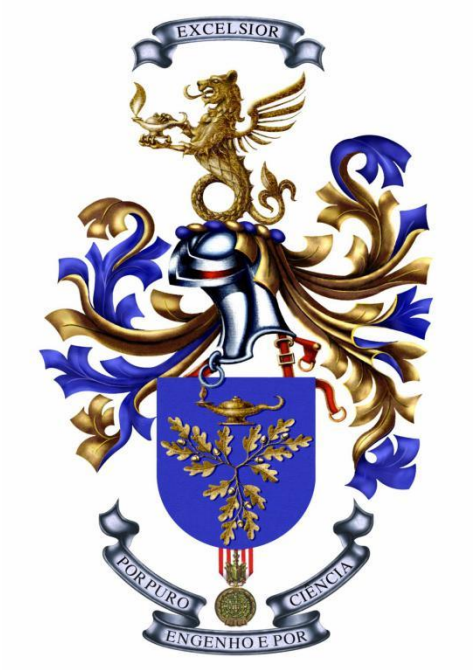
INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2019/2020



TII

IMPLEMENTAÇÃO DE UMA REDE DE DADOS ÚNICA NA DEFESA

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

Rui Fernando da Costa Ferreira

CORONEL ENGENHEIRO ELETROTÉCNICO

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

IMPLEMENTAÇÃO DE UMA REDE DE DADOS ÚNICA NA DEFESA

COR ENGEL Rui Fernando da Costa Ferreira

Trabalho de Investigação Individual do CPOG

Pedrouços 2020

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

IMPLEMENTAÇÃO DE UMA REDE DE DADOS ÚNICA NA DEFESA

COR ENGEL Rui Fernando da Costa Ferreira

Trabalho de Investigação Individual do CPOG

Orientador: CMG EMA Luís Eduardo Moita Rodrigues

Pedrouços 2020

Declaração de compromisso Antiplágio

Eu, Rui Fernando da Costa Ferreira, declaro por minha honra que o documento intitulado "Implementação de uma rede de dados única na Defesa" corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do CPOG 2019/2020 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, 2 de junho de 2020

Rui Fernando da Costa Ferreira

Assinado por : **RUI FERNANDO DA COSTA FERREIRA**
Num. de Identificação: BI08551536
Data: 2020.06.02 20:30:09+01'00'

CHAVE MÓVEL

Agradecimentos

Um trabalho de investigação não é um ato solitário e o que aqui é apresentado é um excelente exemplo disso. Sem a colaboração de todos os quantos que com a sua prestimosa ajuda contribuíram para a sua realização, não teria sido possível concluí-lo.

Assim, gostaria de agradecer a colaboração dos elementos do EMGFA/DIRCSI, destacando o seu Diretor, General João Rocha, que desde o primeiro dia acompanho na Força Aérea, o Coronel Manuel Vinhas e o Tenente-coronel Hélder Guerreiro, que foram essenciais para estabelecer as linhas orientadoras do trabalho.

Agradeço também, à Coronel Ana Telha, da Força Aérea, ao Coronel Tirocinado Carlos Ribeiro, do Exército, e ao Capitão-de-mar-e-guerra Cancela Roque, da Marinha, pela abertura demonstrada e toda a ajuda prestada.

Agradeço ainda a todos os que generosamente dispensaram o seu tempo a responder às questões das entrevistas e que foram fundamentais para o trabalho.

Deixo um especial agradecimento a todos os restantes Auditores do Curso de Promoção a Oficial General 2019/2020, pelo excelente espírito de camaradagem reinante e pelos laços de amizade que certamente subsistirão.

Por último, agradeço aos docentes do IUM, e em especial ao meu orientador Capitão-de-mar-e-guerra Moita Rodrigues, por toda a ajuda e disponibilidade demonstradas.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

As Tecnologias de Informação e Comunicação são um recurso básico e vital para as organizações. São elas que permitem a comunicação, processamento, armazenamento, e tratamento da informação. Pela importância de que se revestem é essencial garantir a sua disponibilidade, fiabilidade e segurança.

Nesse sentido, este estudo foi realizado com o objetivo de propor a implementação de uma rede de dados única na Defesa.

Adotou-se um posicionamento epistemológico interpretativo, tendo-se usado o método indutivo e uma estratégia qualitativa, com recurso ao estudo de casos e recolha de dados através de análise documental e entrevistas semiestruturadas.

Constatou-se que tal como existia nos casos da NATO e da Espanha, e que as levou a realizar programas de modernização, as entidades da Defesa Nacional possuem redes de dados próprias, com arquiteturas diferentes e independentes, com os problemas daí inerentes.

Em resultado, com base nos aspetos comuns das soluções adotadas pela NATO e Espanha, apresenta-se a proposta de uma rede de dados única na Defesa Nacional, com fornecimento centralizado de serviços comuns de cariz administrativo, classificação até ao grau de Reservado, e abrangendo todas as entidades desse universo. Com esta rede de dados única perspetiva-se uma maior interoperabilidade, racionalização de recursos, melhorando a operacionalidade.

Palavras-chave:

Redes de dados da Defesa, Tecnologias de Informação e Comunicações, *Information Technology*.

Abstract

Information and Communication Technologies are a basic and vital resource for any organization. They provide communications, information processing, storage, and treatment. Due to their importance, it is essential to guarantee their availability, reliability, and security.

Having that in mind, this study was carried out with the objective of proposing the implementation of a single data network for the Defense.

In this investigation, an interpretative epistemological position was adopted, using an inductive method and a qualitative strategy, with case study research, and data collection through document analysis and conducting semi-structured interviews.

It was found that, like it happened with NATO and Spain, and made them implement modernization programs, the different National Defense entities have their own data networks, with different and independent architectures and the inherent problems caused by that.

As result, a unique data network for the National Defense was proposed, based on the common aspects of the solutions adopted by NATO and Spain, with administrative services provided centrally, classification up to the level of Restricted, and covering all entities. With this unique data network, greater interoperability and rationalization of resources are foreseen, and an operationally increment.

Keywords

Defense data network, Information and Communication Technologies, Information Technology.

Lista de abreviaturas, siglas e acrónimos

AP	Administração Pública
CD	Centro de Dados
CE	Comissão Europeia
CDC	Cento de Dados Corporativo
CDD	Centro de Dados da Defesa
COC	Centro de Operações Central
CESTIC	*Centro de Sistemas y Tecnologías de la Información y las Comunicaciones*
CPOG	Curso de Promoção a Oficial General
CTIC	Conselho para as Tecnologias de Informação e Comunicação na Administração Pública
DCSI	Direção de Comunicações e Sistemas de Informação
DIRCSI	Direção de Comunicações e Sistemas de Informação do Estado-Maior-General das Forças Armadas
DITIC	Direção de Tecnologias de Informação e Comunicações
DIVCSI	Divisão de Comunicações e Sistemas de Informação
DN	Defesa Nacional
DSCDD	Direção de Serviços do Centro de Dados da Defesa
EMGFA	Estado-Maior-General das Forças Armadas
EMFA	Estado-Maior da Força Aérea
FFAA	Forças Armadas
GPTIC	Grupo de Projeto para as Tecnologias de Informação e Comunicação
IaaS	*Infrastructure as a Service*
I3D	*Infraestructura Integral de Información para la Defensa*
IT	*Information Technology*
ITM	*Information Technology Modernization*
IUM	Instituto Universitário Militar
LAN	*Local Area Network*
MDE	*Ministerio de Defensa de España*
MDN	Ministério da Defesa Nacional
NAF	NATO *Architecture Framework*
NATO	*North Atlantic Treaty Organization*
NCIA	*NATO Communications and Information Agency*

NEP/INV	Norma de Execução Permanente/Investigação
OE	Objetivo Específico
OG	Objetivo Geral
PAS	Plano de Ação Setorial
PECIS	*Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa*
PGETIC	Plano Global Estratégico de racionalização e redução de custos nas Tecnologias de Informação e Comunicação, na Administração Pública
QC	Questão Central
QD	Questão Derivada
RCM	Resolução do Conselho de Ministros
RFCM	Rede Fixa de Comunicações Militares
RH	Recursos Humanos
RHV	Recursos Humanos e Vencimentos
SGMDN	Secretaria-Geral do Ministério da Defesa Nacional
SI	Sistema de Informação
SICOM	Sistema Integrado de Comunicações Militares
SIGDN	Sistema Integrado de Gestão da Defesa Nacional
SUBCEMFA	Subchefe do Estado-Maior da Força Aérea
TIC	Tecnologias de Informação e Comunicação
TII	Trabalho de Investigação Individual
UE	União Europeia
WAN	*Wide Area Network*

1. Introdução

As Tecnologias de Informação e Comunicação (TIC), são um recurso basilar, crítico e fulcral para as organizações e sobretudo para a Defesa Nacional (DN), onde se incluem as Forças Armadas (FFAA).

Na DN, a utilização das TIC vai desde os aspetos administrativos, comuns a qualquer organização, até ao seu uso pelas FFAA a nível operacional. Se a nível administrativo se ambiciona que tenham a máxima eficiência com o menor custo, a nível operacional pretende-se que possibilitem conseguir superioridade de informação nas operações, autonomia e liberdade de ação.

De forma a garantir uma utilização e exploração eficiente, eficaz e segura das TIC, é necessário que as redes de dados em que elas assentam possuam redundância, resiliência, alta disponibilidade e segurança.

Como qualquer outro sistema, as redes de dados têm diversos custos associados, não só financeiros, mas também de Recursos Humanos (RH), necessários para a assegurar a sua implementação, garantir o seu funcionamento e constante atualização ao longo do ciclo de vida.

Devido à evolução tecnológica a que se tem assistido na área das TIC, os RH que lhes estão alocados, necessitam cada vez mais de estarem habilitados com conhecimentos técnicos bastante específicos e diferenciados.

Tendo em conta que os orçamentos são naturalmente limitados, não sendo disso exceção o universo da DN, torna-se essencial garantir que os recursos disponíveis são utilizados da forma mais racional e com a máxima eficácia.

Para além da questão dos recursos, outros aspetos, como a segurança e a interoperabilidade, revelam ser de uma enorme importância. Como reflexo disso, verifica-se que existiram várias determinações governamentais e iniciativas da União Europeia (UE) no sentido de as incentivar e potenciar (Comissão das Comunidades Europeias, 2005; Grupo de Projeto para as Tecnologias de Informação e Comunicação [GPTIC], 2011).

No presente trabalho pretende-se avaliar as soluções que estão a ser utilizadas na DN, no que toca às redes de dados. O tema em investigação é relevante para a DN na perspetiva de analisar a presente situação e avaliar se existem razões para considerar a proposta de adoção de uma rede de dados única, para permitir obter uma maior interoperabilidade, racionalização de recursos e economia de meios, melhorando a operacionalidade.

O objeto da presente investigação são as redes de dados da DN, em particular a forma como estas se encontram implementadas atualmente.

Este estudo, conforme o preconizado no Decreto-Lei n.º 249/2015 de 28 de outubro, enquadra-se no âmbito das Ciências Militares na área das Técnicas e Tecnologias Militares, subárea de Comando, Controlo, Comunicações, Computadores e Informação. Tendo sido seguida a adaptação da norma da *American Psychological Association* efetuada pelo Instituto Universitário Militar (IUM) (Fachada, Ranhola, Marreiros, & Santos, sem data).

A investigação foi delimitada em termos de tempo, espaço e conteúdo, de acordo com o preconizado por Santos & Lima (2019, p. 42).

Assim, em termos de delimitação de espaço, e tendo em conta a sinopse do tema, a investigação foi cingida ao âmbito das entidades que constituem o universo da DN. Nestas, consideraram-se:

- O Ministério da Defesa Nacional (MDN): os serviços centrais e as entidades dele dependentes (Decreto-Lei n.º 183/2014, de 29 de dezembro, 2014);
- O Estado-Maior-General das Forças Armadas (EMGFA) e os órgãos na dependência direta do Chefe do Estado-Maior-General das Forças Armadas (Decreto-Lei n.º 184/2014, de 29 de dezembro, 2014);
- Os três ramos: Marinha (Decreto Regulamentar n.º 10/2015, 2015), Exército (Decreto Regulamentar n.º 11/2015, de 31 de julho, 2015) e Força Aérea (Decreto Regulamentar n.º 12/2015, de 31 de julho, 2015).

Em termos de delimitação temporal considerou-se a forma como as redes de dados estavam implementadas pelos diversos atores alvos de estudo na altura da realização da investigação (ano de 2020).

Em termos de conteúdo, por limitações temporais da investigação, somente se consideraram as redes não classificadas e os serviços comuns de cariz administrativo utilizados por todas as entidades do universo da DN, não se abordando as redes seguras e os serviços de comando e controlo militar por serem específicos dos ramos das FFAA e EMGFA.

A presente investigação foi conduzida de forma a conseguir-se cumprir o Objetivo Geral (OG) indicado no Quadro 1. Também no mesmo Quadro são especificados os Objetivos Específicos (OE) que se pretendem completar, concorrentes para o OG.

Quadro 1 − Objetivo geral e objetivos específicos

Objetivo Geral
OG − Propor a implementação de uma rede de dados única na Defesa.
Objetivos Específicos
OE1 − Analisar as soluções adotadas pela *North Atlantic Treaty Organization* (NATO) e Espanha em matéria de redes de dados únicas.
OE2 − Analisar a forma como estão implementadas as redes de dados no universo de entidades da Defesa.

Com vista a atingir o OG definido para a presente investigação, pretende-se responder a uma Questão Central (QC) e a duas Questões Derivadas (QD), que são as apresentadas no Quadro seguinte:

Quadro 2 − Questão central e questões derivadas

Questão Central
QC – Que solução pode ser adotada pela Defesa para a implementação de uma rede de dados única?
Questões Derivadas
QD1 − Quais as soluções adotadas pela NATO e Espanha em matéria de redes de dados únicas?
QD2 − Como estão implementadas as redes de dados nas diversas entidades da Defesa?

O presente trabalho de investigação foi elaborado seguindo uma lógica de desenvolvimento sequencial e racional, obedecendo a uma estrutura tipo e conteúdo de artigo científico, conforme definido na Norma de Execução Permanente/Investigação (NEP/INV) "Estrutura e regras de citação e referenciação de trabalhos escritos a realizar no IUM" (NEP/INV 003, 2020).

Para além da presente introdução, constam mais quatro capítulos. No segundo capítulo é apresentado o enquadramento teórico e conceptual sendo descrito o estado da arte e conceitos estruturantes, assim como o modelo de análise utilizado. No terceiro apresenta-se a metodologia e método utilizados. O quarto está destinado à apresentação da análise dos dados, discussão de resultados e a resposta a cada uma das questões derivadas e à questão central de investigação. No quinto e último capítulo serão apresentadas as conclusões, os contributos para o conhecimento, limitações, proposta de estudos futuros e indicadas recomendações.

