherschutz, 2017)
[16] Forças Armadas Alemãs

informáticos e para a BWI[17], coordenação das TIC para o FMoD e a *Bundeswehr;*

- Proteção do sistema informático da Bundeswehr - implementação da segurança nas TIC, execução de atividades cibernéticas defensivas, segurança da informação, criptografia, acreditação e gestão de crises informáticas;
- Serviços Nucleares - a implementação de serviços TIC nucleares, transversais a toda a *Bundeswehr*, gestão de contratos da BWI;
- Comunidade de Interesses e Serviços de Comunicações - implementação de serviços com aplicação nas operações e exercícios;
- *Standard Application Software Product Families* (SASPF) - implementação de serviços aplicacionais para logística, baseados em Sistemas SAP.

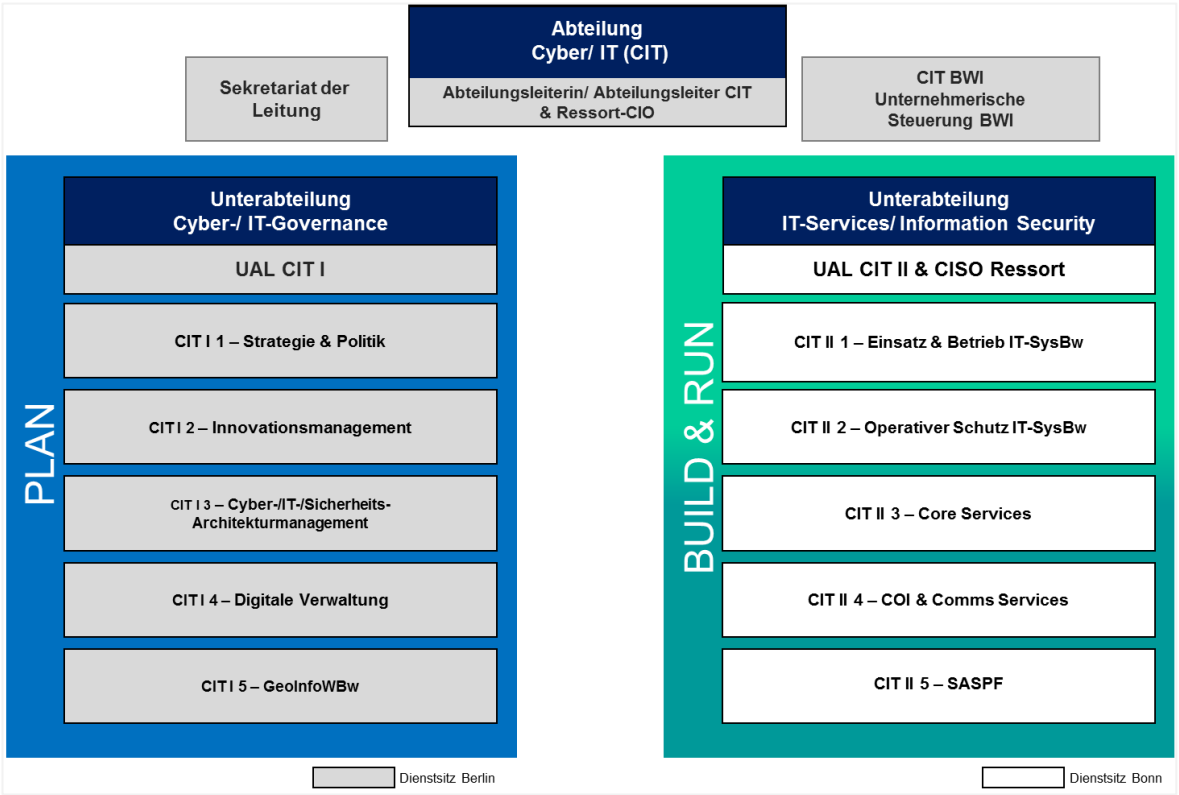


Figura 12 – Organização da Direção-Geral *Cyber*/IT

Fonte: (Bundesministerium der Verteidigung, 2016)

[17]A BWI é uma empresa estatal, fornecedora de serviços TIC para a *Bundeswehr* (BWI Informationstechnik GmbH, 2017).

A Direcção-Geral do CIT tem autonomia financeira, através da atribuição de um orçamento dedicado para a realização das suas atividades, em conformidade com o planeamento da *Bundeswehr* (Bundesministerium der Verteidigung, 2016).

Este modelo de governação prevê que a consolidação das competências e responsabilidades em matérias CIT tenha em conta rápidos ciclos de inovação, sendo para isso necessário recorrer a processos de planeamento ágeis (Bundesministerium der Verteidigung, 2016).

Ao nível do planeamento, o CIO tem a responsabilidade de planear todos os projetos TIC na sua área de responsabilidade, recorrendo a ferramentas de priorização dos projetos e programas. O Processo de planeamento é realizado com uma periodicidade inferior a um ano (Bundesministerium der Verteidigung, 2016).

O primeiro painel de planeamento[18] atribui o orçamento ao CIO, que será determinado com base na estratégia TIC da FMoD, nos seus objetivos e medidas a implementar durante ciclo de planeamento seguinte. O orçamento pode ser adaptado posteriormente por um segundo painel de planeamento (Bundesministerium der Verteidigung, 2016).

Os recursos humanos são um dos pilares importantes neste modelo. Para isso foi identificado a necessidade de criar novas carreiras profissionais, suficientemente dinâmicas e adaptáveis, que garantam as competências e adequadas à realidade tecnológica. O recrutamento através de formas inovadoras (escolas, eventos tecnológicos, *LAN Parties*[19]) é um dos métodos identificados para atrair candidatos para a organização. Outra forma inovadora é a possibilidade de atrair candidatos sem qualquer qualificação académica superior, desde que apresentem as competências necessárias.

A formação básica e avançada também faz parte da estratégia da aposta nos recursos humanos para todos os níveis da organização.

3.3. **Síntese Conclusiva**

Os Ministérios da Defesa aqui analisados apresentam caraterísticas diferentes ao MDN, nomeadamente ao nível da organização e da sua dimensão.

[18] O painel de planeamento é composto por dois Secretários de Estado permanentes, o *Chief of Defence*, o *Director-General for Planning*, o *Director-General for Budget and Controlling* e o CIO

[19] Uma LAN *party* é um evento criado para juntar pessoas com os seus computadores, ao qual os ligam numa rede local, com o objetivo de jogar jogos de computador.

Em ambos os casos as FFAA estão focadas nas suas atividades operacionais, passando para alçada dos respetivos ministérios a consecução das atividades de suporte, entre as quais se inclui as atividades relacionadas com as TIC.

No caso do MDH as TIC foram centralizadas num único organismo, que fornece os serviços de forma transversal no ministério. O âmbito dos serviços TIC disponibilizados é também mais alargado, pois estão incluídos os sistemas militares. Desta forma implementaram um modelo de Governação baseado num modelo *Demand-CIO-Supply*, que separa claramente o papel de quem determina a procura (*Demand*) do papel de quem fornece as necessidades (*Supply*). Neste modelo a componente Militar do Ministério da Defesa determina a procura, e o DMO fornece as necessidades.

O FMoD criou um organismo responsável por todas as matérias relacionadas com as TIC e *cyber*. Para além da governação, gestão e implementação das TIC dentro do ministério, que se encontra definido nas suas competências, o FMoD atribuiu competências a este Organismo para participar em iniciativas legislativas que afetam as TIC na administração publica. O modelo de governação definido foi o *PLAN-BUIL-RUN*.

Desta forma é possível responder à QD2, caraterizando dois modelos de governação implementados nos respetivos Ministérios da Defesa e que satisfazem as necessidades de uma forma transversal, contudo com um âmbito mais alargado.

4. Princípios do Modelo de Governação

Tal como na maioria das normas e *frameworks*, não existe uma receita única que se aplique em todas as organizações. As organizações inserem-se num contexto que é caraterizado por fatores externos (mercado, setor, geopolítica, entre outros) e fatores internos (cultura, organização, apetite ao risco, etc.). Estes fatores têm um impacto tal, que justificam a necessidade de personalizar o modelo de Governação para cada organização.

O COBIT5 é a *framework* utilizada neste trabalho para a definição dos princípios que devem ser seguidos na definição do modelo de governação para as TIC na DN.

Esta *framework*, assim como as restantes normas, define em traços gerais os princípios, linhas de ação e boas práticas que devem ser seguidos e que auxiliem as organizações a governar as TIC.

O COBIT5 é um modelo mais abrangente que define não só a governação como também a Gestão e ajuda as orientar as organizações para a criação de valor (ISACA, 2012).

Esta *framework* baseia-se em cinco princípios básicos, que servem de referencia para a criação de um efetivo modelo de governação e gestão das TIC (ISACA, 2012).

Os próximos subcapítulos irão descrever cada um dos princípios definidos no COBIT5.

Figura 13 – Princípios do COBIT5

Fonte: (ISACA, 2012)

4.1. **Atender às necessidades das partes interessadas**

As necessidades dos *stakeholders* devem ser transformadas em estratégias organizacionais, visto que o objetivo da organização é a criação de valor[20]. Consequentemente a governação deverá visar a criação de valor através da definição de uma estratégia para a organização (ISACA, 2012).

Figura 14 – Objetivo do Modelo de Governação

Fonte: (ISACA, 2012)

Por isso, este princípio está consequentemente relacionado com o alinhamento estratégico entre as TIC e o negócio (ISACA, 2012).

A definição da estratégia da organização, segundo o COBIT5, realizado através de um mecanismo denominado Cascata de Objetivos, o qual traduz as necessidades dos *stakeholders* em objetivos organizacionais específicos, personalizados, exequíveis, objetivos TIC e respetivas metas. Este mecanismo permite um mapeamento de objetivos específicos em cada nível e em cada área da organização alinhados com os objetivos gerais (ISACA, 2012).

