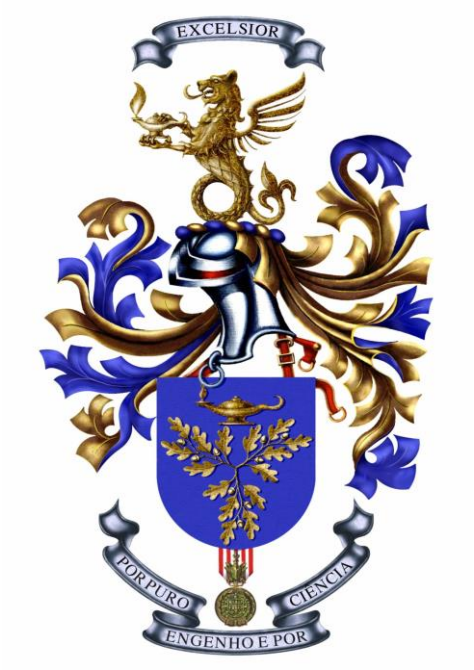
INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE PROMOÇÃO A OFICIAL GENERAL
2020/2021



TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

BIG DATA: DESAFIOS AO ARMAZENAMENTO DE DADOS NAS FORÇAS ARMADAS

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

Ana Cristina Domingos de Oliveira Rodrigues Telha
CORONEL ENGENHEIRA INFORMÁTICA

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

BIG DATA: DESAFIOS AO ARMAZENAMENTO DE DADOS NAS FORÇAS ARMADAS

COR/ENGINF Ana Cristina Domingos de Oliveira Rodrigues Telha

Trabalho de Investigação Individual do CPOG

Pedrouços 2021

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

BIG DATA: DESAFIOS AO ARMAZENAMENTO DE DADOS NAS FORÇAS ARMADAS

COR/ENGINF Ana Cristina Domingos de Oliveira Rodrigues Telha

Trabalho de Investigação Individual do CPOG

Orientador: CMG EMA Luís Eduardo Moita Rodrigues

Pedrouços 2021

Declaração de compromisso Antiplágio

Eu, **Ana Cristina Domingos de Oliveira Rodrigues Telha**, declaro por minha honra que o documento intitulado ***Big Data*: desafios ao armazenamento de dados nas Forças Armadas,** corresponde ao resultado da investigação por mim desenvolvida, enquanto auditora do **CPOG** 2020/2021 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, 18 de julho de 2021

Ana Cristina Domingos de Oliveira Rodrigues Telha
Coronel Engenheira Enformática

Assinado por : **ANA CRISTINA DOMINGOS DE OLIVEIRA RODRIGUES TELHA**
Num. de Identificação: 10038519
Data: 2021.07.18 15:54:21+01'00'

CARTÃO DE CIDADÃO

Agradecimentos

O desenvolvimento deste trabalho, enriquecedor na perspetiva do conhecimento, e motivador, pela minha experiência passada e pela temática potencialmente inovadora e contribuidora para a melhoria das Tecnologias de Informação e Comunicação nas Forças Armadas, não é um ato isolado, mas sim a incorporação do contributo e do saber de diversas fontes, a quem reitero o meu sincero agradecimento.

Ao meu orientador, Sr. Capitão-de-mar-e-guerra Moita Rodrigues, pelo apoio demonstrado desde o primeiro dia, e pelos sábios e ponderados contributos para as decisões tomadas ao longo do percurso.

À Tenente-coronel Cristina Fachada, incansável no apoio prestado, e cujo saber, organização e método me facultaram contributos valiosos.

A todos os entrevistados, um agradecimento especial pela disponibilidade e pelos contributos prestados, resultantes da sua vasta experiência e conhecimento na área, que permitiram valorizar e robustecer as conclusões e resultados apresentados.

Ao Coronel José Mendes, ao Tenente-coronel Bruno Cabaço, ao Tenente-coronel António Valente e ao Major Miguel Maria, a quem recorri inúmeras vezes em busca de esclarecimentos, de documentação de suporte e de pontos de vista distintos que permitiram o trilhar do caminho escolhido.