2. Enquadramento teórico e conceptual

Neste capítulo são apresentados o estado da arte e o modelo de análise.

2.1. Estado da arte e conceitos estruturantes

A partir dos anos sessenta do século XX, as TIC foram sendo cada vez mais utilizadas no universo das entidades da DN. Até ao presente momento passaram por várias fases, desde a informática muito centralizada em torno de *Mainframes*, ao teleprocessamento, ao aparecimento e desenvolvimento da microinformática, à instalação de *Local Area Networks* (LAN) e *Wide Area Networks* (WAN) e à utilização e exploração da *internet* (MDN, 2013).

No entanto, no universo da DN, o desenvolvimento das TIC foi sempre realizado de forma autónoma, e dependeu essencialmente "[…] dos orçamentos disponíveis e da existência nas diferentes entidades dos RH qualificados necessários para a conceção, planeamento, especificação, desenvolvimento, instalação, exploração e manutenção dos sistemas e das tecnologias requeridas para o melhor cumprimento das missões" (MDN, 2013).

Em 2002, após um levantamento, verificou-se que existiam cerca de 13500 utilizadores no universo da DN, com uma grande dispersão geográfica, e que utilizavam cerca de 11000 computadores pessoais. Nesse levantamento verificou-se que existia um *Mainframe* por ramo das FFAA, mais de 300 servidores e uma larga profusão de aplicações distintas. Embora a rede de voz fosse comum através do Sistema Integrado de Comunicações Militares (SICOM), as redes de dados eram autónomas e sem interligação física. Com exceção dos sistemas de comunicações operacionais, não existia qualquer integração ou interoperabilidade das TIC entre as entidades da DN (MDN, 2013).

A Rede Fixa de Comunicações Militares (RFCM), que integrou o SICOM, é a atual infraestrutura de transporte de dados e interliga as entidades do universo da DN (M. C. Vinhas, entrevista presencial, 5 de dezembro de 2019).

A nível da DN, em 2003, foi adotada uma política integradora no âmbito dos sistemas de gestão e administração. Pretendia-se que a integração e a interoperabilidade das TIC entre as diversas entidades do MDN, permitissem ganhos de eficiência operacional, melhoria dos níveis de qualidade de serviço, racionalização de recursos e redução dos orçamentos. Como um dos pilares dessa política, em 2004, deu-se início ao desenvolvimento do Sistema Integrado de Gestão da Defesa Nacional (SIGDN), com o objetivo de ser utilizado por todo o universo da DN (MDN, 2013). À data da elaboração deste estudo, o SIGDN é transversal à DN, está em pleno funcionamento, e comporta vários módulos: orçamental, financeiro,

logístico e o de Recursos Humanos e Vencimentos (RHV), ainda em consolidação (R. A. Francisco, entrevista por *email*, 18 de maio de 2020).

Desde 2005, e até ao momento da elaboração do presente estudo, existiram várias iniciativas com vista a racionalizar e otimizar as TIC a nível nacional, incluindo o universo da DN (Apêndice A).

Considerando o Conceito Estratégico da Defesa Nacional, este preconiza como um dos objetivos nacionais conjunturais: "A racionalização e rentabilização de recursos, mediante o desenvolvimento de capacidades civis e militares integradas." (Resolução do Conselho de Ministros [RCM] n.º 19/2013, de 21 de março, 2013, p. 1988), nas quais se incluem as TIC.

Em termos dos casos selecionados para estudo, quando a *NATO Communications and Information Agency* (NCIA) foi constituída, herdou todos os ativos de *Information Technology* (IT) existentes. De forma a conhecer a realidade herdada, foi realizado um estudo, em conjunto com a indústria, com o objetivo de efetuar a sua avaliação. Desse estudo resultou que a modernização das infraestruturas IT poderia trazer ganhos significativos (NCIA, 2017). De forma a conseguir esses ganhos, a NCIA desenvolveu uma estratégia com vista a melhorar as infraestruturas e fornecer serviços de alta qualidade, robustos, padronizados e económicos (Edwards, Mikla, & Sokolowski, 2016; NATO Communications and Information Agency, 2017).

A estratégia desenvolvida pela NCIA constitui o programa *Information Technology Modernization* (ITM), com os seguintes objetivos (NCIA, 2017):

- Simplificar as ofertas de serviços, aumentando a eficiência e a eficácia das TIC da NATO;
- Aumentar a flexibilidade e escalabilidade dos serviços TIC;
- Fornecer serviços a partir de locais centralizados, otimizando a utilização de recursos (civis e militares);
- Introduzir uma camada comum de gestão das TIC e vigilância de operações, aumentando a governança efetiva;
- Implementar soluções de continuidade de negócio e recuperação de desastre em toda a NATO, propiciando maior segurança e defesa em relação a incidentes ou ciberataques;
- Redução dos custos de operação e com RH, necessários à manutenção e fornecimento de serviços.

A NCIA definiu como objetivo constituir uma *Infrastructure as a Service* (IaaS) privada (Lenk, 2014, p. 3).

Na Figura 1 estão ilustradas três vistas da infraestrutura objetivo da NATO.

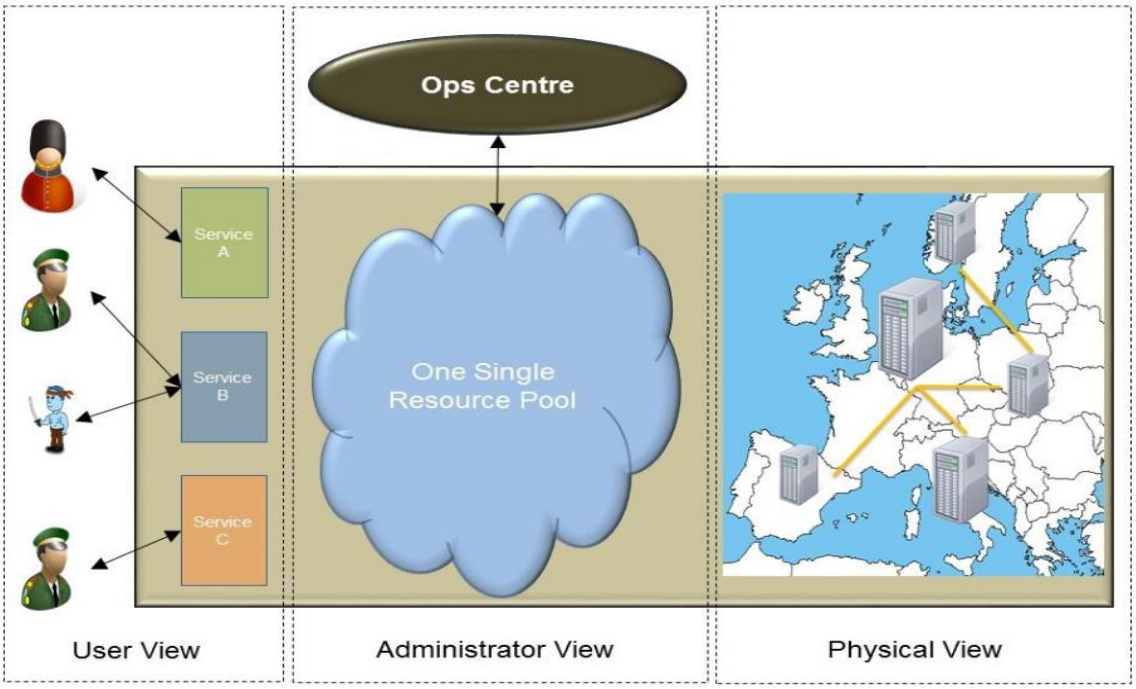


Figura 1 – Infraestrutura tecnológica objetivo da NATO

Fonte: Lenk (2014)

No caso de Espanha, em 2002, foram estabelecidas as primeiras medidas no sentido de implementarem soluções TIC transversais ao *Ministerio de Defensa de España* (MDE) (MDE, 2002).

Em 2015, da avaliação efetuada à implementação das medidas, verificaram que não tinha ocorrido a unificação das redes de comunicações. Na sequência de alterações da organização das suas FFAA e da necessidade de integração das TIC na administração geral do estado, foi estabelecida a política das TIC do MDE (MDE, 2017b).

Em resultado dessa política foi aprovada a arquitetura global das TIC (MDE, 2017a). Esta arquitetura tem bastantes pontos em comum com a solução adotada pela NATO sendo baseada em *cloud computing*, centralizada em centros de dados (CD) redundantes, que permitem a resiliência.

A Figura 2 ilustra a infraestrutura objetivo da Espanha.

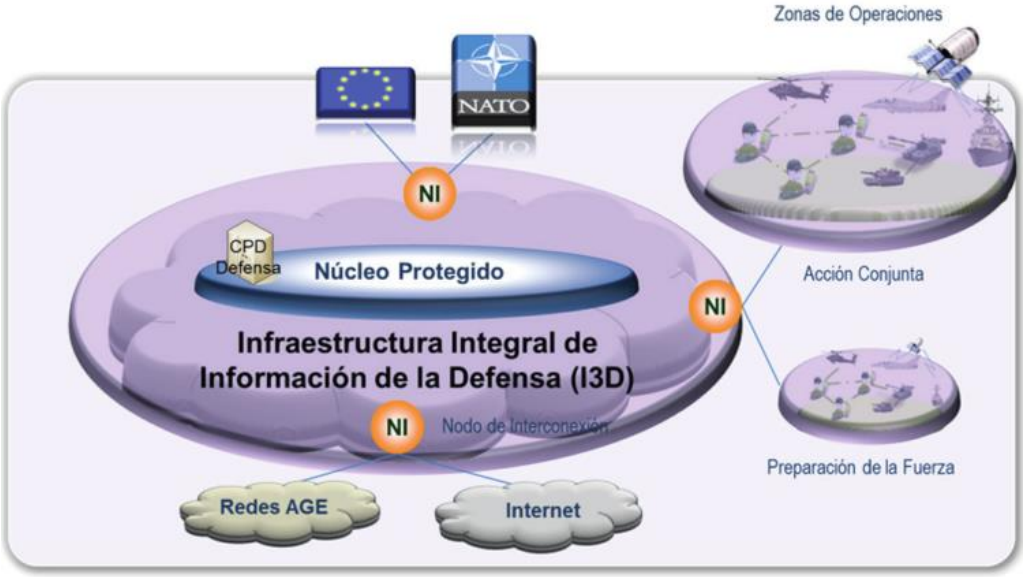


Figura 2 – Infraestrutura TIC objetivo da Espanha

Fonte: MDE (2017a)

A organização fundamental de um sistema pode ser descrita através de uma arquitetura. Essa arquitetura deverá incorporar os diversos componentes do sistema, as relações entre estes, o ambiente e os princípios que guiam o seu desenho e evolução. A arquitetura é um conjunto consistente de princípios, métodos e modelos usados no desenho e materialização da estrutura organizacional, processos de negócios, Sistemas de Informação (SI) e infraestrutura (North Atlantic Council, 2008).

O objetivo de uma arquitetura organizacional é possibilitar o apoio à decisão, no âmbito da estratégia da organização. Alinha a orientação de alto nível com o planeamento estratégico, a organização, a governação, os processos de negócio, os SI e a tecnologia de suporte. (Estado-Maior da Força Aérea [EMFA], 2015)

A NATO definiu a *Architecture Framework* (NAF), que indica as regras, a orientação e as descrições dos produtos para desenvolver, apresentar e comunicar arquiteturas. A NAF serve como denominador comum para entender, comparar e integrar arquiteturas. A aplicação do *framework* permite que as arquiteturas contribuam de forma mais eficaz para a aquisição e implementação de capacidades militares interoperáveis (NATO, 2019).

Na Figura 3 apresenta-se uma arquitetura de referência dos SI/TIC, adaptada da NAF:

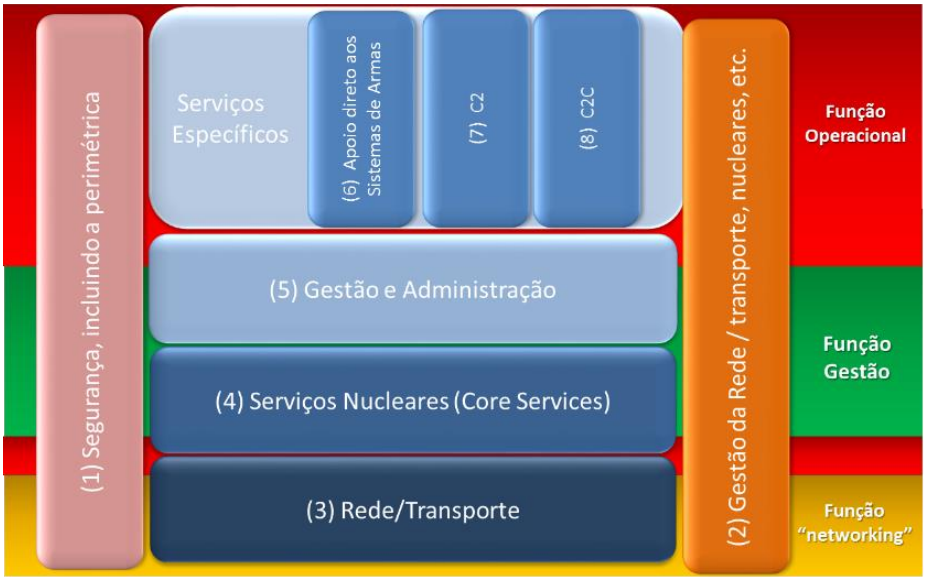


Figura 3 – Arquitetura de referência dos SI/TIC

Fonte: EMFA, 2015

Decorrente dos objetivos e questões da presente investigação, verifica-se que Rede de Dados sobressai como conceito estruturante. Este conceito está patente na sinopse do tema do trabalho de investigação proposto, mas não é um conceito padrão. No presente trabalho como Redes de Dados, tendo em conta a arquitetura atrás referida, consideram-se as infraestruturas tecnológicas, recursos, SI e serviços necessários para a existência, operação e gestão de um ambiente de TIC ou IT corporativo, que permite fornecer soluções e serviços aos utilizadores.

2.2. Modelo de análise

O modelo de análise seguido encontra-se no Apêndice B.

3. Metodologia e método

A investigação foi desenvolvida de acordo com as orientações metodológicas em vigor no IUM (Santos & Lima, 2019), tendo ainda como referência as NEP/INV 001, 2018, e NEP/INV 003, 2020.