A Cascata de Objetivos é um processo definido em quatro passos, conforme demonstrado na Figura 15 (ISACA, 2012):

"1º Passo - Os Direcionadores das Partes Interessadas influenciam as Necessidades das Partes Interessadas

2º Passo - Desdobramento das Necessidades das Partes Interessadas em Objetivos Corporativos

[20] Obtenção de benefícios através da otimização da exploração de recursos e dos riscos a um nível aceitável (ISACA, 2012).

3º Passo - Cascata dos Objetivos Corporativos em Objetivos de TIC

4º Passo - Cascata dos Objetivos de TIC em Metas do Habilitador “

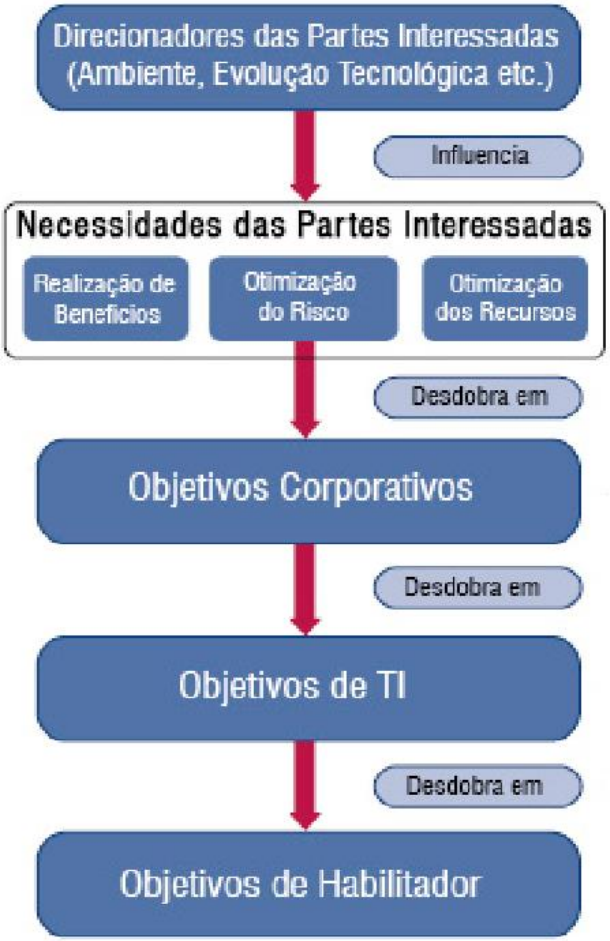


Figura 15 – Visão Geral da Cascata de Objetivos do COBIT5

Fonte: (ISACA, 2012)

4.2. Cobrir a organização de ponta a ponta

O COBIT5 aborda a Governação e a Gestão da informação e da tecnologia de forma transversal a toda a organização. Desta forma a Governação das TIC proposta pelo COBIT5 é passível de ser integrada em qualquer modelo de governação de uma organização. Para além disso, cobre todas as funções e processos necessários para regular e controlar todos os recursos informacionais e tecnologias da organização (ISACA, 2012).

Figura 16 – Governação e Gestão das TIC no COBIT5

Fonte: (ISACA, 2012)

Na Figura 16 podem ser observados os principais componentes de um sistema de governação, nos quais se inclui o Objetivo da Governação; os Habilitadores; o Âmbito (Escopo); e as Funções, Atividades e Relacionamentos (ISACA, 2012).

Os Habilitadores são os recursos organizacionais da governação, tais como modelos, princípios, processos e práticas, que irão ser utilizados para se atingir os objetivos da organização. Os Habilitadores também incluem recursos materiais (infraestrutura TIC, sistemas, etc.), humanos e informacionais (ISACA, 2012).

O Âmbito da Governação é fundamental para definir se a governação se aplica a toda a organização, ou apenas a uma parte, mediante as visões que existem dentro da organização (ISACA, 2012).

As Funções, Atividades e Relacionamentos definem quem está envolvido na governação, de que forma estão envolvidos, o que fazem e como interagem entre si. A Figura 17 apresenta em detalhe as interações entre os diferentes papéis (ISACA, 2012).

Figura 17 – Funções, Atividades e Relacionamentos

Fonte: (ISACA, 2012)

4.3. **Aplicar um *framework* único e integrado**

O COBIT5 tem uma estrutura única e integrada, porque integra um conjunto de *frameworks* da ISACA, tais como o COBIT 4.1, Val IT (valor de TI para o negócio), Risk IT (risco relacionado ao uso de TI), BMIS (segurança). Está alinhado com os mais atuais e relevantes padrões e *frameworks* utilizados (ISACA, 2012).

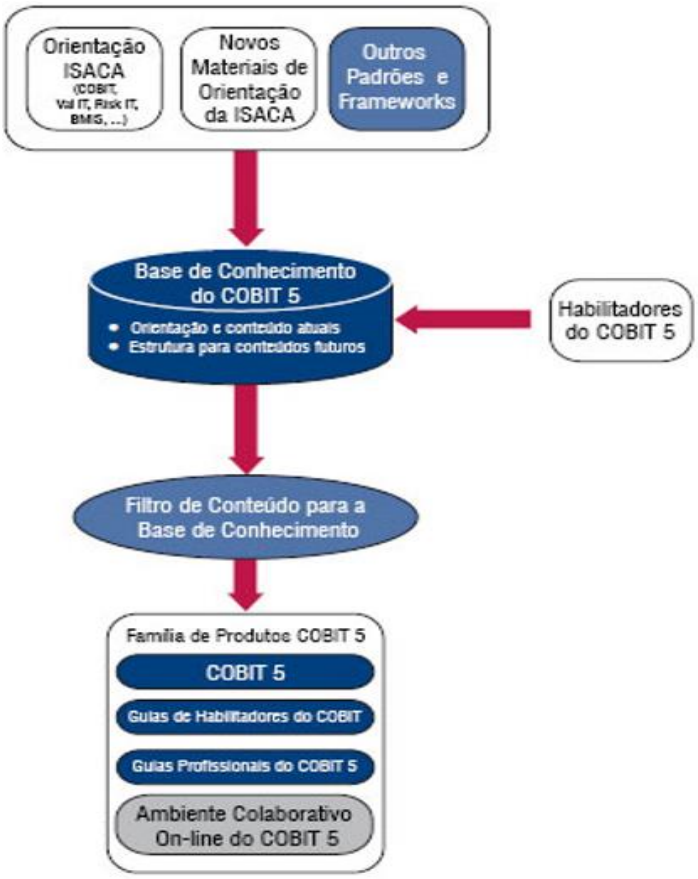


Figura 18 – Modelo Único Integrado do COBIT5

Fonte: (ISACA, 2012)

4.4. **Permitir uma abordagem holística**

Para apoiar a Governação e a Gestão das TIC, utilizando uma abordagem holística, o COBIT5 define um conjunto de sete habilitadores (ISACA, 2012).

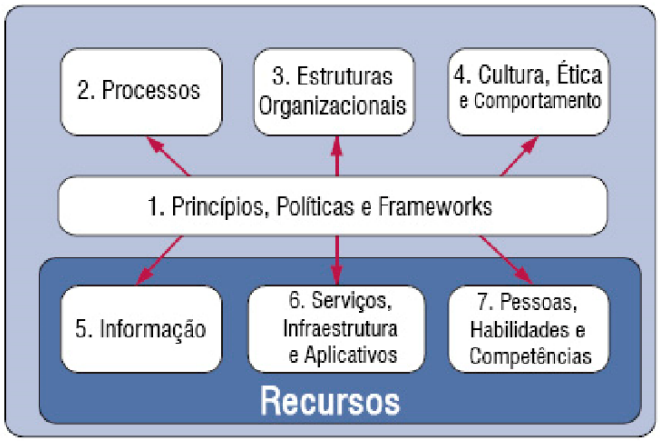


Figura 19 – Habilitadores Organizacionais do COBIT5

Fonte: (ISACA, 2012)

Os habilitadores são os seguintes (ISACA, 2012):

1. Princípios, políticas e *frameworks* - são os mecanismos que traduzem o comportamento desejado num guia prático para a gestão diária;
2. Processos - descrevem de forma organizada o conjunto de práticas e atividades para atingir determinados objetivos. Estes têm uma atividade iniciadora e uma ou mais saídas que deverão estar centrados no cumprimento dos objetivos TIC;
3. Estruturas organizacionais - são as entidades-chave responsáveis pela tomada de decisão numa organização;
4. Cultura, ética e comportamento (dos indivíduos e da organização) - é um fator de sucesso nas atividades de governação e gestão;
5. Informação - está espalhada por toda organização. Pode ser encontrada em diversas formas e é produzida e utilizada pela organização. É imprescindível para manter a organização em funcionamento e bem governada;
6. Serviços, infraestrutura e aplicações - Inclui a infraestrutura, tecnologia e sistemas ao dispor da organização;
7. Pessoas, habilidades e competências - Estão associadas aos recursos humanos e são a base para o sucesso da execução das atividades e da tomada da decisão.

4.5. Distinguir a governação da gestão

O COBIT 5 introduz o conceito de governação e diferencia-o da gestão TIC das organizações, conforme descrito no Capítulo 1. Esta distinção é bastante evidente no Modelo de Referência de Processos (Figura 20), que subdivide os 37 processos de TI em duas principais áreas de atividade – Governação e Gestão – e agrupadas em processos (ISACA, 2012).

Os processos da área da Governação são os seguintes:

- EDM01 – Garantir a Definição e Manutenção do Modelo de Governança: este processo tem como objetivo analisar os requisitos para a Governação das TIC da organização e garantir a implementação dos princípios e processos, definir a responsabilidade e a autoridade dentro da organização para atingir objetivos estratégicos da organização (Gotardo, 2015).
- EDM02 – Garantir a Realização de Benefícios: este processo tem como objetivo otimizar e entregar o valor ao negócio através dos serviços TI disponibilizados, através dos recursos materiais ou informacionais e processos de negócio (Gotardo, 2015).
- EDM03 – Garantir a Otimização do Risco: este processo tem como objetivo assegurar a gestão do risco, a sua análise e definição do apetite que a organização tem ao risco (Gotardo, 2015).
- EDM04 – Garantir a Otimização dos Recursos: este processo tem como objetivo assegurar a disponibilização das capacidades TIC (recursos materiais, informacionais e humanos), para apoiar os objetivos da organização de forma eficaz a um custo ótimo (Gotardo, 2015).
- EDM05 – Garantir a Transparência para as Partes Interessadas: este processo tem como objetivo assegurar a elaboração de relatórios e utilização de mecanismos de análise do desempenho e conformidade das TIC, de forma a garantir transparência no processo de decisão e na definição de ações corretivas necessárias para o alinhamento do modelo de governação (Gotardo, 2015).

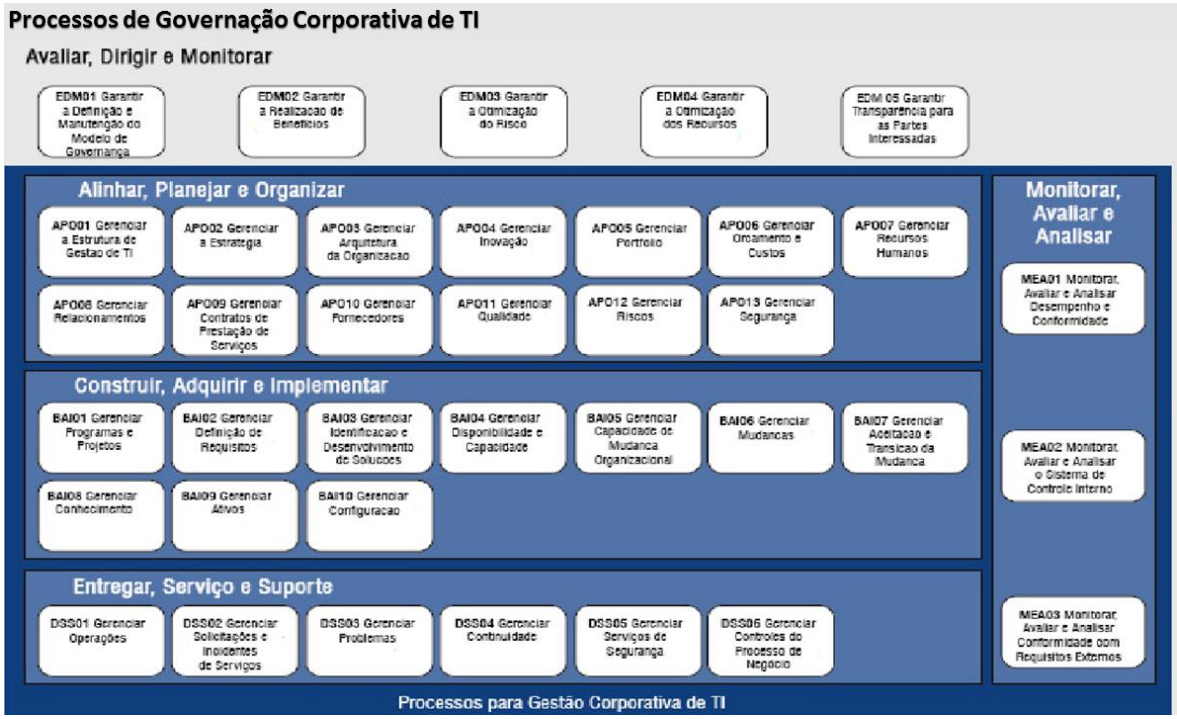


Figura 20 – Modelo de Referência de Processos do COBIT5

Fonte: (ISACA, 2012)

Estas duas áreas compreendem diferentes tipos de atividades, em diferentes estruturas organizacionais e servem a propósitos diferentes (ISACA, 2012).

Na Governação, são discutidas e aprovadas as políticas e as estratégias, a implementação de processos e os mecanismos de controlo que definem as linhas de orientação para a gestão das TIC (ISACA, 2012).

Na maioria das organizações, a Governação é da responsabilidade do Conselho de Administração, sob a liderança do presidente. As Responsabilidades de governação podem, no entanto, ser delegadas em estruturas organizacionais especiais, nomeadamente em organizações de maiores dimensões e mais complexas (ISACA, 2012).

4.6. Síntese Conclusiva

A *framework* COBIT5 apenas auxilia as organizações na criação de um modelo que permita não só a governação, como também a gestão dos SI e consequentemente apoia a criação de valor, mantendo um equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos.

Recorrendo aos cinco princípios da governação definidos nesta *framework* é possível apresentar um modelo de governação que satisfaça as necessidades do MDN, sendo desta forma possível responder à QD3.

Conclusões

Para este trabalho de investigação individual foi proposto a definição de um modelo de governação para o MDN, face à heterogeneidade de infraestruturas e Sistemas de Informação e Tecnologias de Informação e Comunicações disponíveis.

O estudo realizado focou-se essencialmente na análise da metodologia já utilizada no MDN, num projeto cuja dimensão requereu a adoção de um modelo de governação. Como complemento analisou-se também qual a metodologia utilizada em Ministérios da Defesa de dois outros países e que modelos de governação para as TIC têm implementados. Por fim analisou-se uma *framework* de referência para a definição dos princípios essenciais para a definição de um modelo de governação.

A investigação realizou-se recorrendo a uma estratégia qualitativa e método indutivo, com base num Estudo de Caso, que utilizou como base de observação o modelo de governação das TIC da Defesa da Holanda e Alemanha. As técnicas de recolha de dados foram a análise documental e entrevistas.

A investigação teve como objetivo a responder à QC e para isso foram estabelecidas QD as quais foram respondidas nos capítulos segundo, terceiro e quarto.

No segundo capítulo verificou-se a existência e utilização de um modelo de governação para um único SI, o SIGDN. O modelo de governação implementado não inclui todos os organismos do MDN e não contempla a governação de todos os sistemas de gestão comuns ao MDN. A estratégia utilizada, para mitigar a ausência de uma governação de novos sistemas, passou por aproveitar a estrutura organizacional prevista no SIGDN para realizar reuniões de coordenação e gestão dos novos projetos.

Conclui-se neste capítulo que, apesar das competências atribuídas ao CDD e DSSI, que se encontram na dependência da SG, a governação e gestão das TIC de todos os organismos da defesa ainda não se encontra em execução.

Conclui-se também a ausência de alinhamento estratégico com Diretivas do Governo, nomeadamente a Estratégia TIC 2020, definido pelo Concelho de Ministros, e pelo Plano Setorial TIC definido pelo MDN.

Desta forma foi possível responder à QD1, caraterizando o SIGDN como único SI que foi desenvolvido recorrendo a um modelo de governação. Os restantes SI/TIC de gestão comum da DN não estão a ser geridos, desenvolvidos, nem explorados recorrendo a um modelo de governação.

No terceiro capítulo analisou-se os modelos de governação dos Ministérios da Defesa da Holanda e Alemanha. Estes Ministérios apresentam caraterísticas diferentes ao MDN português, nomeadamente ao nível da organização e da sua dimensão.

Em ambos os casos as Forças Armadas estão focadas nas suas atividades operacionais, passando para alçada dos respetivos ministérios a consecução das atividades de suporte, entre as quais se inclui as atividades relacionadas com as TIC.

No caso do MDH as TIC foram centralizadas num único organismo, que fornece os serviços de forma transversal no ministério. O âmbito dos serviços TIC disponibilizados é também mais alargado, pois estão incluídos os sistemas militares. Desta forma implementaram um modelo de Governação baseado num modelo *Demand-CIO-Supply*, que separa claramente o papel de quem determina a procura (*Demand*) do papel de quem fornece as necessidades (*Supply*). Neste modelo a componente Militar do Ministério da Defesa determina a procura, e o DMO fornece as necessidades.

O FMoD criou um organismo responsável por todas as matérias relacionadas com as TIC e *cyber*. Para além da governação, gestão e implementação das TIC dentro do ministério, que se encontra definido nas suas competências, o FMoD atribuiu competências a este organismo para participar em iniciativas legislativas que afetam as TIC na administração pública. O modelo de governação definido foi o *PLAN-BUIL-RUN*.

Conclui-se assim que os dois modelos de governação implementados nos respetivos Ministérios da Defesa satisfazem as necessidades de uma forma transversal, contudo com um âmbito mais alargado, respondendo desta forma à QD2.

No capítulo quarto sintetizaram-se os princípios a serem adotados pelo modelo de governação do MDN. Analisou-se a *framework* COBIT5, que auxilia as organizações na criação de um modelo que permita não só a governação, como também a gestão dos SI e consequentemente apoia a criação de valor, mantendo um equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos.

Recorrendo aos cinco princípios da governação definidos nesta *framework* é possível apresentar um modelo de governação que satisfaça as necessidades do MDN, respondendo assim à QD3.