O percurso metodológico, conforme Santos & Lima (2019, pp. 41-154), integrou as seguintes fases:

- Exploratória em que se recorreu à análise documental, entrevistas exploratórias e efetuou-se o enquadramento concetual, formulação do problema, objetivos e perguntas, conforme o modelo de análise disponível no Apêndice B;
- Analítica em que se procedeu à recolha, análise e apresentação dos dados;
- Conclusiva onde foi efetuada avaliação e discussão dos resultados, elaboradas as conclusões, apresentados os contributos para o conhecimento, as limitações, as recomendações e verificada a ética da investigação.

Foi adotado um posicionamento epistemológico interpretativo, no sentido de compreender padrões, sistemas e processos (Santos & Lima, 2019, pp. 16-18).

A investigação foi desenvolvida através do recurso ao método indutivo utilizando uma estratégia qualitativa.

Recorreu-se ao estudo de casos, através da observação das soluções adotadas pela NATO e Espanha.

3.1. Participantes e procedimento

Nas entrevistas exploratórias foram contactados vários elementos da Direção de Comunicações e Sistemas de Informação (DIRCSI) do EMGFA.

Contactaram-se elementos da Direção de Comunicações e Sistemas de Informação (DCSI) da Força Aérea, incluindo o Diretor, e a Chefe da Divisão de Comunicações e Sistemas de Informação (DIVCSI) do EMFA.

Na Marinha foi efetuado o contacto com o Diretor da Direção de Tecnologias de Informação e Comunicações (DITIC).

No Exército foi entrevistado o Subdiretor da DCSI.

Na Secretaria Geral do Ministério da Defesa Nacional (SGMDN), o Diretor da Direção de Serviços do Centro de Dados da Defesa (DSCDD).

Nas entrevistas semiestruturadas foram entrevistados, por *email*, todos os elementos anteriores, considerados como sendo do escalão operacional, assim como os respetivos

chefes, diretores e ainda o Subchefe do Estado-Maior da Força Aérea (SUBCEMFA), escalão superior, conforme as listas do Apêndice C.

3.2. Instrumentos de recolha de dados

Para além da análise documental, foram realizadas entrevistas semiestruturadas aos responsáveis pela implementação e gestão das estruturas de redes de dados na DN, com o objetivo de analisar a situação atual e validar a proposta de solução futura.

Foram utilizados dois guiões nas entrevistas conduzidas por *email*. Estes, foram constituídos por uma parte comum, contendo um enquadramento e o objetivo do trabalho, e uma parte com questões, que foram diferentes para o escalão superior e o operacional.

Os guiões de entrevista, e uma síntese da informação mais importante recolhida, encontram-se no Apêndice D.

3.3. Técnicas de tratamento dos dados

Com base na análise qualitativa dos dados recolhidos é proposta uma solução de rede de dados única na DN e as razões pela qual deve ser adotada.

4. Análise dos dados e discussão dos resultados.

Seguidamente, são apresentados e discutidos os dados da investigação. Inicia-se com a caraterização da situação dos casos de estudo, do universo da DN e com base nestes, é apresentada uma proposta de solução futura.

4.1. Soluções adotadas pela NATO e Espanha em matéria de rede de dados

4.1.1. Apresentação dos dados

4.1.1.1. NATO IT Modernization

Para conhecer a situação das estruturas de redes de dados implementadas na NATO, a NCIA encomendou um estudo ao *Network Centric Operations Industry Consortium* e que acabou por dar origem ao programa ITM (Lenk, 2014). Posteriormente o ITM foi incluído como sendo um dos quatro projetos do programa Polaris (Dron, 2019).

Como resultado desse estudo, verificou-se que até então, os investimentos em IT na NATO tinham sido efetuados em pacotes de capacidades, através de projetos e programas individuais, de forma desagregada e, devido à arquitetura distribuída criada, existiam soluções idênticas replicadas em várias localizações. Com a proliferação de recursos por vários locais e devido à quantidade e complexidade dos sistemas, tornou-se necessária mão de obra qualificada adicional para os manter operacionais, o que resultou em custos totais muito elevados. Basicamente, a infraestrutura de IT desenvolveu-se com base em requisitos locais, sem planeamento centralizado, nem uma arquitetura padrão definida. Como resultado existiam múltiplas infraestruturas locais heterogéneas, de difícil e cara manutenção e muito baixa flexibilidade. Existiam infraestruturas altamente redundantes, embora não necessariamente resilientes, onde serviços idênticos eram geridos e apoiados em muitas localizações com diferentes processos, pessoas, *hardware e software*. Foi estimado que somente cerca de 9% da capacidade dos servidores estaria a ser utilizada. Verificaram ainda, que os diversos *sites*[1] não se apoiavam entre si em situações de desastre. Embora fossem efetuados *backups*, em caso de desastre num *site*, não se sabia o tempo que demoraria a repor os dados e serviços. Devido à existência de *software* e *hardware* diferentes, a segurança estava também em risco por ser muito difícil garantir que todas as últimas atualizações estavam instaladas (Lenk, 2014).

[1] *Site* – local que contém diverso *hardware* e *software* da infraestrutura de rede, incluindo servidores.

Com a adoção de soluções centradas em rede poderiam reduzir a quantidade de RH e a dimensão da infraestrutura de IT necessária. O programa ITM deveria ser planeado no sentido de implementar um sistema de prestação de serviços, para serem custeados pelos utilizadores (Lenk, 2014).

O programa ITM teve como objetivo proporcionar uma IaaS privada, baseada em *cloud computing*, para fornecer os serviços necessários à NATO, através de uma infraestrutura única, resiliente, logicamente integrada, geograficamente dispersa e contendo todas as aplicações em utilização. Deveria haver uma camada comum de gestão e controlo, um número limitado de combinações de sistemas operativos e *hardware*, um aumento dos níveis de virtualização e capacidade de recuperação de desastres. Pretendia-se facilitar a sustentação, através da padronização de *software*, de *hardware*, de processos e também das necessidades de formação e de logística (Lenk, 2014).

Em termos físicos, o objetivo foi interligar toda a organização NATO, incluindo a estrutura de comando, a sede e as agências. Teve também como objetivo, abranger dois domínios de segurança, a rede operacional, fornecendo serviços com nível de classificação até NATO Secreto e a rede administrativa protegida, com nível de classificação até NATO Reservado, incluindo acesso à *internet*. A nível técnico, a solução passou por consolidar a infraestrutura de IT em três Centros de Dados Corporativos (CDC) centrais e implantação distribuída de *sites* locais contendo nós padrão ou avançados. Estes CDC deveriam possuir altos níveis de resiliência e ter toda a informação replicada entre eles. A recuperação de desastres deveria ser efetuada centralmente, permitindo restaurar os serviços em curto prazo e com uma perda de dados previsível. Em caso da falha de um CDC ou de um nó avançado, o fornecimento de serviços deveria passar automaticamente a ser efetuado pelos restantes, havendo capacidade de recuperação de desastres transparente e dispersa geograficamente (Lenk, 2014).

Foi ainda, definida a criação de um Centro de Operações Central (COC), com outro como *backup*, para gestão e apoio centralizados de todos os serviços de IT e dos nós locais. Foi previsto que os nós padrão forneceriam apenas um conjunto mínimo de serviços de processamento e armazenamento local, enquanto os nós avançados incluiriam algum nível de processamento e armazenamento, contribuindo para a resiliência, e contendo as aplicações antigas (*legacy*) que não fossem possíveis de adaptar para a nova arquitetura. Foi objetivo efetuar a centralização e padronização das aplicações e serviços, existentes e futuros (Lenk, 2014).

A solução ITM foi planeada com as seguintes caraterísticas (Lenk, 2014):

- Fornecimento de IaaS privada, baseada em *cloud computing*, e capaz de hospedar todas as aplicações, com o objetivo de ser fornecida como um serviço aos utilizadores;
- Implementação de três CDC em Mons, Bruxelas e Lago Patria;
- Inclusão de *sites* locais, de nós padrão, com fornecimento local muito limitado ou inexistente de serviços e nós avançados, com fornecimento local limitado de serviços para contributo da resiliência ou para lidar com aplicações antigas;
- Implementação de um COC em Mons, com capacidade reforçada, fornecendo gestão centralizada de todos os serviços de IT, incluindo a gestão dos nós locais e com um *backup* em local a definir;
- RH ajustados à nova arquitetura, em termos de quantitativos e competências;
- Nas unidades locais, existência de equipas para apoio de primeira linha. No COC, pessoal para apoio de primeira e segunda linha. Linhas de serviço para apoio de segunda e terceira linha;
- Um conjunto de processos e de ferramentas de apoio, para o fornecimento eficiente de IaaS e a correspondente formação quanto à sua utilização;
- Definição da configuração de *hardware* e *software* base para facilitar a gestão e aumentar o apoio, com a renovação dos dispositivos clientes, periféricos e infraestruturas de rede locais, conforme necessário.

A previsão inicial era que se conseguiria centralizar nos CDC 80% de todos os serviços existentes. Os restantes seriam mantidos a nível local e à medida que fossem realizadas atualizações e substituições, deveria proceder-se à sua gradual centralização (Lenk, 2014).

Em termos de implementação, o programa ITM foi previsto ocorrer de forma incremental, em quatro fases e num período de cinco anos. A duração do projeto teve em atenção o tempo médio de vida dos servidores, que é considerado ser cinco anos, pelo que os existentes na NATO iriam já ser todos substituídos nesse período (Lenk, 2014).

A preparação do programa implicou um levantamento de todas as aplicações que existiam nas redes da NATO. Foram catalogadas cerca de 550 aplicações consideradas significativas, das quais cerca de 400 podiam ser eliminadas e somente cerca de 40 específicas NATO, com contributos diretos para as operações. Era objetivo também que se reduzissem os custos com as licenças e com a mão-de-obra de apoio necessária (Lenk, 2014).

O programa ITM não foi idealizado com vista a ter somente benefícios económicos, mas também, permitir a prestação de serviços com maior qualidade aos utilizadores. Na NATO, os RH qualificados de que a operação do IT depende, são cada vez mais escassos e as nações pretendem reduzi-los. Era necessário encontrar soluções para esta redução e o programa ITM foi uma delas (Lenk, 2014).

Os benefícios previstos podem ser agrupados naqueles que contribuem para a eficácia da organização e naqueles que contribuem para a eficiência (Lenk, 2014):

Benefícios em eficácia (Lenk, 2014):

- Resiliência, recuperação de desastres e sustentação. Os dados replicados em três servidores facilitam a recuperação de desastres, aumentando a resiliência. O número menor de configurações de *hardware* e *software*, e de acordo com a arquitetura estabelecida, facilita a sustentação e a evitar a obsolescência;
- Troca de informação. A integração de todas as redes NATO com classificação até ao nível Reservado, facilitará a troca de informação;
- Partilha de serviços. A redução da classificação permitirá facilitar a partilha de serviços;
- Abordagem global. A redução da classificação e a possibilidade de utilização da *internet* facilita a comunicação com entidades externas;
- Flexibilidade e agilidade. A virtualização do processamento, armazenamento e rede, permite flexibilidade na gestão e na alocação de recursos;
- Postura de segurança. A redução da superfície de ataque e a maior padronização facilita a cibersegurança;
- Mobilidade. Maior facilidade de acesso remoto;
- Conformidade com as políticas da NATO. Cumprir com a política de racionalização de infraestruturas de informação, conforme a sua classificação;
- Métricas e testes comparativos. A consolidação da infraestrutura permite contabilizar a qualidade e custos dos serviços.

Benefícios em eficiência para o utilizador (Lenk, 2014):

- Continuidade de operações. A existência dos serviços em múltiplos CDC reduz a probabilidade de interrupção no seu fornecimento, aumentando a resiliência.
- Mobilidade/produtividade. A mobilidade melhora a produtividade.

Benefícios em eficiência para a NCIA (Lenk, 2014):

- Menos redes para gerir. Menos sistemas e instâncias de aplicações para apoiar e menos soluções de gestão a implementar e manter;
- Menos contas de utilizadores. Menor necessidade de armazenamento, processamento, largura de banda etc.;
- Economia de mão de obra. O programa ITM prevê uma menor necessidade de mão-de-obra, sendo este o principal objetivo, com maior prioridade que a redução de custos:
- Sustentação. A padronização e redução dos tipos de *hardware* e *software* utilizados permite reduzir o número de licenças em utilização, os custos de sustentação e os níveis de conhecimentos necessários dos administradores dos sistemas.

Benefícios financeiros em RH.

- Em termos de RH, a previsão era que o ITM iria permitir a redução de 515 lugares nas linhas e unidades de apoio, com a previsão de poupança de 24,5 milhões de euros por ano (Lenk, 2014).

4.1.1.2. Arquitetura IT Espanha

Na Espanha, em 2002, foi aprovado o plano diretor de SI e telecomunicações, que estabelecia a criação de duas redes WAN corporativas. Uma delas para comando e controlo militar, com ligação à NATO, e a outra de uso administrativo geral, ligada ao MDE e incluía acesso à *internet*. Essas redes deveriam estar isoladas fisicamente uma da outra (MDE, 2002).

Esse plano identificava já que a crescente necessidade de pessoal técnico na área das TIC, tornava os RH um recurso crítico, advogando mesmo a necessidade da criação de carreiras próprias e atribuição de incentivos para atração de interessados (MDE, 2002).

Em 2015, verificaram que a rede de suporte dos SI não tinha sido unificada, pelo que consideraram necessário renovar o plano diretor (MDE, 2017b).

Verificaram ainda, que possuíam uma grande diversidade de redes WAN e LAN, CD, sistemas TIC e equipamentos dos utilizadores, que transmitiam, processavam e armazenavam a informação do Departamento de Defesa. Tal situação causava graves disfunções, redundâncias e limitações no acesso à informação. Dificultava a gestão e multiplicava as necessidades das redes e sistemas TIC e dos recursos de processamento e armazenamento (MDE, 2018).

De forma a dar continuidade a todo este processo através da *Orden DEF/2639/2015,* de 3 de dezembro (MDE, 2017b), foi aprovada a *Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa* (política de sistemas e TIC).

Foi determinado que se incorporassem as estratégias, políticas e iniciativas da NATO e da UE, para garantir a interoperabilidade com estes. Para comportar todas estas condicionantes o MDE, deveria considerar a informação como um recurso estratégico, sustentado pelas TIC. A nova política de sistemas e TIC devia contemplar a existência de uma única infraestrutura de informação da Defesa, designada por *Infraestructura Integral de Información para la Defensa* (I3D). Deveria haver integração, convergência e, quando apropriado, a unificação das infraestruturas TIC existentes, para permitir a gestão otimizada da informação necessária aos utilizadores e facilitar a obtenção de recursos e a contratação dos serviços necessários A transição da situação inicial para a planeada, deveria ser realizada através da convergência física das redes de uso geral com as redes de comando e controle, e a racionalização dos CD, de forma a integrar tudo na infraestrutura única. Essa infraestrutura

deveria ser gerida de forma centralizada pelo *Centro de Sistemas y Tecnologías de la Información y las Comunicaciones* (CESTIC)[2]. (MDE, 2017b).