Presente o que precede, concretizou-se o modelo de governação que se encontra no Apêndice A — Modelo de Governação Proposto. Este modelo foi construído através dos seguintes pressupostos que respondem à QC:

- O modelo de governação TIC na DN deverá estar alinhado com um planeamento estratégico/diretivas politicas;
- O modelo deverá prever a elaboração de um planeamento estratégico das TIC, que defina a médio prazo (quatro anos), os objetivos estratégicos, linhas de ação, metas e indicadores para as TIC;
- O modelo deverá prever a criação de três níveis de decisão;
- Os níveis de decisão deverão ter representantes de todos os organismos do MDN (FFAA, Serviços Centrais e IASFA);
- O nível mais alto de decisão deverá ser composto pelos Diretores/Chefes dos organismos do MDN e deverá ter a competência para definir as Políticas das TIC na Defesa Nacional;
- O nível médio de decisão, composto pelos CIO dos organismos, deverá ter a competência para determinar as responsabilidades da governação, definição da visão e estratégia das TIC;
- O nível mais baixo da decisão (gestão), composto por representantes técnicos dos organismos, deverá ter a competência para determinar o Plano Anual de Atividades, Análise e monitorização dos Projetos TIC;
- Cada um dos níveis de decisão deverá reunir com uma frequência que se adeque ás necessidades de resposta da tomada de decisão;
- Deverão ser criadas comissões de carater permanente, sem afetar a alterações à Lei Orgânica do MDN;
- O modelo deverá prever a capacidade de monitorização/avaliação do desempenho da execução do plano estratégico para as TIC;
- Deverá ser elaborado um plano de Atividades tendo por base o Planeamento Estratégico TIC do MDN;
- As atividades (projetos/programas) deverão satisfazer as necessidades de todos ou parte dos organismos da DN;
- Deverão ser elaborados e publicados relatórios que apresentem o estado da execução do plano estratégico TIC.

Este trabalho contribuiu para o conhecimento através da apresentação de um modelo de governação para as TIC, que é possível consultar no Apêndice A — Modelo de Governação Proposto.

Como recomendação prática, sugere-se que o modelo seja submetido à SG e analisado, de forma a estabelecer um plano para implementação do modelo de governação proposto neste trabalho.

Durante o trabalho de investigação foram identificadas limitações com impacto para a investigação, a saber: a obtenção da informação requerida aos Ministérios das Defesa da Holanda, Alemanha; Obtenção de toda a bibliografia relacionada com a implementação de um modelo de governação através da *framework* COBIT5, face aos custos de obtenção da mesma e à complexidade desta área de conhecimento.

Bibliografia

Agência para Modernização Administrativa, 2016. *Taxa de Execução do PGETIC - MDN*. [Em linha] Disponível em: https://tic.gov.pt/pgetic/ministerios/mdn [Consult. 08 dezembro 2016].

Bundesministerium der Justiz und fur Verbraucherschutz, 2017. *Federal Act Governing Access to Information held by the Federal Government*. [Em linha] Disponível em: http://www.gesetze-im-internet.de/englisch_ifg/index.html [Consult. 04 março 2017].

Bundesministerium der Verteidigung, 2016. *Final Report of the Activation Staff of the Joint Cyber and Information Domain Service*.

Bundesministerium der Verteidigung, 2016. *Organisationsübersicht des Bundesministeriums der Verteidigung*. [Em linha] Disponível em: https://www.bmvg.de/resource/resource/UlRvcjZYSW1RcEVHaUd4cklzQU4yMzFYNnl6UGxhbm1vNGx0VVVuZlIvaFpodndZMnQvdDRDWGY4S1lhN0IrNHNzQ1ZTQlRHSmJlbmdUZllwMmt2NytxY0VTRlBLYm5iMG5IVmNydmx0MWc9/161101_OrgPlan_BMVg.pdf [Consult. 04 março 2017].

BWI Informationstechnik GmbH, 2017. *BWI Informationstechnik*. [Em linha] Disponível em: https://www.bwi-it.de/unternehmen/wer-sind-wir/ [Consult. 04 março 2017].

Cecere, M., Cullen, A. e DeGennaro, T., 2008. *Demand/Supply Organization Models have Pros and Cons*. [Em linha] Disponível em: http://c.ymcdn.com/sites/www.simnet.org/resource/collection/5DD9A06C-4C50-46ED-A313-3992A14320DC/2008.03_Forrester_Demand_Supply_Organizations.pdf [Consult. 24 Fevereiro 2017].

Conselho de Ministros, 2017. *Comunicado do Conselho de Ministros de 2 de março de 2017*. [Em linha] Disponível em: http://www.portugal.gov.pt/pt/o-governo/cm/comunicados/20170302-com-cm.aspx [Consult. 02 março 2017].

Diário da República, 1998. Decreto-Lei n.o 59/98 de 17 de Março. *Diário da República*, 17 março. p.1124.

Diário da República, 2012. Portaria n.º 86/2012 - Organização interna da Secretaria-Geral do Ministério de Defesa Nacional. *Diário da República*, 30 março.

Diário da República, 2014. Decreto-Lei n.º 183/2014 - Lei Orgânica do MDN. *Diário da República*, 29 dezembro.

Diário da República, 2014. Decreto-Lei n.º 185/2014 - Lei Orgânica da Marinha. *Diário da República*, 29 dezembro.

Diário da República, 2014. Lei Orgânica do EMGFA. *Decreto-Lei n.º 184/2014*, 29 dezembro.

Diário da República, 2015. Decreto Regulamentar n.º 10/2015. *Diário da República*, 31 julho.

Diário da Republica, 2016. Resolução do Conselho de Ministros n.º 33/2016. *Diário da República*, 03 junho. p.1735.

Francisco, C.R.M.A., 2017. *Governação das TIC no MDN* [Entrevista]. Lisboa (24 fevereiro 2017).

Gorgulho, M., 2007. *As melhores práticas da Gestão de Serviços de Tecnologias da Informação – ITIL*. Lisboa: IESM.

Gotardo, R., 2015. *Governança em Tecnologia da Informação*. 1ª ed. Rio de Janeiro: SESES.

Government of the Netherlands, 2017. *Ministry of Defense - Organization Chart*. [Em linha] Disponível em: https://www.government.nl/ministries/ministry-of-defence/contents/organisation-chart [Consult. 24 fevereiro 2017].

GPTIC, 2011. *Plano global estratégico de racionalização e redução - Horizonte 2012-2016*. Lisboa: Governo de Portugal.

GPTIC, 2012. *Plano de ação setorial de racionalização das TIC no Ministério da Defesa Nacional - Horizonte 2012-2016*. Lisboa: Ministério da Defesa Nacional.

IESM, 2015. *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação*. Lisboa: IESM.

Inspeção-Geral da Defesa Nacional, 2016. *Processo de Implementação de Sistemas de Informação no ãmbito da Defesa Nacional- SIGDN*. Inspeção-Geral da Defesa Nacional.

International Organization for Standardization, 2008. *ISO/IEC 38500 - Corporate governance of information technology*. Geneva: International Organization for Standardization.

ISACA, 2012. *COBIT 5 - Modelo Corporativo para Governança e Gestão de TI da Organização*. Rolling Meadows: isaca.

Lambrichs, C., 2016. *The Defence Materiel Organisation*.

Laudon, K.C. e Laudon, J.P., 2012. *Management Information Systems - Managing the digital Firm*. 12ª ed. Harlow: Pearson.

Lévy, P., 1999. *Cibercultura*. 1ª ed. São Paulo: Editora 34.

Maizière, T., 2013. *Die Neuausrichtung der Bundeswehr*. Berlin: Bundesministerium der Verteidigung.

Marques, C.-A.A.J.G., 2016. *Governação das TIC no MDN* [Entrevista]. Lisboa (05 dezembro 2016).

Miguel, A., 2010. *Gestão de Projetos de Software*. 4ª ed. Lisboa: FCA.

Ministério da Defesa Nacional, 2013. *Sistema Integrado de Gestão da Defesa Nacional - O Modelo de Governação*.

Ministry of Defense, 2017. *NL MoD - organization*. [Em linha] Disponível em: https://www.defensie.nl/english [Consult. 15 fevereiro 2017].

Montana, P.J. e Charnov, B., 2008. *Management*. 4ª ed. New York: Barron's Educational Series.

Murugan, M., 2007. *Management Principles And Practices*. New Age International.

Pinho, C.V., 2017. *Estrutura de Coordenação do SIGDN* [Entrevista]. Lisboa (24 Fevereiro 2017).

Presidência do Concelho de Ministros, 2011. Resolução do Conselho de Ministros n.º 46/2011. *Diário da República*, 14 novembro.

Project Management Institute, 2013. *A Guide to the Project Management Body of Knowledge*. 5ª ed. Pennsylvania: PMI.

Salvado, C.A.M.R., 2017. *Governação das TIC no MDN* [Entrevista]. Lisboa (17 Janeiro 2017).

Salvado, A.M., s.d. *Sistema Integrado de Gestão da Defesa Nacional - Organização Interna*. Ministério da Defesa Nacional.

Seuanes, J., 2013. *Reorganização das TIC na Defesa Nacional*. Pedrouços: IESM.

Silva, S.d.S.M.C., 2011. *O Sistema Integrado de Gestão da Defesa Nacional na Marinha: Situação actual e perpetivas futuras*. Lisboa: Instituto de Estudos Superiores Militares.

Sousa, C.-d.-M.-e.-G.L.F.F.d. e Garcia, C.-F.J.J.G.P., 2017. *Governação do SIGDN* [Entrevista]. Lisboa (15 fevereiro 2017).

The Federation of Enterprise Architecture Professional Organizations, s.d. *A Common Perspective on Enterprise Architecture*. [Em linha] Disponível em:

http://feapo.org/wp-content/uploads/2013/11/Common-Perspectives-on-Enterprise-Architecture-v15.pdf [Consult. 24 ferereiro 2017].

Weill, e Ross, W., 2013. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Press.

Anexo A — Competências da Direção de Serviços dos Sistemas de Informação

Direção de Serviços dos Sistemas de Informação

À Direção de Serviços dos Sistemas de Informação, abreviadamente designada por DSSI, compete (Diário da República, 2012):

- Elaborar e propor as orientações para a integração dos sistemas de informação (SI) da defesa nacional, em colaboração com a estrutura das Forças Armadas;
- Elaborar e propor o plano estratégico e o modelo de governação dos SI da defesa nacional;
- Assegurar a gestão de informação e a administração de dados da defesa, no âmbito das atribuições previstas no modelo de governação dos SI da defesa;
- Coordenar as atividades dos SI no universo da defesa nacional, garantindo a articulação dos SI de gestão com os sistemas de informação de comando e controlo militares, e exercer as competências de entidade de coordenação setorial;
- Conceber, desenvolver e administrar os sistemas de informação de gestão comuns;
- Garantir a normalização, qualidade e segurança dos SI de gestão;
- Dar parecer sobre os projetos de SI dos vários organismos da defesa, no âmbito do modelo de governação dos SI;
- Apoiar as entidades competentes na realização de auditorias aos SI dos serviços e organismos da defesa, assegurando a adoção de boas práticas.

Compete à DSSI, no âmbito do Sistema Integrado de Gestão:

- Garantir a gestão global do Sistema Integrado de Gestão da Defesa Nacional (SIGDN);
- Planear e implementar novas funcionalidades;
- Garantir apoio específico com vista ao arranque em produtivo de novas entidades;
- Executar ações de manutenção corretiva e evolutiva ao sistema em produtivo;
- Elaborar e distribuir documentação técnica de suporte ao sistema;
- Executar ações de apoio funcional e técnico aos utilizadores, com vista à resolução de incidentes que resultem de erros de parametrização.

Anexo B — Competências do Centro de Dados da Defesa

Centro de Dados da Defesa

Ao Centro de Dados da Defesa, abreviadamente designado por CDD, compete (Diário da República, 2012):

- Assegurar a prestação de serviços de tecnologias de informação a todos os organismos da defesa, no âmbito das atribuições previstas no modelo de governação dos SI da defesa;
- Assegurar a administração da infraestrutura tecnológica partilhada que suporta os sistemas de informação de gestão;
- Assegurar a administração de sistemas aplicacionais e de bases de dados da defesa, no âmbito das atribuições previstas no modelo de governação dos SI da defesa;
- Assegurar a administração da rede informática da defesa, garantindo a sua adequada segurança, capacidade, disponibilidade, bem como a interoperabilidade e interconexão entre todos os serviços e organismos da área da defesa e outras entidades nacionais e internacionais, no âmbito das atribuições previstas no modelo de governação dos SI da defesa;
- Assegurar o apoio centralizado aos utilizadores dos SI de gestão.

Apêndice A — Modelo de Governação Proposto

Âmbito do Documento

Este documento visa definir o modelo de governação das TIC para a Defesa Nacional, para melhorar a eficiência da exploração dos recursos humanos, materiais e informacionais na área das TIC, e promover a comunicação e a transparência.

O modelo proposto foi baseado na *framework* COBIT5.

Este modelo de governação não prevê a alterações às leis orgânicas dos organismos envolvidos e desta forma está fora do âmbito a criação ou extinção de entidades, organismos ou departamentos.

1. Processos do Modelo de Governação

O objetivo desta seção é a descrever os processos de Governação.

a. Descrição

O modelo de Governação encontra-se definido num processo de negócio que define todo o ciclo do modelo de governação e que se encontra na Figura 21. Este modelo de governação agrega os cinco processos definidos no COBIT5 para a Governação.

Os processos definidos no COBIT5 para a área da Governação são os seguintes:

- **EDM01 – Garantir a Definição e Manutenção do Modelo de Governação**: este processo tem como objetivo analisar os requisitos para a Governação das TIC da organização e garantir a implementação dos princípios e processos, definir a responsabilidade e a autoridade dentro da organização para atingir objetivos estratégicos da organização.
- **EDM02 – Garantir a Realização de Benefícios**: este processo tem como objetivo otimizar e entregar o valor ao negócio através dos serviços TI disponibilizados, quer seja através dos recursos materiais ou informacionais e processos de negócio.
- **EDM03 – Garantir a Otimização do Risco**: este processo tem como objetivo assegurar a gestão do risco, a sua análise e definição do apetite que a organização tem ao risco.
- **EDM04 – Garantir a Otimização dos Recursos**: este processo tem como objetivo assegurar a disponibilização das capacidades TIC (recursos materiais, informacionais e humanos), para apoiar os objetivos da organização de forma eficaz a um custo ótimo.

- **EDM05 – Garantir a Transparência para as Partes Interessadas**: este processo tem como objetivo assegurar a elaboração de relatórios e utilização de mecanismos de análise do desempenho e conformidade das TIC, de forma a garantir transparência no processo de decisão e na definição de ações corretivas necessárias para o alinhamento do modelo de governação.

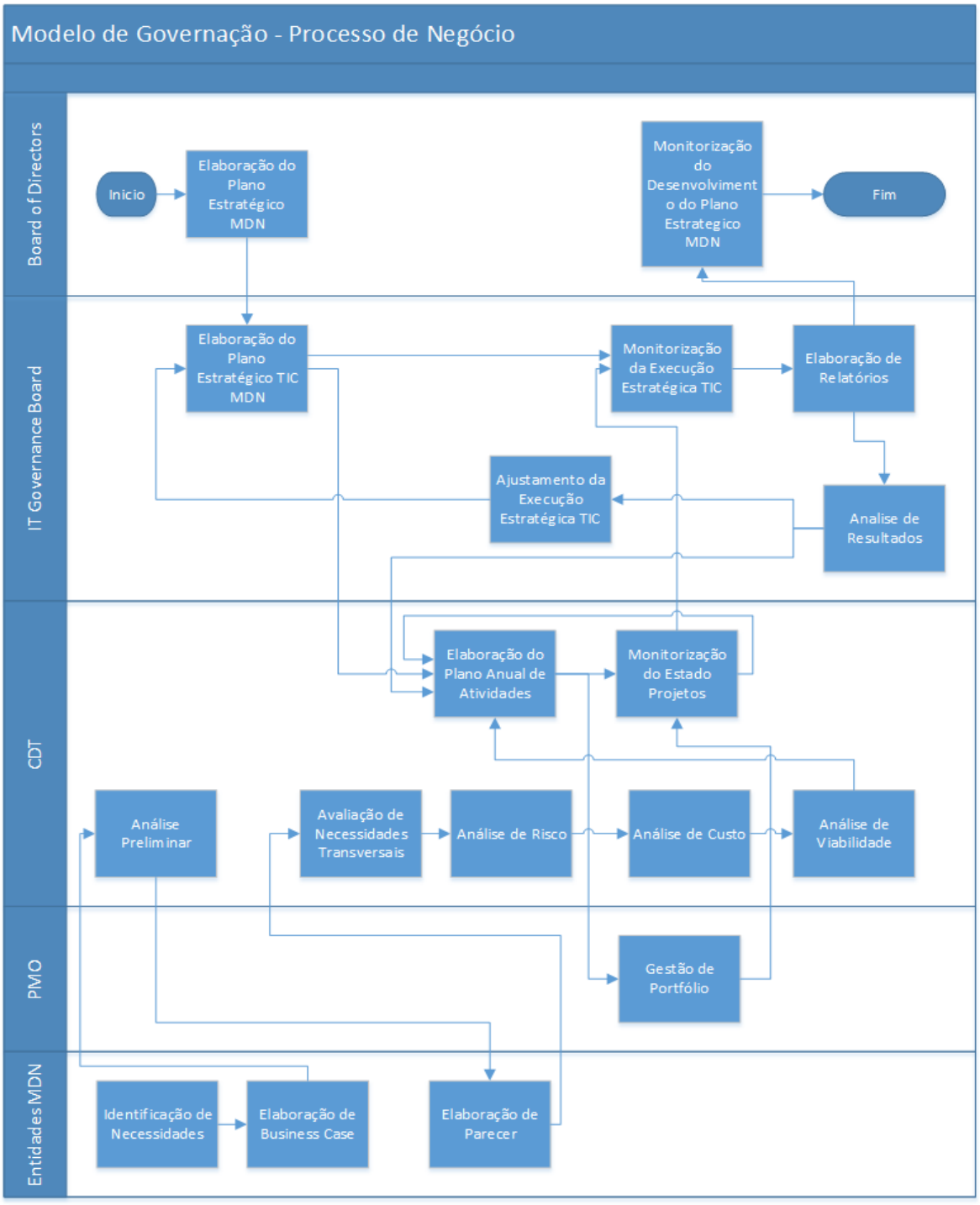


Figura 21 – Processo de Negócio do Modelo de Governação

Fonte: (autor, 2017)