Em cumprimento da política de sistemas e TIC, foi desenvolvida a *Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa*, aprovada pela *Instrucción 58/2016*, de 28 de outubro, do Secretário de Estado da Defesa de Espanha (MDE, 2017a).

Em termos de implantação foi definido que a infraestrutura contemplasse todos os órgãos do MDE e unidades existentes no território nacional espanhol. Deveriam ser tidas também em conta as localizações internacionais, onde a Espanha tem missões e operações permanentes, e ainda considerar a necessidade de projetação de unidades das FFAA no exterior. Em termos organizacionais, deveria contemplar o MDE, os seus órgãos e os ramos das FFAA (MDE, 2017a).

Os objetivos operacionais que foram identificados para os recursos TIC, são os seguintes: (MDE, 2017a)

- Proporcionar uma infraestrutura TIC unificada, tecnologicamente avançada e otimizada;
- Conseguir e manter a superioridade de informação, garantindo a total autonomia e liberdade de ação, no contexto estratégico e operacional, quanto à tomada de decisões e condução das operações, mesmo em cenários complexos;
- Possibilitar o acesso atempado e seguro à informação, em qualquer momento, em qualquer lugar e considerando a evolução do contexto tecnológico;
- Garantir adaptação, interoperabilidade, total autonomia, adequação, alta qualidade, eficiência, agilidade, caráter projetável, mobilidade estratégica, sustentabilidade e resiliência, de forma a permitir o desenvolvimento de operações, a sinergia entre as forças conjuntas e as ações conjuntas no âmbito das alianças da Espanha.

A partir desses objetivos, foram estabelecidos os seguintes requisitos operacionais: (MDE, 2017a)

- Uma infraestrutura única. O requisito é fornecer um ambiente de serviços TIC, garantindo o tratamento exclusivo da informação a que os utilizadores acedem, de maneira ágil, segura, confiável e contínua. Essa infraestrutura deve integrar todas

[2] Órgão do MDE responsável pela definição, gestão e controlo dos sistemas TIC da defesa. (MDE, s.d.)

as capacidades TIC do MDE existentes e futuras. Deve conter um núcleo protegido, que garanta a sobrevivência dos serviços TIC necessários à operação dos sistemas de comando e controlo militar, mesmo em situações adversas ou em caso de qualquer tipo de incidente. Pretende-se facilitar a gestão centralizada dos recursos TIC e a unificação dos serviços. Deverá permitir o estabelecimento de regras de segurança de forma homogénea, centralizada e automatizada, melhorando a eficácia e garantindo o controlo e proteção, reduzindo a superfície de ataque. Com a infraestrutura única pretende-se obter sinergias, resultando numa melhor utilização dos recursos disponíveis. A infraestrutura deve garantir o fornecimento de serviços TIC a todos os utilizadores, em qualquer local, plataformas, locais de trabalho e operações. Deve permitir a interação dos utilizadores com outras organizações, nacionais e internacionais, através de *gateways* e pontos de interconexão TIC devidamente protegidos e padronizados. As ligações com a NATO serão efetuadas seguindo as políticas desta;

- Continuidade dos serviços TIC. Pretende-se que seja garantida a continuidade de serviços de extremo a extremo, quer nas localizações fixas, quer nas destacáveis, sendo para tal essencial garantir a interoperabilidade dos sistemas TIC;
- Controlo global de acessos. O controlo de acessos deverá ter uma autenticação única e global, incluindo a gestão de identidades, autorização e controlo de acesso dos utilizadores. Os utilizadores terão identidades e credenciais universais para acesso a informação e serviços. No que toca a informação classificada, serão implementados diferentes domínios de segurança. A informação, incluindo a não classificada, fluirá na infraestrutura de telecomunicações encriptada e de acordo com os requisitos de segurança;
- Gestão única centralizada. Conforme definido na política de sistemas e TIC, toda a gestão da infraestrutura única será efetuada pelo CESTIC. Este será responsável pelo sistema, pelas especificações, desenvolvimento, operação, instalação, manutenção e monitorização do seu correto funcionamento ao longo do ciclo de vida. Será ainda o responsável por estabelecer e garantir o cumprimento das regras de segurança. Deverá ter ainda em conta a necessidade de formação do pessoal ligado às TIC, na nova I3D.

A taxonomia que foi idealizada para a arquitetura global, está traduzida na Figura 4:

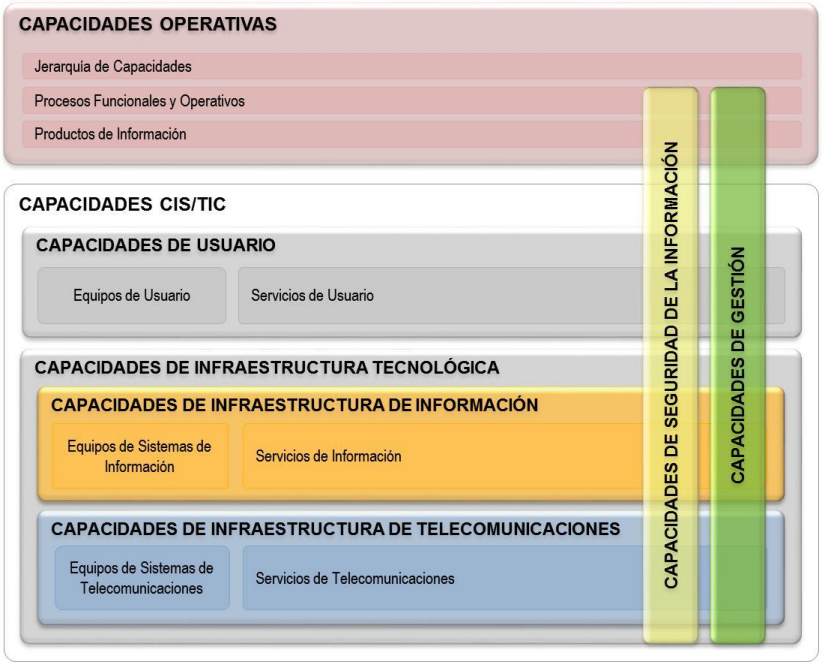


Figura 4 – Taxonomia das capacidades TIC do MDE

Fonte: (MDE, 2018)

Para realizar a implementação da política de sistemas e TIC, e da I3D de acordo com a arquitetura global definida, foi elaborado o *Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa* (PECIS). Este plano contém os diversos aspetos da implementação da política de sistemas e TIC a médio prazo, devendo ser complementado por planos de ação de curto prazo. O PECIS prevê que a implementação ocorra de 2018 a 2023, em duas fases (MDE, 2018).

4.1.2. Análise e conclusões retiradas

Analisando os estudos de caso, NATO e Espanha, é possível identificar aspetos comuns que condicionaram e levaram à necessidade de efetuar a modernização das suas TIC.

As principais condicionantes identificadas, foram:

- Existência de múltiplas infraestruturas de rede, heterogéneas, redundantes e sem uma arquitetura tipo definida. A existência de várias infraestruturas causava dificuldades de gestão, monitorização e controlo. Diminuía a resiliência por dificultar a recuperação de desastres, aumentar a superfície a possíveis ataques e condicionar a segurança. Levava à existência de diversos tipos de *hardware*, *software*, que dificultavam a gestão, manutenção, apoio à utilização e segurança;
- RH. Em ambos os casos, os RH foram considerados um recurso escasso e crítico, para garantir o devido funcionamento das TIC. O facto de ser necessário conhecimento sobre as várias infraestruturas, diferentes equipamentos, *hardware*

e *software*, em exploração a que tinha de ser dado apoio, causava a dispersão deste parco recurso;

- Desperdícios financeiros. A multitude de equipamentos, *hardware* e, *software*, provocava o aumento dos custos, por dificultar a sua aquisição, não permitir economia de escala e exigir pessoal habilitado com conhecimentos mais diversificados.

Da análise resulta que em ambas as soluções de modernização e otimização das TIC, foram adotadas filosofias com base comum. Em ambos os casos, optaram pela criação de uma rede de dados única, com as seguintes características comuns:

- Uma infraestrutura única de rede, com cobertura de todas as localizações das organizações, incluindo os locais de destacamento e missões operacionais;
- Padronização do *hardware*, *software* e equipamentos utilizados;
- Fornecimento centralizado de aplicações e serviços, classificados e não classificados;
- Gestão centralizada, incluindo o controlo global de identidades e acessos;
- Racionalização dos RH com formação adequada às tecnologias adotadas;
- Utilização de *cloud computing* e serviços centrados em rede, com racionalização de CD com informação e serviços replicados.

As principais vantagens que foram identificadas em ambas as soluções são as seguintes:

- A adoção de uma arquitetura TIC única e transversal, facilita a gestão, monitorização e controlo. Aumenta a resiliência, facilitando a recuperação de desastres, reduzindo a superfície de possíveis ataques e possibilitando o reforço da segurança. Evita ainda problemas de interoperabilidade entre as organizações utilizadoras;
- Com a padronização reduz-se a diversidade de *hardware* e *software*, facilitando a sua gestão, manutenção, apoio à utilização e a segurança;
- Em termos de RH, uma arquitetura única, facilita a sua racionalização e a padronização da formação, aumentando o universo de elementos com conhecimentos e capacidades para a gestão e apoio das TIC;
- Otimização dos recursos financeiros pela redução da diversidade de *hardware* e, *software*, facilitando a sua aquisição e manutenção e permitindo economias de escala.

4.1.3. Síntese conclusiva e resposta à questão derivada

Face às diversas condicionantes atrás descritas, das quais se destacam as várias arquiteturas TIC em utilização que dificultavam a interoperabilidade, a criticidade dos RH a elas afeta e à necessidade de otimização dos recursos financeiros, levaram à necessidade da NATO e da Espanha enveredarem por programas de modernização.

Em ambos os casos, devido às vantagens percebidas, decidiram optar por implementar redes de dados únicas, estabelecendo arquiteturas padrão, utilizando *cloud computing*, IaaS, com fornecimento centralizado de aplicações e serviços e abrangendo todas as entidades das respetivas organizações.

Com a descrição e análise das soluções adotadas nos casos em estudo, considera-se respondida a QD1 - Quais as soluções adotadas pela NATO e Espanha em matéria de rede de dados única?

4.2. Redes de dados no universo da Defesa

4.2.1. Apresentação dos dados

Da informação recolhida nas entrevistas realizadas às entidades descritas em "3.1 Participantes e procedimento", apresenta-se de seguida um ponto de situação geral, da forma como as redes de dados estão implementadas no universo da DN.

A nível das infraestruturas de transporte, as diversas entidades estão interligadas pela RFCM, que pode ser considerada a WAN da DN e é gerida centralmente pelo EMGFA/DIRCSI. Em 2012, iniciou-se a utilização de fibra-ótica na RFCM, estando esta em expansão (M. C. Vinhas, *op. cit.*).

As diversas entidades possuem redes próprias, que podem ser vistas como LAN. Na RFCM circula a informação classificada e não classificada em simultâneo, utilizando encriptação adequada. Atualmente, a parte das aplicações e serviços de cariz administrativo é não classificada. A parte classificada, materializada na rede segura das FFAA, *Secure Network*, visa satisfazer necessidades operacionais de comando e controlo militar e está em fase de extensão aos ramos. A RFCM possui capacidade de ligação via satélite, usada pelos navios da Marinha e nos teatros de operação no estrangeiro, entre outros (M. C. Vinhas, *op. cit.*).

Das entrevistas resultou unânime que apesar de interligadas pela mesma infraestrutura de transporte, as redes de dados possuem arquiteturas próprias, com gestão autónoma, não havendo garantia de comunalidade tecnológica ou de procedimentos. Cada entidade do universo da DN, possui ou está ligada a pelo menos um CD ou servidores próprios, que

contêm a sua informação, serviços, aplicações e sistemas, mas que não estão interligados com os das restantes. A nível de continuidade de negócios, esta é da responsabilidade de cada uma.

Foi ainda unanimemente confirmado nas entrevistas, que todas as entidades possuem e utilizam serviços, sistemas e aplicações administrativas com finalidades idênticas, mas de diferentes fabricantes e fornecedores, tais como email, gestão documental, acesso à *internet*, e outras. Cada entidade é responsável pela aquisição e gestão das respetivas licenças. Também a gestão e controlo de acessos é efetuada separadamente, o que dificulta o reconhecimento das identidades pelas restantes, causando dificuldades de interoperabilidade e necessidade de redundância de processos.

A cibersegurança é uma das áreas em que foi decidida a centralização, estando a sua tutela atribuída ao Centro de Ciberdefesa sob o comando do EMGFA/DIRCSI. A falta de comunalidade das TIC, pela multiplicidade de plataformas e *software* em utilização, dificulta a cibersegurança sendo desejável a nível de segurança existirem soluções integradas (Jesus, 2020).

A falta de pessoal na área das TIC apresenta-se como um problema crítico, igualmente reconhecido de forma unânime. Todas as entidades têm um menor número de elementos face aos quantitativos previstos. Este pessoal é essencial para garantir a autonomia das TIC. Os ramos têm vindo a ter uma cada vez maior dificuldade em atrair e recrutar militares para as TIC, exponenciada pela grande procura de profissionais da área a nível civil, com oferta de melhores condições. Sendo os ramos quem fornece a grande maioria do pessoal com estas valências ao resto do universo da DN, esta lacuna repercute-se assim a todos. Igualmente se assiste a uma grande dificuldade de contratação de pessoal civil, na área, para a Administração Pública (AP). O pessoal das TIC é um fator que pode mesmo pôr em causa o futuro do atual Centro de Dados da Defesa (CDD) (R. A. Francisco, op. cit.).

Apesar da falta de pessoal, foi considerado que de um modo geral não há problemas no que toca à formação do que existe.

A nível do orçamento da DN, foram atribuídas ao EMGFA as verbas destinadas às comunicações e à ciberdefesa (J. C. Rocha, entrevista presencial, 5 de dezembro de 2019). Neste aspeto, os ramos e outras entidades, são responsáveis pelos orçamentos referentes a todos os seus sistemas e aplicações, excluindo os fornecidos pela SGMDN (Apêndice E).

No caso do SIGDN, é reconhecido que contribuiu para a redução do número de pessoas dos ramos alocadas à manutenção dos anteriores sistemas de gestão de informação

financeira, tendo havido também poupanças a nível orçamental. Aguarda-se que o módulo RHV se venha a traduzir em poupança idêntica. (B. M. Domingues, entrevista por *email*, 21 de maio de 2020).