b. Processos

- EDM01 – Garantir a Definição e Manutenção do Modelo de Governança

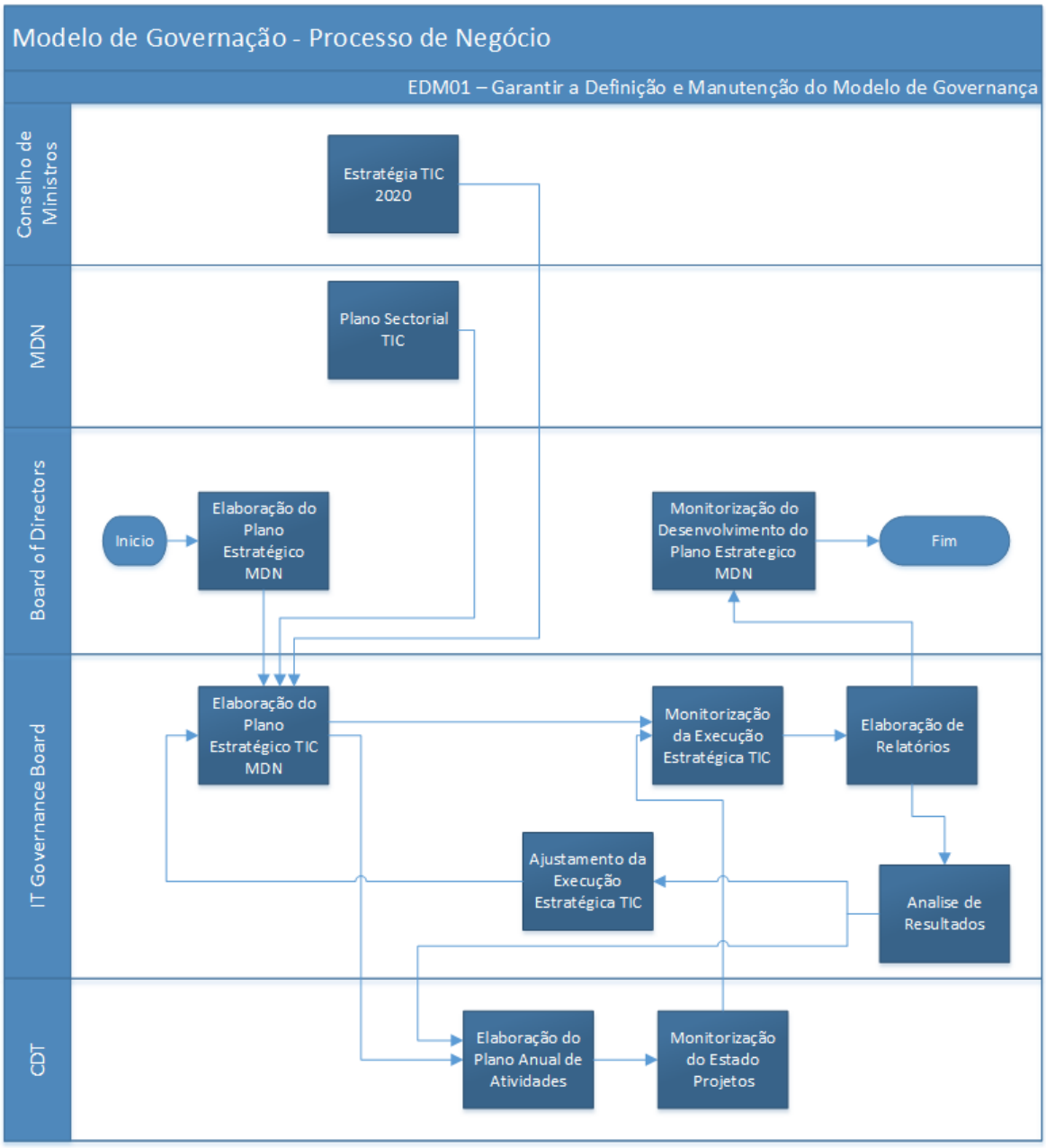


Figura 22 – Atividades do EDM01 incluídas no Processo de Negócio do Modelo de Governação

Fonte: (autor, 2017)

O processo será iniciado com a Elaboração do Plano Estratégico do MDN. Este documento deverá ser elaborado no início do mandato do Ministro da Defesa Nacional e tem como objetivo definir os Objetivos Estratégicos a atingir no MDN. Como consequência será elaborado, no âmbito do *IT Governance Board*, o Plano Estratégico para as TIC, onde serão definidos os Objetivos Estratégicos para as TIC no MDN, as linhas de Ação, as metas a atingir, os Indicadores, e o Planeamento Financeiro. Este documento será

elaborado de forma a cumprir com as diretivas Estratégia TIC 2020, definido pelo CTIC, e pelo Plano Setorial TIC definido pelo MDN. Este documento será elaborado sempre que for definido um novo Plano Estratégico para o MDN.

A Monitorização da Execução Estratégica TIC é uma atividade que deverá decorrer de forma anual, para avaliação da performance do modelo de governação. Após cada avaliação será identificada a necessidade de implementar medidas de correção do modelo de governação a longo prazo. Será também será realizado um relatório que apresenta o estado da Execução Estratégica TIC, e onde se poderá consultar a taxa de execução das linhas de ação através dos indicadores definidos, e o impacto do investimento realizado na organização. Os relatórios deverão ser enviados para o *Board of Directors* (BoD), que irá realizar a Monitorização do Desenvolvimento do Plano Estratégico do MDN.

Após a Elaboração do Plano Estratégico será elaborado o Plano Anual de Atividades que tem como objetivo e materialização das Linhas de Ação em Projetos com o objetivo da concretização dos Objetivos Estratégicos. O Plano Anual de Atividades do ano seguinte deverá ocorrer no final do segundo semestre de cada ano.

O Plano de Atividades é um documento vivo, e que deverá ser ajustado à necessidades contextuais. No Portefólio de Projetos será possível identificar os projetos que integram o Plano de Atividades em cada momento.

A cada trimestre deverá ocorrer uma Atividade de Monitorização do estado de execução dos projetos.

- EDM02 – Garantir a Realização de Benefícios

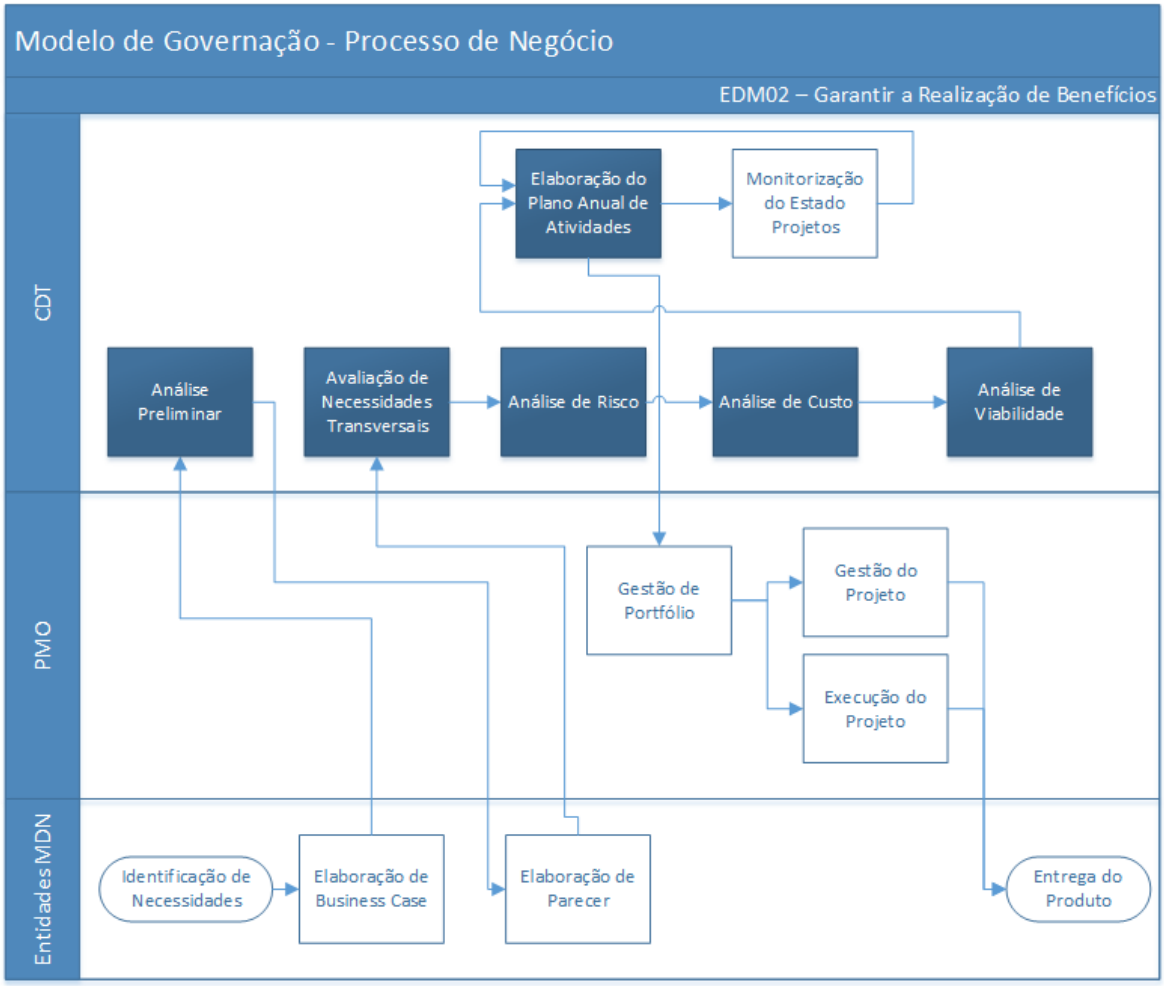


Figura 23 – Atividades do EDM02 incluídas no Processo de Negócio do Modelo de Governação

Fonte: (autor, 2017)

A Realização de Benefícios para o negócio do MDN será obtida através da realização de um conjunto de atividades, identificados na Figura 23, que fazem parte do processo de negócio modelo de governação.

Após ser identificada uma Necessidade para Edificação ou alteração de um sistema, por parte de uma entidade do MDN e com base num Business Case simplificado, será elaborada uma Análise Preliminar por parte do CDT. Após esta análise será enviado para todas as Entidades do MDN o *Business Case* para elaboração de um parecer. Os pareceres serão enviados para o CDT para uma avaliação das Necessidades transversais ao MDN. Caso a necessidade seja comum às entidades, ou a uma parte substancial das entidades, será elaborada uma Análise de Risco e consequentemente uma Análise de Custo da implementação da necessidade identificada. Após a Análise de Custo será realizada uma Análise de Viabilidade. Caso seja identificada a viabilidade será enviado um Relatório com

toda a informação compilada desde o *Business Case* até à Análise de Viabilidade para que seja introduzido no Plano de Anual de Atividades do Ano seguinte.