Apesar das TIC serem um recurso basilar e essencial para o funcionamento das organizações, no caso do universo da DN e no que toca aos orçamentos, são muitas vezes preteridas em relação às rúbricas da área operacional.

Os orçamentos dos serviços e sistemas comuns, RFCM, cibersegurança e os do Apêndice E, já estão atribuídos ao EMGFA/DIRCSI e SGMDN (J. C. Rocha, R. A. Francisco, *op. cit.*).

4.2.2. Análise e conclusões retiradas

Ao longo dos últimos anos assistiu-se a várias iniciativas, planos e intenções de se proceder à integração e racionalização das TIC do universo da DN, no entanto, continuam a coexistir arquiteturas TIC diferentes e independentes causando problemas de interoperabilidade. Neste período, existiram alguns serviços e sistemas que foram integrados e são transversais, tais como a RFCM e o SIGDN, que reconhecidamente trouxe vantagens.

Apesar de existirem serviços e aplicações de cariz administrativo e uso geral, idênticos, ou com as mesmas finalidades, não há comunalidade na sua aquisição, manutenção e exploração.

No que toca à continuidade de negócios e recuperação de desastres, cada entidade é responsável pela segurança, gestão e manutenção dos seus serviços e sistemas, não havendo qualquer tipo de cooperação com os restantes, o que não contribui para a resiliência.

Os RH são reconhecidamente o recurso mais crítico, devido ao seu reduzido número, dificuldade de contratação de civis e recrutamento de militares. Se não se acautelar este recurso, a autonomia das TIC pode ser posta em causa no universo da DN, pelo que é essencial estudar possíveis soluções. A exemplo do SIGDN, a integração e centralização das TIC apresenta-se como um primeiro passo para a racionalização dos RH.

A nível orçamental, o EMGFA e a SGMDN já têm atribuído o orçamento das atuais partes comuns. Nos ramos, as TIC concorrem a nível orçamental com todas as restantes rúbricas e nem sempre assumem a prioridade desejável. Devido às diversas arquiteturas independentes existentes, não é possível tirar partido da potencial economia de escala.

4.2.3. Síntese conclusiva e resposta à questão derivada

Em resultado da análise efetuada verifica-se que as entidades do universo da DN possuem redes de dados independentes, com informação Não Classificada, arquiteturas

diferentes, estabelecidas e administradas independentemente. Possuem aplicações e serviços de cariz administrativo utilizados para finalidades semelhantes, mas adquiridos e geridos autonomamente. As redes de dados apresentam questões de interoperabilidade, dificuldades quanto aos orçamentos e os RH são um recurso crítico e escasso.

Considera-se assim que foi respondida a QD2 – "Como estão implementadas as redes de dados nas diversas entidades da Defesa?"

4.3. Rede de dados única na Defesa, e resposta à QC

Atualmente e apesar de todas as iniciativas que levaram a uma maior uniformização e integração das TIC no universo da DN, podemos considerar que estamos num ponto semelhante ao que a NATO e a Espanha tinham, e que levaram à decisão da adoção dos programas de modernização. Nesse sentido, as condicionantes e as vantagens, identificadas no subparágrafo 4.1.3 aplicam-se igualmente à situação nacional, considerando-se que tornam evidente a necessidade de uma modernização das TIC da DN.

Tomando como exemplo a filosofia base adotada pela NATO e a Espanha e corroborada nas entrevistas efetuadas, apresenta-se de seguida uma proposta de rede de dados única para a DN.

A nível macro a proposta é a seguinte:

- Adoção de uma arquitetura TIC única e transversal à DN;
- Criação de *cloud computing* na Defesa, com informação até Reservado, para utilização por todas as entidades do universo da DN;
- Infraestruturas para processamento, armazenamento de dados e comunicações, fornecidas como serviços (*IaaS*), com gestão, e apoio centralizados no EMGFA e Secretaria Geral do MDN, e com acordos de nível de serviço estabelecidos;
- Disponibilização de forma centralizada e automatizada de serviços comuns de cariz administrativo.

A um nível mais operacional, a solução preconizada é a que a seguir se descreve:

- Garantir a existência de CD centrais com dispersão geográfica, ligados por canais de comunicação de alto débito, com informação replicada em tempo real, sendo redundantes entre eles (*backup* total uns aos outros) e servindo todas as entidades da DN;
- Utilização da RFCM como infraestrutura de comunicações única, com gestão centralizada pelo EMGFA;

- Criação de um Centro de Operações de Rede tutelado pelo EMGFA, para gestão, monitorização e apoio centralizado da infraestrutura de rede, remotos;
- Criação de módulos destacáveis compatíveis com a nova arquitetura, para utilização em missões e operações no exterior, garantindo qualidade das comunicações e dos serviços;
- Estabelecimento de normas e regras de cibersegurança únicas e comuns, devendo estas ser da responsabilidade do Centro de Ciberdefesa;
- Gestão centralizada de identidades, autenticação, autorização e controlo de acesso dos utilizadores;
- Gestão e aquisição de licenças de software centralizadas, a serem da responsabilidade da Secretaria Geral do MDN, através da sua Unidade Ministerial de Compras;
- O EMGFA, ramos, órgãos e entidades envolvidas, deverão manter e ser responsáveis únicos por todos os serviços e sistemas que sejam específicos para as suas missões;
- Deverão ser garantidas as marcas identitárias e culturais das diferentes entidades, como p. ex., a manutenção de distintos portais da *Internet* e Intranet, endereços de email e outros;
- Deverá ser criada a possibilidade de os utilizadores terem acesso aos seus serviços e informação a partir de qualquer ponto da rede, e prever o acesso remoto com segurança;
- Criação de programas de formação dos RH na administração, gestão, controlo e apoio adequados à nova infraestrutura;
- Em termos de governação, o programa de modernização das TIC da DN deveria ser controlado por um grupo com representantes de topo do EMGFA, ramos, órgãos e entidades da DN envolvidas, incluindo representantes do Centro de Ciberdefesa;
- O grupo de governação, numa primeira fase, deverá coordenar a definição da arquitetura a implementar, garantindo a compatibilidade e interoperabilidade com as normas NATO, UE e restantes organismos públicos nacionais;
- Deverá coordenar também o levantamento de todos os serviços e SI em utilização com vista à sua centralização, integração, padronização e funcionamento na nuvem;

- Em termos financeiros a nova arquitetura única e centralizada deverá passar a estar prevista nos ciclos orçamentais, devendo a parte referente aos serviços, sistemas e equipamentos comuns, ser incluída nos orçamentos do EMGFA e SGDM. Os serviços e sistemas específicos, deverão continuar a ser incluídos pelos ramos, órgãos e entidades por eles responsáveis, nos respetivos orçamentos.

Todas as entidades entrevistadas concordaram que existe a necessidade de integração e centralização das infraestruturas e dos serviços de cariz administrativo da DN, devido às vantagens que pode trazer. Da análise das entrevistas decorre que as vantagens percecionadas são muito semelhantes às das soluções adotadas pela NATO e pela Espanha.

As divergências de opinião que surgiram em relação à solução proposta prenderam-se em aspetos como: o número e tipos de CD e quanto à constituição do grupo de governação.

Apesar de estar fora do âmbito do presente trabalho, foi opinião de vários entrevistados que apesar de apresentar um grau de dificuldade superior, deveria ser equacionada a centralização de alguns dos serviços de comando e controlo militar, a exemplo do que aconteceu na NATO e Espanha.

Como potenciais riscos quanto à adoção de uma rede única de dados na DN, nas entrevistas foram identificados os seguintes:

- Perda do controlo da informação, de dados operacionais e outros;
- Redução do pouco pessoal das TIC existente para níveis que coloquem em causa a garantia da disponibilidade dos serviços e sistemas de cada entidade;
- Qualidade dos níveis de serviço fornecidos insuficiente e inferior à atual;
- Falta de capacidade de resposta adequada em termos de suporte ao utilizador;
- Tempo de resposta a novos requisitos ou alterações solicitadas.

Com a proposta de implementação de uma rede com arquitetura única, com fornecimento centralizado de serviços comuns de cariz administrativo, IaaS, classificação até ao grau de Reservado, e abrangendo todas as entidades do universo da DN, considera-se que se respondeu à QC – "Que solução pode ser adotada pela Defesa para a implementação de uma rede de dados única?"

5. Conclusões

As TIC tornaram-se um recurso básico e vital para qualquer organização, permitindo a comunicação, processamento, armazenamento, e tratamento da informação. Assumindo uma tal importância, torna-se fundamental garantir a sua disponibilidade, fiabilidade e segurança. No caso das FFAA são essenciais para manter a autonomia, conseguir superioridade de informação e são fundamentais para os sistemas de comando e controlo militar. As TIC, são utilizadas na DN há várias dezenas de anos, tendo durante esse período sofrido várias alterações e desenvolvimentos quanto à forma como estão implementadas. No momento do presente estudo e em resultado da sua evolução, existem várias arquiteturas e soluções TIC diferentes, independentes, em exploração pelas diversas entidades do universo da DN. Esta situação, traz problemas de interoperabilidade, de redundâncias e de falta de otimização de recursos. A adoção de alguns sistemas transversais, como o SIGDN, e as vantagens percecionadas que trouxe, realçam ainda mais esses problemas e apontam a integração como uma potencial solução. Por outro lado, tem-se assistido a que várias organizações e países têm vindo a encetar programas de modernização das suas TIC, com uma tendência para a centralização e integração.

O presente estudo teve como OG, propor a implementação de uma rede de dados única na Defesa, tendo sido delimitado nos domínios: espacial, ao universo das entidades da DN; temporal, à atualidade (ano de 2020); e no conteúdo, às redes não classificadas e aos serviços comuns de cariz administrativo utilizados por todas as entidades.

Quanto ao procedimento metodológico, adotou-se um posicionamento epistemológico interpretativo, recorreu-se ao método indutivo utilizando uma estratégia qualitativa e ao estudo de caso. Em termos de recolha de dados recorreu-se a análise documental e a entrevistas semiestruturadas.

De forma a atingir o OG, estabeleceram-se dois OE. O OE1, visou analisar as soluções adotadas pela NATO e Espanha em matéria de rede de dados única.

Dessa análise resulta que no caso da NATO, quando a NCIA assumiu o controlo da área de IT, ordenou a realização de um estudo para conhecer a situação real. Dos resultados obtidos desse estudo, ficou evidente que a modernização das infraestruturas IT poderia conduzir a ganhos significativos, em termos de eficácia, eficiência, RH e financeiros.

Verificaram que ao longo do tempo, e fruto de terem sido criadas através de projetos e programas individuais desconexos, existiam diversas arquiteturas IT idênticas, replicadas em várias localizações. De forma a gerir, manter e apoiar essas arquiteturas, os níveis de RH

tornaram-se bastante superiores aos necessários para os serviços efetivamente fornecidos, aumentando os respetivos custos. O facto de existirem infraestruturas redundantes, não garantia a resiliência, devido à sua gestão e apoio não serem centralizados e não se apoiarem em caso de desastre. A segurança também não saía beneficiada, devido à dificuldade em garantir que as últimas atualizações eram aplicadas. Concluíram que a adoção de soluções centradas em rede, a gestão e o controlo comuns, a limitação de combinações de sistemas operativos e *hardware*, o aumento dos níveis de virtualização, a inclusão de *cloud computing* e capacidade de recuperação de desastres, permitiria reduzir a quantidade de RH e a infraestrutura IT. O objetivo era proporcionar uma IaaS privada, baseada em *cloud computing* para fornecer os serviços através de uma infraestrutura única, resiliente, logicamente integrada, geograficamente dispersa e contendo todas as aplicações em utilização. Pretendiam também facilitar a sustentação, através da padronização de *software*, de *hardware*, dos processos e da formação.

De forma a resolverem os problemas existentes e conseguir obter os ganhos identificados, elaboraram o programa ITM com vista à modernização das infraestruturas IT. O objetivo era criar uma rede de dados única para interligar toda a organização NATO, com o fornecimento de serviços operacionais e administrativos através de dois domínios, com classificação até NATO Secreto e até NATO Reservado, respetivamente, e acesso à *internet*.

Tecnicamente foi prevista a criação de três CDC centrais com altos níveis de resiliência, com toda a informação replicada entre eles e com hipótese de recuperação de desastres a partir de qualquer um. Foi ainda prevista, a criação de um COC e respetivo *backup*, deslocalizado, para fornecimento da gestão e do apoio às IT, de forma centralizada.

Da análise do caso da Espanha, verificou-se que em 2002 tinha sido estabelecido que a nível da Defesa deveriam ser criadas duas redes corporativas independentes, uma para os sistemas de comando e controlo militar, com ligação à NATO e a outra para uso administrativo geral. Nessa altura, identificaram que a crescente necessidade de pessoal técnico na área das TIC, tornava os RH um recurso crítico, e previam a necessidade da criação de carreiras próprias e atribuição de incentivos para atração de interessados.

Em 2015, verificaram que a rede de suporte dos SI não tinha sido unificada, que possuíam uma grande diversidade de redes, CD e sistemas TIC, o que causava disfunções, redundâncias e limitações no acesso à informação. Dificultava a gestão e multiplicava as necessidades de redes e sistemas TIC.

Para dar continuidade ao processo de integração, aprovaram a política de sistemas e TIC. Essa política determinou a incorporação e o cumprimento das normas da NATO e EU, para garantir a interoperabilidade com estes e que o MDE deveria considerar a informação um recurso estratégico, sustentado pelas TIC. Estabeleceu que deveria ser criada uma infraestrutura única, a I3D, gerida centralmente. De acordo com essa política, desenvolveram ainda uma arquitetura única e global para as TIC da Defesa. A I3D deveria abranger todos os órgãos do MDE e unidades existentes no território nacional espanhol, os locais das missões e operações permanentes e a projetação de unidades das FFAA no exterior.

Os objetivos pretendidos foram a criação de uma rede de dados única, para fornecer serviços TIC, garantindo o tratamento exclusivo da informação de forma segura, confiável e contínua e deveria integrar todas as capacidades TIC existentes e futuras, do MDE. Com a integração, convergência e unificação das infraestruturas pretendem otimizar a gestão da informação e facilitar a obtenção de recursos e a contratação dos serviços necessários. Foi objetivo fazer convergir fisicamente as redes de uso administrativo geral, com as redes de comando e controlo e racionalizar os CD, integrando tudo na infraestrutura única. Deveria ser criado um núcleo protegido para garantir os serviços TIC necessários à operação dos sistemas de comando e controlo militar, em todas as situações, mesmo em caso de incidentes. Era objetivo ter uma gestão centralizada dos recursos TIC, unificar os serviços, estabelecer regras de segurança de forma homogénea, central e automatizada e reduzir a superfície de ataque. A infraestrutura deveria garantir o fornecimento de serviços TIC a todos os utilizadores, em qualquer local, plataformas, locais de trabalho e de operações e permitir a interação com outras organizações, nacionais e internacionais. Deveria ser garantida a continuidade de serviços de extremo a extremo e haver um controlo global de acessos, com autenticação única. Previram a implementação de domínios diferentes de segurança para tratamento da informação de acordo com a sua classificação e a necessidade de formação do pessoal ligado às TIC, na nova I3D.