- EDM03 – Garantir a Otimização do Risco

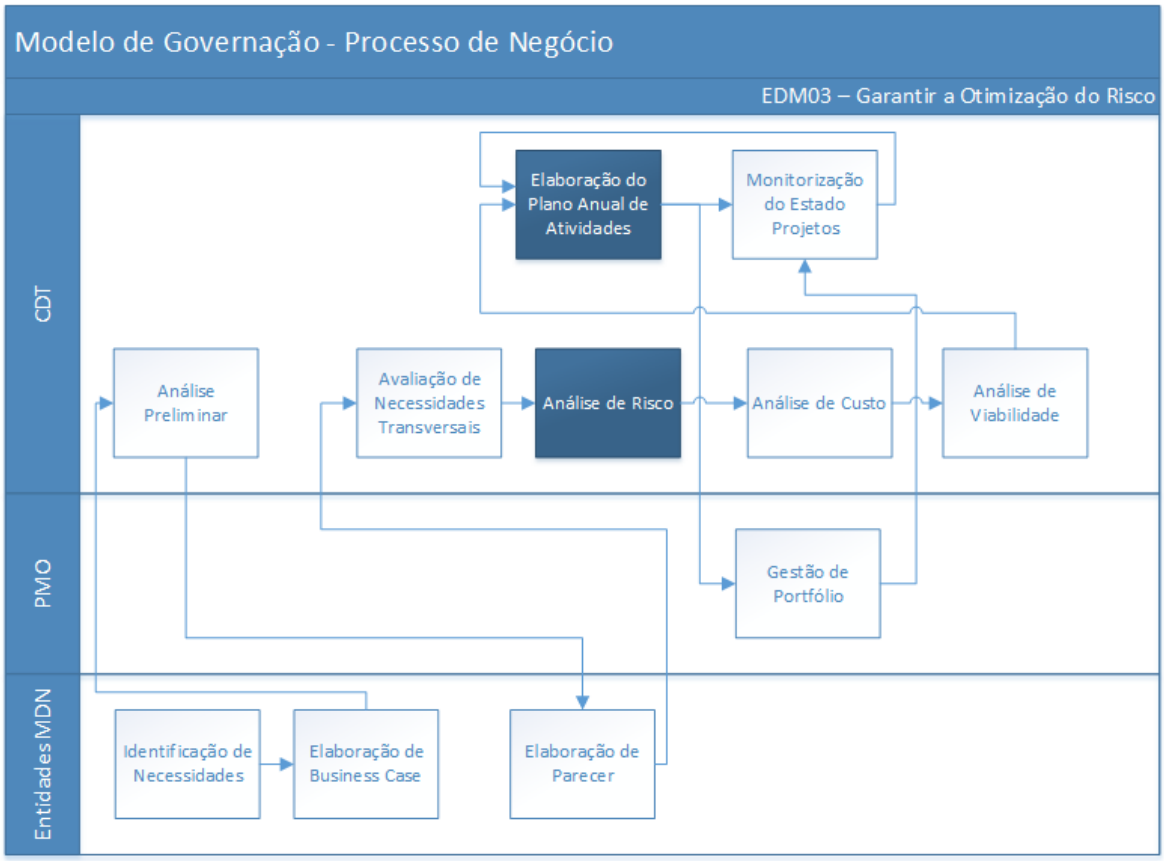


Figura 24 – Atividades do EDM03 incluídas no Processo de Negócio do Modelo de Governação

Fonte: (autor, 2017)

A Otimização do Risco será executado em duas atividades distintas. Numa primeira fase, quando o Plano Anual de Atividades é elaborado, será realizada uma análise do risco de todos os projetos que concorrem para o Plano de Atividades do ano seguinte. O risco dos projetos deverá estar em linha com o risco que o MDN estará disposto a assumir. Numa segunda fase, quando é identificado uma necessidade que poderá dar origem à criação ou alteração de um projeto. O risco será analisado de uma forma mais pormenorizada, pois nesta fase poderá inviabilizar a continuidade deste processo.

- EDM04 – Garantir a Otimização dos Recursos

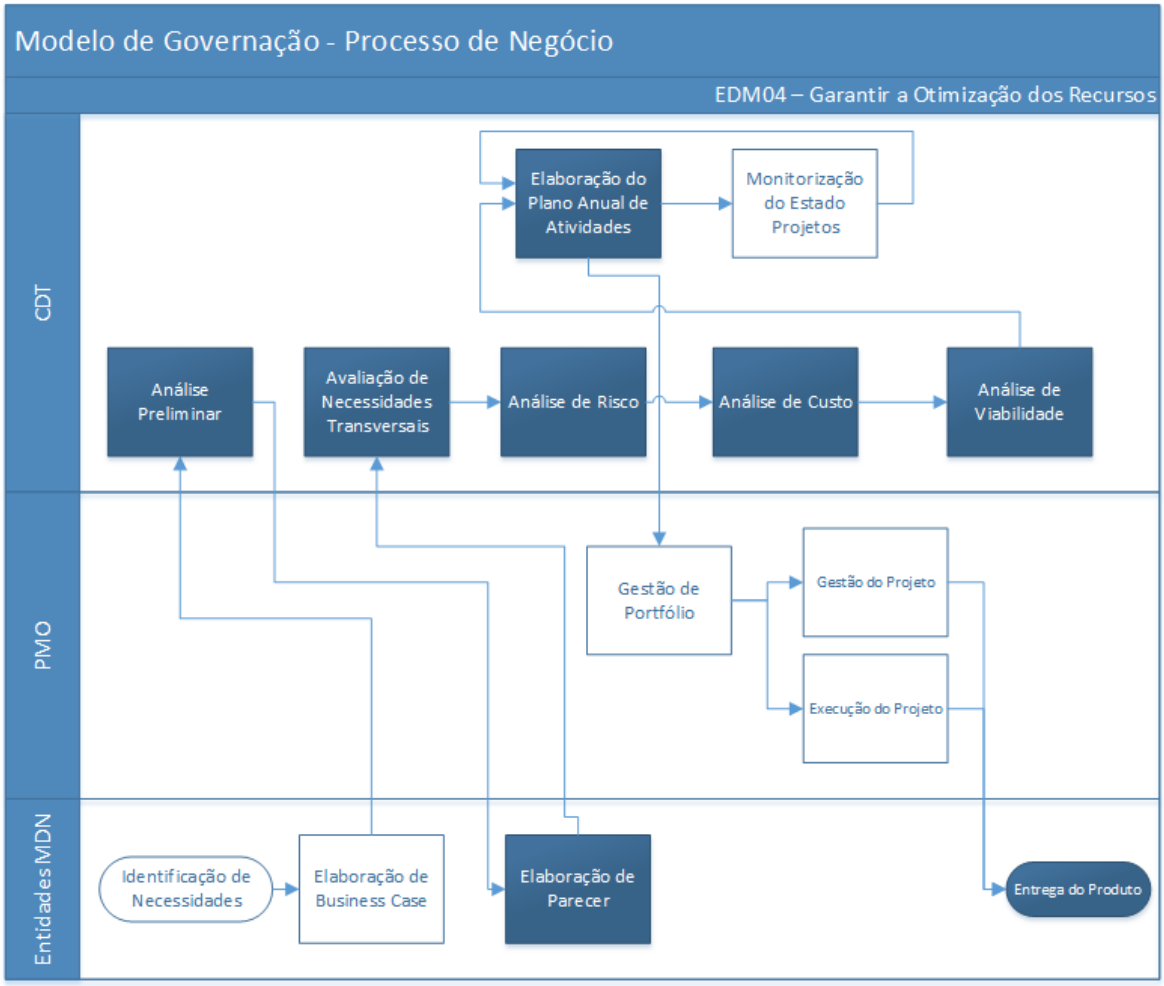


Figura 25 – Atividades do EDM04 incluídas no Processo de Negócio do Modelo de Governação

Fonte: (autor, 2017)

A otimização de recursos é realizada através do mesmo conjunto de atividades do EDM02. A necessidade de envolver as entidades na identificação das necessidades, validação de necessidade comum, e após todo o processo de analise e validação, será implementado o projeto e consequentemente entregue o produto do mesmo ás entidades para sua exploração. A execução de projetos que tenham interesse comum tem como objetivo a otimização dos recursos, pois estes serão apenas utilizados aquando da identificação de uma necessidade comum.