Com o OE2 pretendeu-se analisar a forma como estão implementadas as redes de dados nas diversas entidades da DN.

Resultante da informação recolhida, verifica-se que a nível do transporte de dados, as entidades do universo da DN estão interligadas por uma infraestrutura única, a RFCM, gerida centralmente pelo EMGFA/DIRCSI, e onde circula informação classificada e não classificada. A responsabilidade pela cibersegurança foi também centralizada nesta entidade.

As diversas entidades do universo da DN possuem arquiteturas TIC próprias e com gestão autónoma, desenvolvidas de forma independente. Neste universo, as entidades possuem vários CD e servidores que não estão interligados com os das restantes e têm tecnologias e procedimentos de utilização diferentes. No que toca à continuidade de negócios e recuperação de desastres, cada entidade é responsável pela segurança, gestão e manutenção dos seus serviços e sistemas.

Apesar de utilizarem sistemas e aplicações administrativas com as mesmas finalidades, não há comunalidade na sua aquisição, manutenção e exploração o que por vezes causa problemas de interoperabilidade e não permite beneficiar de possíveis sinergias e economia de escala.

Para além dos sistemas e serviços administrativos de uso geral, existem SI de comando e controlo militar, específicos do EMGFA e dos ramos, muitos deles classificados.

Os RH qualificados são um recurso cada vez mais crítico que é necessário ser acautelado para garantir a autonomia do universo da Defesa quanto às TIC. A centralização de sistemas e serviços é essencial numa primeira fase para mitigar este risco, sendo necessário equacionar e adotar medidas para o tentar resolver no futuro.

A nível orçamental, a parte referente aos serviços e sistemas comuns já foi centralizada, quanto aos restantes, as TIC concorrem com todas as outras rúbricas, sendo muitas vezes preteridas em relação à área operacional a que é dada prioridade.

Em cumprimento do OG, o estudo foi orientado no sentido de responder à QC – "Que solução pode ser adotada pela Defesa para a implementação de uma rede de dados única?"

Em resposta à QC, e após a análise realizada em cumprimento dos objetivos específicos, verifica-se que no universo da DN, a nível das TIC, se tem uma situação semelhante à que levou a NATO e a Espanha a terem de enveredar pela adoção de programas de modernização com o objetivo de implementarem redes de dados únicas. Considera-se que todas as vantagens por eles identificadas, com a adoção de redes únicas, se aplicam e poderão ser replicadas a nível nacional.

Com base nessa assunção propõe-se a adoção pela DN, de uma rede de dados única, de cariz administrativo, com grau de classificação até Reservado, utilizando *cloud computing*, CD redundantes, IaaS com gestão e apoio centralizados, acordos de nível de serviço estabelecidos e disponibilização centralizada e automatizada de serviços comuns.

Tendo esta proposta sido colocada à consideração dos diversos responsáveis pelas TIC do universo da DN, obteve uma concordância generalizada, e confirmação de que podem

decorrer vantagens na centralização e integração dos serviços administrativos comuns. Não obstante ter havido opiniões divergentes quanto a alguns pontos, considera-se que foi validada a necessidade da adoção de uma rede de dados única na DN,

Em termos de contributos para o conhecimento, verificou-se que com a adoção pelas diversas entidades da Defesa de uma rede de dados única, permitiria evitar as atuais redundâncias, ineficiências e disfunções. Que a falta de RH habilitados na área das TIC, coloca em risco o futuro de alguns serviços e exige ações urgentes. Para além das melhorias na operacionalidade, interoperabilidade, segurança e outras, ficou evidente que a implementação de uma rede única de dados pela DN, a exemplo do SIGDN, é uma das medidas para a mitigação da lacuna de RH, tornando-se necessário ser considerada.

Em relação às limitações da investigação, destaca-se a necessidade de confinamento imposta pela *Coronavirus Disease*, que dificultou os contactos e a realização das entrevistas, tendo estas sido ocorrido à distância por *email*. Outra das dificuldades encontradas foi o acesso à informação NATO, visto não estarem estabelecidos mecanismos no IUM que possam ser utilizados para esse fim.

No que toca a estudos futuros, sendo os RH na área das TIC um recurso crítico, e dada a dificuldade de recrutamento de pessoal habilitado devido, entre outros, à oferta de melhores condições a nível civil, sugere-se que sejam estudadas as possíveis formas de solucionar este problema, incluindo adoção de medidas excecionais e discriminação positiva de carreiras. Sugere-se ainda o estudo de uma possível solução de rede de dados comum para os sistemas e serviços de comando e controlo militar, unificada como a que foi aqui proposta.

A recomendação de ordem prática que pode ser feita nesta área, é que sendo as TIC um recurso essencial e crítico para a autonomia da DN e o cumprimento e execução das missões das FFAA, tal como qualquer sistema de armas, é necessário que lhes seja atribuída a devida importância pelo escalão máximo e estabelecidas diretivas claras nesse sentido.

Referências Bibliográficas

Agência para a Modernização Administrativa. (2015, junho). PGETIC Taxa de execução do Plano de Ação Setorial do MDN [Página *online*]. Retirado de https://pgetic.tic.gov.pt/ticgov/pgetic/ministerios/mdn

Agência para a Modernização Administrativa. (2016a, dezembro). PGETIC Arquitetura de sistemas de informação do MDN [Página *online*]. Retirado de https://pgetic.tic.gov.pt/ticgov/pgetic/ministerios/mdn/arquitetura-de-sistemas-de-informacao-do-mdn

Agência para a Modernização Administrativa. (2016b, dezembro). PGETIC Cloud computing no MDN [Página *online*]. Retirado de https://pgetic.tic.gov.pt/ticgov/pgetic/ministerios/mdn/cloud-computind-go-mdn

CISCO. (s. d.). O que é um centro de dados? [Página *online*]. Retirado de https://www.cisco.com/c/pt_pt/solutions/data-center-virtualization/what-is-a-data-center.html

Comissão das Comunidades Europeias. (2005). *COM(2005)229 final − "i2010 – Uma sociedade da informação europeia para o crescimento e o emprego"* [Versão PDF]. Retirado de http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PT:PDF

Comissão Europeia. (2010c). *COM(2010)245 final − Uma Agenda Digital para a Europa* [Versão PDF]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52010DC0245&qid=1575500704184&from=PT

Comissão Europeia. (2010a). *COM(2010) 744 final − Para a interoperabilidade dos serviços públicos europeus* [Versão PDF]. Retirado de https://ec.europa.eu/commission/presscorner/api/files/document/print/pt/ip_10_1734/IP_10_1734_PT.pdf

Comissão Europeia. (2010d). *COM(2010)744 final − Anexo 2 − Quadro Europeu de Interoperabilidade (QEI) para os serviços públicos europeus* [Versão PDF]. Retirado de https://ec.europa.eu/transparency/regdoc/rep/1/2010/PT/1-2010-744-PT-F1-1-ANNEX-2.Pdf

Comissão Europeia. (2010b). *COM(2010)2020 final − Europa 2020* [Versão PDF]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52010DC2020&qid=1575501205570&from=PT

Decreto-Lei n.º 183/2014, de 29 de dezembro. (2014). *Lei Orgânica do Ministério da Defesa Nacional*. Diário da República, 1.ª Série, 250, pp. 6375–6382. Lisboa: Ministério da Defesa Nacional.

Decreto-Lei n.º 184/2014, de 29 de dezembro. (2014). *Aprova a Lei Orgânica do Estado-Maior General das Forças Armadas*. Diário da República, 1.ª Série, 250, pp. 6382–6397. Lisboa: Ministério da Defesa Nacional.

Decreto-Lei n.º 249/2015, de 28 de outubro. (2015). *Aprova a orgânica do ensino superior militar e o Estatuto do Instituto Universitário Militar*. Diário da República, 1.ª Série, 211, pp. 9298–9311. Lisboa: Ministério da Defesa Nacional.

Decreto Regulamentar n.º 6/2015, de 31 de julho. (2015). *Aprova a orgânica da Secretaria-Geral do Ministério da Defesa Nacional*. Diário da República, 1.ª Série, 148, pp. 5191–5193. Lisboa: Presidência do Conselho de Ministros.

Decreto Regulamentar n.º 10/2015, de 31 de julho. (2015). *Aprova a orgânica da Marinha*. Diário da República, 1.ª Série, 148, pp. 5200–5237. Lisboa: Ministério da Defesa Nacional.

Decreto Regulamentar n.º 11/2015, de 31 de julho. (2015). *Aprova a orgânica do Exército*. Diário da República, 1.ª Série, 148, pp. 5237–5259. Lisboa: Ministério da Defesa Nacional.

Decreto Regulamentar n.º 12/2015, de 31 de julho. (2015). *Aprova a Orgânica da Força Aérea*. Diário da República, 1.ª Série, 148, pp. 5259–5275. Lisboa: Ministério da Defesa Nacional.

Dron, A. (2019). Polaris: Transforming NATO's digital presence. *NITECH: NATO Innovation and Technology*, *Issue 1*, pp. 62–66. Retirado de https://issuu.com/globalmediapartners/docs/nitech_issue_01_may_2019?e=25557842/69717603

Edwards, G., Mikla, F., & Sokolowski, L. (2016). IT Modernization. *Communicator*, *Issue 1*, pp. 14–15. Retirado de https://issuu.com/nciagency/docs/nci_agency_communicator_magazine_-_

Estado-Maior da Força Aérea. (2015). *Plano Diretor dos Sistemas de Informação da Força Aérea*. Alfragide: Força Aérea Portuguesa

Fachada, C. P. A., Ranhola, N. M. B., Marreiros, J. P. R., & Santos, L. A. B. (2020). *Normas de Autor no IUM*. (3.ª ed., revista e atualizada). IUM Atualidade, 7. Lisboa: Instituto Universitário Militar.

Gartner. (s. d.). Scalability [Página *online*]. Retirado de https://www.gartner.com/en/information-technology/glossary/scalability

Grupo de Projeto para as Tecnologias de Informação e Comunicação. (2011). *Plano global estratégico de racionalização e redução de custos nas TIC, na Administração Pública Horizonte 2012-2016* [Versão PDF]. Retirado de https://tic.gov.pt/pgetic/PGETIC_v1.0.pdf

IBM. (2019, 25 de junho). Networking [Página *online*]. Retirado de https://www.ibm.com/cloud/learn/networking-a-complete-guide#toc-what-is-a--lC8pLPAs

Jesus, H. F. (2020). Ciberdefesa. Em: Área de Ensino de Operações Militares. *Palestra ao CPOG 2019/2020*. Palestra organizada pelo Instituto Universitário Militar. Lisboa.

Lenk, P. J. (2014). ITM White Paper No . 1 NATO's First Step to the Cloud: Overview and Business Drivers [Versão PDF]. Retirado de https://www.ncia.nato.int/it-modernization/PublishingImages/Pages/default/WP1 - One Small Step.pdf

Microsoft. (s. d.). O que é IaaS? [Página *online*]. Retirado de https://azure.microsoft.com/pt-pt/overview/what-is-iaas/

Ministério da Defesa Nacional. (2013). *Plano de ação setorial de racionalização das TIC no Ministério da Defesa Nacional. (Versão 4.0)* [Versão PDF]. Retirado de https://pgetic.tic.gov.pt/ticgov/pgetic/ministerios/mdn/resolveuid/42d5c3ad33c241b79e6dda5fd070221d

Ministerio de Defensa de España. (2002). *Orden DEF/315/2002, de 14 de febrero, por la que se aprueba el Plan Director de Sistemas de Información y Telecomunicaciones y se establece, para su dirección, gestión y seguimiento, el Comisionado del Plan*. Boletín Oficial del Estado, 44, pp. 6752–6756. Retirado de https://boe.es/boe/dias/2002/02/20/pdfs/A06752-06756.pdf

Ministerio de Defensa de España. (2017a). *Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC)* [Versão PDF]. Retirado de https://publicaciones.defensa.gob.es/arquitectura-global-de-sistemas-y-tecnologias-de-informacion-y-comunicaciones-del-ministerio-de-defensa-ag-cis-tic.html

Ministerio de Defensa de España. (2017b). *Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa* [Versão PDF]. Retirado

de https://publicaciones.defensa.gob.es/politica-de-los-sistemas-y-tecnologias-de-la-informacion-y-las-comunicaciones-del-ministerio-de-defensa.html

Ministerio de Defensa de España. (2018). *Plan estratégico de los sistemas y tecnologías de la información y las comunicaciones del Ministerio de Defensa (PECIS)* [Versão PDF]. Retirado de https://publicaciones.defensa.gob.es/plan-estrategico-de-los-sistemas-y-tecnologias-de-la-informacion-y-las-comunicaciones-del-ministerio-de-defensa-pecis.html

Ministerio de Defensa de España. (s. d.). Centro de Sistemas y Tecnologías de la Información y las Comunicaciones - Ministerio de Defensa de España [Página *online*]. Retirado de https://www.defensa.gob.es/ministerio/organigrama/sedef/cestic/

National Institute of Standards and Technology. (2011, 28 de setembro). The NIST Definition of Cloud Computing [Página *online*]. Retirado de https://www.nist.gov/publications/nist-definition-cloud-computing

NATO Communications and Information Agency. (2017, s. d.). NCIA IT Modernization (ITM) [Página *online*]. Retirado de https://www.ncia.nato.int/it-modernization/Pages/default.aspx

NEP/INV-001. (2018). *Trabalhos de investigação*. Lisboa: Instituto Universitário Militar.

NEP/INV-003. (2020). *Estrutura e regras de citação e referenciação de trabalhos escritos a realizar no Instituto Universitário Militar*. Lisboa: Instituto Universitário Militar.

North Atlantic Council. (2008). *C-M(2008)0113(INV) The Primary Directive on Information Management*. Bruxelas: North Atlantic Treaty Organization.

North Atlantic Treaty Organization. (2005). *ADatP-02 - NATO information technology glossary*. Bruxelas: North Atlantic Treaty Organization.

North Atlantic Treaty Organization. (2014). *AAP-31 - NATO Glossary of Communication and Information Systems Terms and Definitions*. Bruxelas: North Atlantic Treaty Organization

North Atlantic Treaty Organization. (2015, 13 de outubro). NATO Network Enabled Capability (NNEC) (archived) [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_54644.htm?selectedLocale=en

North Atlantic Treaty Organization. (2019). *NATO Architecture Framework Version 4* [Versão PDF]. Retirado de https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_12/20191203_191203-NAFv4_2019.10_print.pdf

Resolução do Conselho de Ministros n.º 46/2011, de 14 de novembro. (2011). *Cria o Grupo de Projecto para as Tecnologias de Informação e Comunicação*. Diário da República, 1.ª Série, 218, p. 4848. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 12/2012, de 12 de janeiro. (2012). *Aprova o plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública, apresentado pelo Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC)*. Diário da República, 1.ª série, 27, pp. 596–605. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 60/2012, de 10 de julho. (2012). *Procede à primeira alteração à Resolução do Conselho de Ministros n.º 46/2011, de 14 de novembro, que cria o Grupo de Projeto para as Tecnologias de Informação e Comunicação*. Diário da República, 1.ª Série, 132, pp. 3584–3586. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 19/2013, de 21 de março. (2013). *Aprova o Conceito Estratégico de Defesa Nacional*. Diário da República, 1.ª série, 67, pp. 1981–1995. Retirado de https://dre.pt/application/dir/pdf1sdip/2013/04/06700/0198101995.pdf

Resolução do Conselho de Ministros n.º 33/2016, de 3 de junho. (2016). *Constitui o Conselho para as Tecnologias de Informação e Comunicação*. Diário da República, 1.ª série, 107, pp. 1735–1737. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 108/2017, de 2 de março. (2017). *Aprova a Estratégia TIC 2020 e o respetivo Plano de Ação*. Diário da República, 1.ª série, 143, pp. 3938–4201. Lisboa: Presidência do Conselho de Ministros.

Santos, L. A. B., & Lima, J. M. M. (Coord.). (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação*. (2.ª ed., revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Zitek, N. (s. d.). ITIL Incident Management – How to separate roles at different support levels [Página *Online*]. Retirado de https://advisera.com/20000academy/knowledgebase/itil-incident-management-separate-roles-different-support-levels/

Apêndice A – Iniciativas para a racionalização das TIC do universo da DN

Desde 2005 que a UE tem vindo a promover e a estabelecer orientações aos seus membros para que seja fomentado o emprego das Tecnologias de Informação e Comunicações de forma interoperável (Comissão das Comunidades Europeias, 2005, p. 13).

Em 2010 quando foi estabelecida a estratégia Europa 2020 (Comissão Europeia [CE], 2010d), da qual derivou a Agenda Digital para a Europa (CE, 2010a), os membros foram instados mais uma vez a promover a interoperabilidade (CE, 2010b). Para além da interoperabilidade foram também incumbidos de criar serviços públicos com base nas TIC (CE, 2010c).

Devido a questões económicas, em 2011 o XIX Governo assumiu como vetor estratégico a redução e a racionalização dos custos suportados pelo Orçamento do Estado (RCM n.º 46/2011, de 14 de Novembro, 2011). Compromissos idênticos foram assumidos com o Fundo Monetário Internacional, Banco Central Europeu e a CE (RCM n.º 46/2011, de 14 de novembro, 2011). De forma a cumprir a estratégia e compromissos assumidos, a RCM n.º 46/2011, de 14 de novembro, determinou a constituição do GPTIC com o objetivo de delinear e implementar uma estratégia para redução de custos referentes às TIC de forma transversal na Administração Pública.

O GPTIC no cumprimento da missão de que foi incumbido elaborou o Plano Global Estratégico de racionalização e redução de custos nas TIC, na Administração Pública (PGETIC) (GPTIC, 2011), que pretendia potenciar a eficiência e a eficácia de operação ao menor custo possível. Este plano foi aprovado pela RCM n.º 12/2012, de 12 de janeiro. Esta resolução determinou também que todos os ministérios deveriam elaborar os respetivos Planos de Ação Sectorial (PAS) de racionalização das TIC e entre estes o Ministério da Defesa Nacional (MDN).

Através da RCM n.º 60/2012, de 10 de julho, que alterou a RCM n.º 46/2011, de 14 de Novembro, foi estabelecido que o GPTIC cessaria funções em 31 de dezembro de 2015.

O PAS do PGETIC do MDN, da responsabilidade da SGMDN, continha vinte medidas e de acordo com a última atualização, em junho de 2015, a taxa de execução da totalidade destas era de 53% (Agência para a Modernização Administrativa, 2015).

Dessas medidas realçam-se:

- "Arquitetura de sistemas de informação do MDN: Definição da arquitetura de referência no MDN atendendo ao modelo que será definido para a AP e às especificidades das FFAA (arquitetura de referência *North Atlantic Treaty*

Organization (NATO))", com execução de 0% (Agência para a Modernização Administrativa, 2016a);

- *"Cloud Computing* no MDN: Estudar a viabilidade da implementação de uma *cloud* privada no MDN", com execução de 20% (Agência para a Modernização Administrativa, 2016b).

O XXI Governo através da RCM n.º 33/2016, de 3 de junho, vem prosseguir o mesmo intento constituindo desta feita o Conselho para as Tecnologias de Informação e Comunicação na Administração Pública (CTIC).

O CTIC elaborou a Estratégia TIC 2020 e os respetivos planos setoriais, aprovada pela RCM n.º 108/2017, de 2 de março, e que à data da elaboração da investigação continua em execução. Entre os planos sectoriais encontra-se o Plano Setorial TIC da Área Governamental da DN da responsabilidade da SGMDN.

Analisando esse plano sectorial (RCM n.º 108/2017, de 2 de março, 2017, p. 3944), verifica-se que a integração e centralização das TIC deixou de constar como um objetivo claro.

Apêndice B – Modelo de Análise

De acordo com o objeto de estudo, os objetivos, geral e específicos e respetivas questões, central e derivadas, foi estabelecido o modelo de análise que se apresenta no quadro seguinte.

Quadro 3 – Modelo de análise

Objetivo Geral	Propor a implementação de uma rede de dados única na Defesa.				
Objetivos Específicos	**Questão Central**	Que solução pode ser adotada pela Defesa para a implementação de uma rede de dados única?			
	Questões Derivadas	**Conceitos**	**Dimensões**	**Indicadores**	**Técnicas de recolha de dados**
OE1 Analisar as soluções adotadas pela NATO e Espanha em matéria de rede de dados única.	**QD1** Quais as soluções adotadas pela NATO e Espanha em matéria de rede de dados única?	Rede de dados única.	Processos e Tecnologia	Arquiteturas	Análise documental e entrevistas semiestruturadas
				Interoperabilidade	
				Forma de gestão	
			Organização / Pessoas	Quantitativos	
			Financeira.	Orçamento	
OE2 Analisar a forma como estão implementadas as redes de dados nas diversas entidades da Defesa.	**QD2** Como estão implementadas as redes de dados nas diversas entidades da Defesa?	Rede de dados.	Processos e Tecnologia.	Arquiteturas	
				Interoperabilidade	
				Forma de gestão	
			Organização / Pessoas	Quantitativos	
			Financeira.	Orçamento	

Apêndice C – Listas de entrevistados

Quadro 4 – Entrevistados do escalão superior

Função	Posto	Nome
SUBCEMFA	MGEN	T. D. Lopes
Diretor da DIRCSI	BGEN	J. C. Rocha
Superintendente das Tecnologias da Informação da Marinha	COM	B. M. Domingues
Diretor da DCSI do Exército	BGEN	F.B. Soares
Secretário-adjunto da SGMDN	COM	R. A. Francisco

Quadro 5 – Entrevistados do escalão operacional

Função	Posto	Nome
Diretor da DCSI da Força Aérea	BGEN	A. C. Barros
Chefe da DIVCSI da Força Aérea	COR	A. R. Telha
Diretor da DITIC da Marinha	CMG	J. C. Roque
Subdiretor da DCSI do Exército	COR	L. G. Afonso
*2.º Comandante da Academia Militar	COR TIR	C. O. Ribeiro
Diretor da Direção de Serviços do Centro de Dados da Defesa	CMG	F. P. Silva

* O 2.º Comandante da Academia militar foi entrevistado porque, na fase das entrevistas exploratórias era o Subdiretor da DCSI do Exército, considerando-se relevante a sua opinião.

Apêndice D – Guiões de entrevista e síntese da informação recolhida

Neste Apêndice é apresentada a parte comum dos guiões de entrevista utilizados, o enquadramento e o objetivo do trabalho, e a parte das questões colocadas a cada escalão. No final inclui-se uma breve síntese da informação mais importante recolhida. As respostas originais não foram incluídas por limitações de espaço.

Guiões de Entrevista

Enquadramento

Nos últimos anos, a NATO, assim como a Espanha, deram início à atualização das suas infraestruturas de Tecnologias de Informação e Comunicações (TIC).

Nas soluções que adotaram é possível identificar vários pontos de convergência:

- Adoção de uma arquitetura das TIC única, com cobertura de todas as localizações das organizações, incluindo os locais de destacamento e das missões operacionais;
- Fornecimento de serviços, gestão e apoio centralizados, incluindo centralização de identidades e controlo de acessos;
- Racionalização de centros de dados, contendo informação replicada;
- Utilização de *cloud computing* e serviços centrados em rede;
- Racionalização dos recursos humanos e ajuste na sua formação nas TIC de acordo com as tecnologias adotadas.

Como vantagens da modernização, essas organizações identificaram as seguintes:

- A adoção de uma arquitetura TIC única e transversal, facilita a gestão, monitorização e controlo. Aumenta a resiliência, facilita a recuperação de desastres, reduz a superfície de possíveis ataques e possibilita reforçar a segurança. Reduz a diversidade de hardware e software, facilitando a sua gestão, manutenção, apoio à utilização e segurança;
- Em termos de recursos humanos, a arquitetura de rede única facilita a padronização da formação, permitindo aumentar o universo de elementos com o nível de conhecimentos e capacidades necessários para a gestão e apoio das TIC;
- Otimização dos recursos financeiros pela redução da diversidade de equipamentos, hardware e, software, facilitando a sua aquisição e permitindo economias de escala.

A nível nacional decorreram vários programas de racionalização das TIC, determinados por vários Governos, nos quais a Defesa Nacional tem estado incluída. Apesar do preconizado nesses programas, verifica-se que atualmente, a nível da Defesa Nacional

(Ministério da Defesa Nacional, serviços centrais e entidades dele dependentes, EMGFA e órgãos dependentes e os três Ramos), continuam a existir várias soluções a nível das TIC.

Como exemplo de uma solução transversal adotada na Defesa Nacional, surge o Sistema Integrado de Gestão da Defesa Nacional (SIGDN). Apesar da sua transversalidade, as diferentes soluções TIC existentes dificultaram a sua implementação e exploração, o que continua a acontecer.

Objetivo do trabalho

O presente trabalho, pretende avaliar a pertinência da implementação de uma rede de dados única na Defesa Nacional, a exemplo do que está a ser efetuado pela NATO e outros países membro.

Tendo como exemplo as soluções da NATO e da Espanha, pretende-se avaliar a possibilidade de implementação de uma solução em moldes idênticos.

A visão a nível macro dessa solução é a seguinte:

- Criação de *cloud computing* na Defesa, através da constituição de Centros de Dados redundantes e para utilização pelo EMGFA, ramos, órgãos e entidades da Defesa;
- Infraestruturas para processamento, armazenamento de dados e comunicações, fornecidas como serviços (*Infrastructure as a Service*), com gestão, e apoio centralizados no EMGFA e Secretaria Geral do MDN, e com acordos de nível de serviço estabelecidos;
- Disponibilização de forma centralizada de serviços comuns, tais como: gestão de identidades, controlo de acessos, email, gestão documental, acesso à internet, e outros.

A um nível mais baixo, a solução preconizada é a que a seguir genericamente se descreve:

- Implementação de uma arquitetura TIC única e transversal à Defesa, para tratamento de informação até ao grau de classificação de Reservado;
- Utilização de uma infraestrutura de comunicações única, com gestão centralizada do EMGFA (continuação da implementação da RFCM);
- Implementação de três centros de dados, um em cada ramo, garantindo dispersão geográfica, ligados por canais de comunicação de alto débito, com informação replicada em tempo real, sendo redundantes entre eles (servindo de backup total uns aos outros) e servindo todas as entidades da Defesa abrangidas;

- Criação de módulos destacáveis compatíveis com a nova arquitetura, para utilização em missões e operações no exterior, garantindo qualidade das comunicações e serviços;
- Utilização de *cloud computing* e serviços centrados em rede;
- Estabelecimento de normas e regras de segurança cibernética únicas e comuns, devendo estas ser da responsabilidade do Centro de Ciberdefesa;
- Gestão, monitorização e apoio centralizado da infraestrutura de rede, a serem efetuados pelo EMGFA, com reforço de pessoal, constituído por parte dos elementos que atualmente têm esse tipo de funções nos ramos e diversas entidades da Defesa;
- Gestão centralizada de identidades, autenticação, autorização e controlo de acesso dos utilizadores;
- Gestão e aquisição de licenças de software centralizadas, a serem coordenadas pela Secretaria Geral do MDN;
- O EMGFA, ramos, órgãos e entidades envolvidos, deverão manter e ser responsáveis únicos por todos os serviços e sistemas que sejam específicos para a suas missões;
- Deverá ser criada a possibilidade de os utilizadores terem acesso aos seus serviços e informação a partir de qualquer ponto da rede, incluindo acesso remoto;
- Criação de programas de formação dos recursos humanos na gestão, controlo e apoio adequados à nova infraestrutura (a formação em soluções de última geração, com paralelo a nível civil, poderá ser um ponto de atratividade para o recrutamento);
- Em termos de governação, a exemplo do que acontece com a Comissão de Acompanhamento do SIGDN, o programa de modernização das TIC da Defesa Nacional deveria ser controlado por um grupo com representantes de topo do EMGFA, ramos, órgãos e entidades envolvidos, incluindo representantes do Centro de Ciberdefesa. Uma das possibilidades seria a referida Comissão de Acompanhamento;
- O grupo de governação, numa primeira fase, deverá coordenar a definição da arquitetura a implementar, garantindo a compatibilidade e interoperabilidade com as normas NATO, União Europeia e restantes organismos públicos nacionais;

- Deverá coordenar também o levantamento de todos os serviços e SI em utilização com vista à sua centralização, padronização e funcionamento na nuvem;
- Em termos financeiros a nova arquitetura única e centralizada deverá passar a estar prevista nos ciclos orçamentais, devendo a parte referente aos serviços, sistemas e equipamentos comuns, ser incluída nos orçamentos do EMGFA e Secretaria Geral. Os serviços e sistemas específicos, deverão continuar a ser incluídos pelos ramos, órgãos e entidades por eles responsáveis nos respetivos orçamentos;
- Como possível calendário de implementação, a modernização deveria ser planeada de forma a ser alinhada com o ciclo de modernização dos equipamentos e serviços TIC em exploração nos diversos ramos e entidades, garantindo que os substitutos já sejam adquiridos de acordo com a arquitetura que for definida.