- EDM05 – Garantir a Transparência para as Partes Interessadas

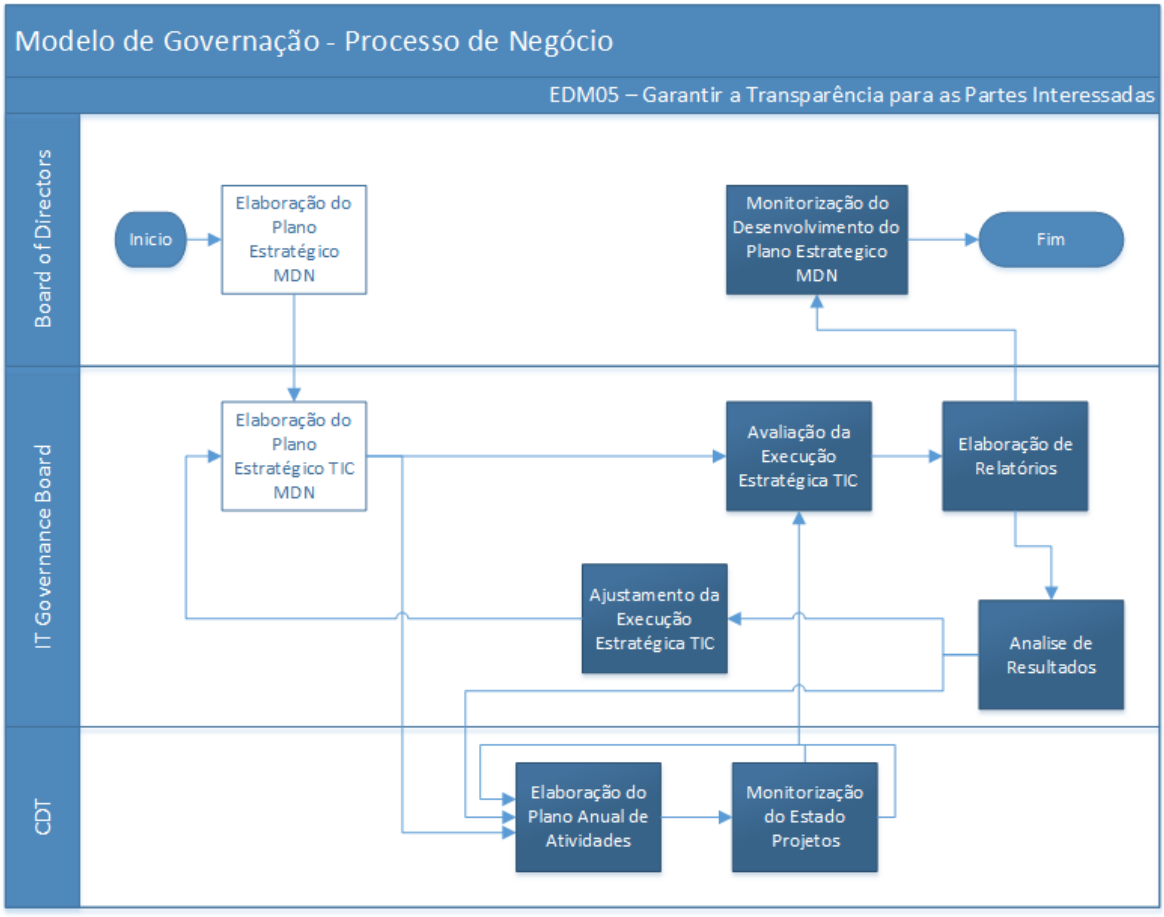


Figura 26 – Atividades do EDM05 incluídas no Processo de Negócio do Modelo de Governação

Fonte: (autor, 2017)

A transparência para todas as partes interessadas será garantida através da utilização de mecanismos que garantam o acesso à informação que faz parte do processo de decisão.

A informação do Estado dos projetos será utilizada para a Avaliação da Execução Estratégica TIC, que consequentemente dará origem a Relatórios de para o BoD realizar a monitorização do Desenvolvimento do Plano Estratégico do MDN. Os Relatórios serão também utilizados para realizar uma Análise dos Resultados e desta forma contribuir para o Plano Anual de Atividades do Ano seguinte.

2. Estrutura Organizacional do Modelo de Governação

O objetivo desta seção é a descrever da Estrutura Organizacional prevista no Modelo de Governação.

a. Organograma

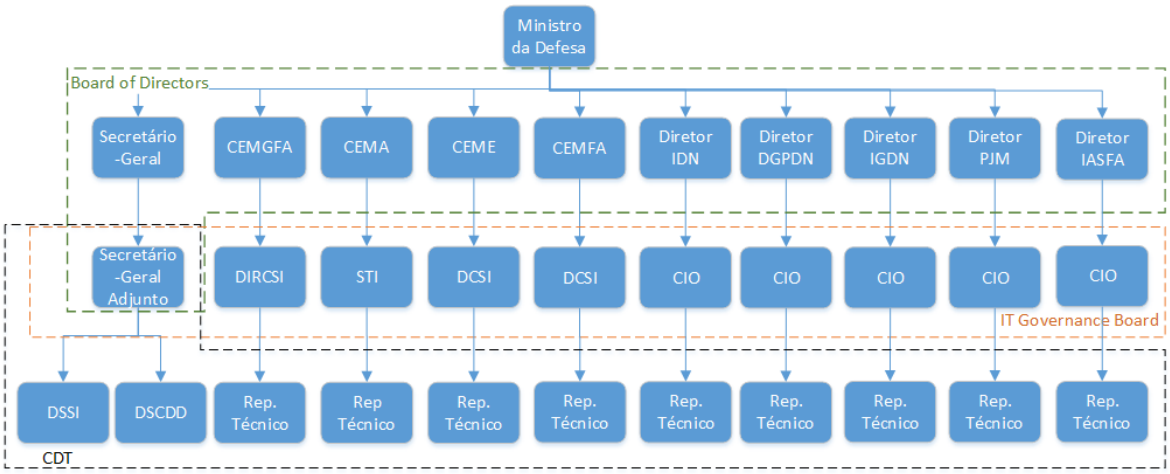


Figura 27 – Estrutura da Governação

Fonte: (autor, 2017)

Na Figura 27 encontra-se definida a Estrutura Organizacional do Modelo de Governação das TIC da DN. Neste Organograma encontram-se todos os organismos do MDN, e chefiado pelo Ministro da Defesa Nacional. Do ponto de vista funcional na área das TIC, foram definidos três níveis de decisão:

- *Board of Directors*, composto pelo Secretário-Geral, Secretário-Geral Adjunto, CEMGFA, Chefes dos Ramos e Diretores/Chefes dos organismos que compõem os Serviços Centrais MDN
- Comissão de Politicas e Auditoria do Sistema de Informação da Defesa Nacional, composto pelo Secretário-Geral Adjunto, e os repetivos CIO do CEMGFA (DIRCSI) e dos Ramos (STI, VCEME e Comando da Logistica da FA) e CIO de cada Organismo que compõem os Serviços Centrais MDN
- Comissão Direção Técnica, composto pelo Secretário-Geral Adjunto, Diretor da DSSI, Diretor do CDD, representantes técnicos do CEMGFA, dos Ramos e dos organismos que compõem os Serviços Centrais MDN

O CIO do MDN é o Secretário-Geral Adjunto.

2. *Stakeholders* e Responsabilidades da Governação

O objetivo desta seção é a descrever que s*takeholders* estão envolvidos e quais as responsabilidades previstas no Modelo de Governação.

a. Orgãos e Participantes

A Tabela 2 apresenta que comissões estão previstas nos modelos de Governação, os seus participantes e as respetivas responsabilidades.

Tabela 2 – Órgãos de Governação

Nivel Organiz.	Orgão/Estrutura	Participantes	Responsabilidade	Dependencia
Senior	*Board Of Directors*	Secretário-Geral, Secretário-Geral Adjunto, CEMGFA, Chefes dos Ramos e Diretores/Chefes Serviços Centrais MDN e IASFA	Definição das Politicas das TIC na Defesa Nacional	Reporta ao MDN
	IT Governance Board	Secretário-Geral Adjunto, CIO do CEMGFA (DIRCSI) e dos Ramos (STI, DCSI e DCSI) e CIO de cada Serviço Central do MDN e IASFA	Determinação das responsabilidades da governação, definição da visão e estratégia das TIC	Reporta ao BoD
Intermédia	Comissão Direção Técnica	Secretário-Geral Adjunto, Dir. DSSI, Dir. CDD, Representante do CEMGFA, dos Ramos, Representantes dos Serviços Centrais MDN e IASFA	Determinação do Plano Anual de Atividades, Análise e monitorização dos Projetos TIC	

Fonte: (autor, 2017)

b. Matriz de Responsabilidades

A matriz de responsabilidades apresenta a relação entre cada uma das atividades definidas no processo de negócio do Modelo de Governação e cada um dos atores.

As responsabilidades estão categorizadas em *Responsible* (R), *Accountable* (A), *Consulted* (C) e *Informed* (I):

R: Responsável pela execução da atividade;

A: Dono da atividade;

C: Deve ser consultado, participar da decisão ou na atividade;

I: Deve ser informado da execução de uma atividade.

Tabela 3 – Matriz de Responsabilidades

Stakeholders / Atividades	Ministro da Defesa Nacional	Secretário-Geral	CEMGFA	CEMA	CEME	CEMFA	Diretor IDN	Diretor DGPDN	Diretor IDN	Diretor PJM	Secretário-Geral Adjunto	DIRCSI	STI	VCEME	CL	CIO IDN	CIO DGPDN	CIO IDN	CIO PJM	Dir. DSSI	Dir. CDD	Rep. Técnico Orgenismo X	Rep. Orgenismo X
Elaboração do Plano Estratégico MDN	A	C	C	C	C	C	C	R	C	C	C												
Monitorização do Desenvolvimento do Plano Estratégico MDN	A	C	C	C	C	C	C	R	C	C	C												
Elaboração do Plano Estratégico TIC MDN		I	I	I	I	I	I	I	I	I	A/R	C	C	C	C	C	C	C	C				
Monitorização da Execução Estratégica TIC		I	I	I	I	I	I	I	I	I	A/R	C	C	C	C	C	C	C	C				
Elaboração de Relatórios		I	I	I	I	I	I	I	I	I	A/R	C	C	C	C	C	C	C	C				
Análise de Resultados		I	I	I	I	I	I	I	I	I	A/R	C	C	C	C	C	C	C	C				
Ajustamento da Execução Estratégica TIC		I	I	I	I	I	I	I	I	I	A/R	C	C	C	C	C	C	C	C				
Elaboração do Plano Anual de Atividades											A/R									C	C	C	
Monitorização do Estado Projetos											A/R									C	C	C	
Análise Preliminar											A/R									C	C	C	
Avaliação de Necessidades Transversais											A/R									C	C	C	
Análise Risco											A/R									C	C	C	
Análise Custo											A/R									C	C	C	
Análise de Viabilidade											A/R									C	C	C	
Identificação de Necessidades																							R
Elaboração de Business Case																							R
Elaboração de Parecer																							R

Fonte: (autor, 2017)