O objetivo da entrevista

Pretende-se com esta entrevista, obter a opinião e perceção das diversas entidades contactadas quanto à solução idealizada, vantagens e desvantagens que dela decorrem.

Nesse sentido foram colocadas as seguintes questões:

Questões colocadas ao escalão superior

1. Quais as vantagens e desvantagens que o SIGDN trouxe (pessoal, orçamental e fiabilidade)?
2. Considera que existe interoperabilidade em termos das TIC, a nível dos diversos atores da Defesa (serviços, sistemas e comunicações)?
3. Vê que possam existir vantagens e necessidade em ter serviços TIC comuns (gestão de identidades, controlo de acessos, email, gestão documental, acesso à internet, e outros), geridos e fornecidos de forma centralizada? E desvantagens?
4. Tem havido renovação / contratação / recrutamento de pessoal das TIC em quantidade suficiente? Qual a perspetiva de evolução futura?
5. Poderia a centralização dos orçamentos referente aos serviços e sistemas comuns facilitar a gestão e obtenção das capacidades TIC?
6. Seria o EMGFA a entidade mais adequada para assumir a responsabilidade pela infraestrutura TIC única, a exemplo do que acontece com as comunicações militares atualmente?

7. Como acontece com o SIGDN, e outras iniciativas, considera que a Secretaria Geral do MDN seria a entidade mais adequada para coordenar e gerir a contração das licenças dos serviços comuns?
8. Em termos de governação, considera que poderia a Comissão de Acompanhamento do SIGDN ser a base para assumir a responsabilidade pelo programa de atualização das TIC?
9. A haver uma modernização das TIC, mesmo sendo dada prioridade aos sistemas de comando e controlo militar, deveria envolver todas as entidades da Defesa, ou restringir-se ao EMGFA, órgãos dele dependentes e ramos?

Questões colocadas ao escalão operacional

1. A infraestrutura TIC em utilização na sua organização, incluindo a arquitetura e implementação, foi coordenada de alguma forma com os restantes ramos, órgãos ou entidades da Defesa?
2. Já alguma vez ocorreram interrupções no fornecimento de serviços TIC, que não fossem possíveis de restabelecer por falta de sistemas alternativos de *backup*?
3. Considera que existe interoperabilidade e compatibilidade entre as TIC que são utilizados atualmente no EMGFA, ramos, órgãos e entidades?
4. Considera que nos vários locais de operação, incluindo estrangeiro, é possível estabelecer e manter o acesso aos serviços TIC de forma simples e transparente (incluindo a qualidade das comunicações e diversidade de serviços)?
5. Quantos elementos existem atualmente na sua organização para efetuar a gestão e apoio das TIC (centros de dados, equipamentos, serviços, etc.) e quantos estão previstos existirem?
6. Tem havido renovação / contratação / recrutamento de pessoal em quantidade suficiente para as funções TIC? Qual a perspetiva de evolução futura?
7. Considera que a formação dos novos elementos existe em quantidade e qualidade adequada? E no que toca a atualização de conhecimentos?
8. Considera que a nível de conhecimentos e proficiência, é fácil o intercâmbio e integração do pessoal das TIC, entre os diversos locais possíveis de colocação na Defesa?

9. Tem conseguido obter o financiamento necessário e adequado para a aquisição e manutenção dos equipamentos e serviços TIC, incluindo para as licenças necessárias?
10. Considera que haveria vantagens na gestão centralizada de identidades, autenticação, autorização e controlo de acesso dos utilizadores?
11. Encontra vantagens na possibilidade de os vários serviços TIC comuns poderem ser geridos e fornecidos de forma centralizada?
12. Em relação às soluções anteriores TIC que existiam, quais foram as vantagens e desvantagens que o SIGDN trouxe em termos de: pessoal dedicado aos sistemas e equipamentos, recursos financeiros e à sua fiabilidade.
13. Concorda com a solução para a modernização das TIC da Defesa Nacional apresentada?
14. Que vantagens e desvantagens encontra na solução proposta?

Síntese da informação recolhida nas entrevistas

SIGDN:

Foi unanimemente reconhecido que o SIGDN trouxe poupanças em recursos humanos, que estavam alocados à parte da manutenção e desenvolvimento das aplicações que substituiu. Igualmente se traduziu em poupanças financeiras devido a esses mesmos aspetos e incluindo as necessidades de *hardware.* Permitiu ainda uniformizar os procedimentos a nível da DN.

Como desvantagens foi indicado que há alguma dificuldade quanto à flexibilidade para atender a situações específicas dos ramos e na demora com que são implementadas alterações, devido à necessidade de harmonização entre as várias entidades. Verifica-se também que as entidades têm a tendência de não considerarem o SIGDN como um recurso próprio.

Arquiteturas TIC:

Todos confirmaram que as arquiteturas TIC que utilizam foram estabelecidas de forma independente em relação às restantes, e que devido a isso, naturalmente são diferentes entre elas.

Interoperabilidade:

O SIGDN e a Ciberdefesa foram apresentados como os grandes exemplos de interoperabilidade. Devido às redes de dados estarem baseadas em tecnologias padrão,

permitem que haja sempre alguma interoperabilidade entre elas. A dificuldade prende-se com o facto de haver várias arquiteturas em utilização, assim como SI, que não são compatíveis entre si. Foi apontada a necessidade de se definir uma arquitetura comum para possibilitar a interoperabilidade entre as entidades da DN. Houve unanimidade na opinião de que serviços TIC comuns apresentam vantagens, sendo, no entanto, necessário acautelar os que são específicos e os operacionais.

RH:

Os recursos humanos foram por todos considerado o aspeto mais crítico. A grande dificuldade prende-se em conseguir pessoal devidamente habilitado com a formação necessária. O recrutamento deste tipo de pessoal é extremamente difícil, por haver melhores condições a nível civil, e o número de ingressos para os quadros permanentes é insuficiente. Este é o recurso que se considera que num futuro próximo coloca as TIC em causa, sendo urgente tomar medidas. Foi por todos considerado que a centralização das TIC pode ser uma forma de mitigar o problema. Foi ainda referida a necessidade de se encontrarem outras medidas para resolver a situação. Uma das dúvidas presentadas prende-se com o receio de uma solução comum para as TIC poder implicar a redução dos RH nos ramos colocando em causa as suas próprias necessidades.

A nível da formação não foram identificadas grandes necessidades, para além da dificuldade de não se conseguir recrutar pessoal para a área com formação de base adequada. Também no que toca à proficiência do pessoal não foram indicados problemas, não têm sido identificados problemas a esse nível com as colocações noutras entidades da DN.

Orçamento:

Atualmente os orçamentos do SIGDN, da RFCM e da Ciberdefesa já estão centralizados na SGMDN e no EMGFA. Foi opinião geral que em termos orçamentais o estabelecimento de serviços comuns pode permitir economias de escala e reduzir os respetivos custos. Uma dúvida apresentada, prende-se com as potenciais dificuldades que podem advir da lei da contratação pública com o aumento dos valores dos contratos trazidos pela centralização do fornecimento dos serviços.

Administração de uma infraestrutura comum:

Em termos da administração de uma infraestrutura TIC comum, os entrevistados consideraram que esta deveria ficar a cargo da SGMDN, como atualmente acontece no caso do SIGDN, e do EMGFA, no que toca às infraestruturas de comunicações.

Proposta de rede única apresentada:

Em termos da proposta de rede única que lhes foi apresentada houve uma concordância generalizada. Foi referida a necessidade e acautelar as especificidades de cada ramo e as questões de cariz identitário. Igualmente se torna necessário acautelar os sistemas específicos das entidades e acima de tudo planear a alocação de recursos humanos.

Vantagens percecionadas com a rede única:

- Obtenção do efeito de economia de escala nos processos de aquisição e de manutenção da área de TIC;
- Racionalização dos recursos humanos, evitando duplicação das estruturas de administração e de apoio nas diferentes entidades;
- Criação de mais condições para aplicação de políticas de cibersegurança eficazes;
- Uniformização de procedimentos e familiarização de todas as entidades com as mesmas ferramentas, potenciando o funcionamento em ambiente conjunto;
- Aumento da interoperabilidade entre as diversas entidades da Defesa Nacional.

Desvantagens

- Dependência dos ramos para a gestão e administração de recursos na área das TIC;
- Redução dos níveis de RH colocando em causa as necessidades dos ramos;
- Aumento na demora da resolução de problemas;
- Existência de um risco de os acordos de nível de serviço não serem cumpridos como esperado.

Apêndice E – Sistemas transversais da DN

A SGMDN, de acordo com a alínea h) do n.º2 do artigo 2.º do Decreto Regulamentar n.º 6/2015, de 31 de julho, tem a atribuição de implementar uma política integradora para a área dos SI e TIC no universo da defesa nacional, competindo-lhe coordenar e administrar os SI/TIC de natureza comum. A definição de requisitos operacionais e técnicos, da segurança e da gestão dos sistemas de comando e controlo militares são da responsabilidade da FFAA.

No âmbito dessa atribuição a SGMDN tem centralizados no CDD vários SI de gestão comuns, assim como o respetivo orçamento, designadamente e entre outros (R. A. Francisco, *op. cit.*):

- O SIGDN, quer ao nível do suporte *SAP*, quer no respeitante ao suporte ao desenvolvimento e manutenção dos diversos módulos e serviços, totalizando cerca de 2 M€/ano;
- O Sistema Integrado de Gestão Documental, incluindo a despesa associada à sua implementação faseada (implementada a fase 1 de 3 que inclui a expansão do sistema na Marinha e na SGMDN e a sua instalação na Polícia Judiciária Militar, Direção Geral da Política da Defesa Nacional e Inspeção Geral da Defesa Nacional, bem como a interoperabilidade entre todas estas instâncias que se encontra em curso) e a manutenção anual;
- O Sistema de Informação de Avaliação do Mérito dos Militares das Forças Armadas, incluindo os custos de implementação efetuados (o sistema encontra-se em exploração) e a sua manutenção anual;
- As Instituições da Memória da Defesa Nacional (https://portalmemoria.defesa.gov.pt) que disponibiliza acesso a virtualmente todo o acervo dos museus, arquivos e bibliotecas da DN, incluindo o seu desenvolvimento (encontra-se em exploração desde 2018) e a sua manutenção anual;
- Portal Internet da Defesa Nacional (https://www.defesa.gov.pt/), incluindo desenvolvimento e manutenção anual.

Apêndice F – Corpo de Conceitos

De seguida apresentam-se os conceitos fundamentais utilizados no trabalho de modo a garantir uma melhor compreensão do estudo:

Apoio de primeira, segunda e terceira linha – Nível de apoio prestado aos utilizadores: primeira linha – balcão de atendimento, segunda linha – técnico de IT e terceira linha – perito de IT, apoio externo ou do vendedor (Zitek, s. d.).

Centro de Dados − É uma rede de recursos de computação e armazenamento que permite a entrega de aplicações e dados de software partilhados (CISCO, s. d.).

Cloud Computing − É um modelo que permite o acesso a aplicações e serviços, debaixo de uma infraestrutura partilhada, com recurso a plataformas tecnológicas configuráveis e diferenciadas e com grande capacidade de armazenamento e resiliência (National Institute of Standards and Technology, 2011).

Disponibilidade – Capacidade de uma unidade funcional estar num estado capaz de executar a função necessária sob determinadas condições, num dado instante de tempo ou durante um determinado intervalo de tempo, assumindo que os recursos externos necessários são fornecidos (NATO, 2005).

Escalabilidade – É a capacidade de um sistema em aumentar ou diminuir o seu desempenho em resposta a alterações às solicitações de processamento por parte de aplicações e sistemas. (Gartner, s. d.).

Information Technology – Arte e ciências aplicadas que tratam de operações de dados e informações. As áreas de intervenção incluem: teoria da informação, operações aritméticas e lógicas, organização de dados, representação, transferência, troca e processamento, técnicas de operação, tecnologia de equipamentos, desenvolvimento e manutenção de sistemas, segurança e interoperabilidade, interconexão de sistemas, automação de processos, inteligência artificial, multimédia e hipermédia (NATO, 2005).

Infrastructure as a Service − É uma infraestrutura de computação, rede e armazenamento, instantânea, vigiada e gerida remotamente (Microsoft, s. d.).

Interoperabilidade – Capacidade de organizações díspares e diversas de interagirem com vista à consecução de objetivos comuns com benefícios mútuos e definidos de comum acordo, num processo que implica a partilha de informações e conhecimentos entre as organizações no âmbito dos processos produtivos a que dão apoio, mediante o intercâmbio de dados entre os respetivos sistemas e TIC (CE, 2010a, p. 34).

Local Area Network – Uma rede de dados local que liga computadores numa área relativamente pequena (IBM, 2019).

Rede de computadores – Compreende dois ou mais computadores interligados com o objetivo de transmitir, partilhar, ou trocar dados e recursos (IBM, 2019).

Redundância – A existência de um meio, além dos meios que seriam suficientes, para uma unidade funcional executar a função requerida ou para que os dados signifiquem informação (NATO, 2005).

Resiliência – A capacidade de uma unidade funcional em continuar a executar a função necessária na presença de falhas ou erros (NATO, 2005).

Serviço – Meios ou funcionalidades que satisfaçam os requisitos de troca e processamento e informação aos utilizadores das TIC (MDE, 2017a, pp. 109-110).

Sistema de Informação – Um conjunto de equipamentos, métodos e procedimentos e se necessário, pessoal, organizados para realizar as funções de processamento de informações (NATO, 2014).

Superioridade de Informação – Capacidade de conseguir entregar as informações corretas às pessoas certas no momento certo. É a vantagem operacional que advém da capacidade de recolher, processar e disseminar um fluxo ininterrupto de informação enquanto se explora ou nega a capacidade a um adversário de fazer o mesmo (NATO, 2015).

Tecnologias de Informação e Comunicações – Tecnologias de hardware, de software e de comunicações, utilizadas na conversão, armazenamento, proteção, processamento, transmissão e recuperação de informação. (CE, 2010a, p 37). Por TIC designam-se o conjunto de artefactos tecnológicos que instrumentam o habitat humano, 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 são desencadeadas em consequência das decisões que se tomam (GPTIC, 2012, p.3).

Wide Area Network – Rede de dados que liga computadores abrangendo uma grande área geográfica, que pode ser de região para região ou mesmo de continente para continente (IBM, 2019).