Aos camaradas do Curso de Promoção a Oficial General 2020/2021, um curso *sui generis* pela componente decorrida de forma remota, mas que, ainda assim, permitiu criar laços de amizade, e reforçar o espírito de entreajuda.

Por fim, à minha família, pilar de suporte fundamental, que me apoiou ao longo deste percurso. Ao meu marido, aos meus filhos, em particular, fonte de orgulho e de motivação, e aos meus pais, a quem devo o que hoje sou, esperando que esta nova etapa seja para eles motivo de orgulho redobrado.

Índice

Índice de Apêndices

Índice de Figuras

Resumo

O crescimento exponencial de dados, provenientes de múltiplas fontes e a velocidades diversas, utilizados para a execução dos processos e o apoio à tomada de decisão, torna premente nas organizações, em geral, e nas Forças Armadas, em particular, a existência de estruturas adequadas ao seu armazenamento e processamento, de forma a permitir a sua plena exploração utilizando tecnologias inovadoras.

É, assim, objetivo deste estudo avaliar formas de otimizar o modelo de armazenamento e processamento de dados em vigor nas Forças Armadas, à luz dos requisitos emergentes associados ao *Big Data*, seguindo um raciocínio indutivo, uma estratégia de investigação qualitativa e um desenho de pesquisa do tipo de estudo de caso.

Através da análise documental de estratégias implementadas pela *North Atlantic Treaty Organization* e pelas áreas da Defesa de França e Estados Unidos da América, e de conteúdo dos dados das entrevistas semiestruturadas realizadas a 13 *experts* da Defesa Nacional, do Gabinete Nacional de Segurança e de órgãos associados à investigação e ensino, foram propostas várias medidas, organizadas por vetores de edificação de capacidades militares, tendentes à incorporação de modelos *cloud computing* na capacidade de armazenamento e processamento de dados das Forças Armadas, de acordo com a premissa *cloud first*.

Palavras-chave: Armazenamento e Processamento de Dados, *Cloud Computing*, *Big Data*, Forças Armadas.

Abstract

The exponential growth of data, incoming from multiple data sources, at different rates, used in process execution and decision making processes, demands for proper storage and processing structures in Organizations, in general, and in the Armed Forces, in particular, in order to allow its adequate exploitation using innovative technologies.

The purpose of this research is to evaluate ways to optimize the data storage and processing models used in the Armed Forces, in light of Big Data emergent requirements, using inductive reasoning, a qualitative research strategy and a case study approach.

Through documental analysis on the strategies implemented by North Atlantic Treaty Organization and the defense areas of France and the United States of America, as well as data contents resulting from the interviews convened to 13 experts on National Defense, the National Security Office and academia and research entities, a set of measures is presented, grouped by military capabilities building vectors, in order to incorporate cloud computing models in the Armed Forces data storage and processing capability, under the cloud first premise.

Keywords: *Data Storage and Processing, Cloud Computing, Big Data, Armed Forces.*

Lista de abreviaturas, siglas e acrónimos

A

AP	Administração Pública
APEC-SIFICAP	Sistema de Apoio ao Planeamento, Execução e Controlo da Atividade de Fiscalização Marítima no âmbito do Sistema de Fiscalização e Controlo das Atividades de Pesca
AMA	Agência para a Modernização Administrativa
ARTEMIS	*Architecture de Traitement et d'Exploitation Massive de l'Information multi-Sources*

B

B	*Byte*
BI	*Business Intelligence*

C

C2	Comando e Controlo
C3B	*Consultation, Command and Control Board*
CapEx	*Capital Expenditure*
CD	Centro de Dados
CDD	Centro de Dados da Defesa
CE	Comissão Europeia
CEM	Conceito Estratégico Militar
CIO	*Chief Information Officer*
CPOG	Curso de Promoção a Oficial General
CSI	Comunicações e Sistemas de Informação
CSP	*Cloud Service Provider*

D

DAGI	Direção de Análise e Gestão da Informação
DCSI	Direção de Comunicações e Sistemas de Informação
DGNUM	*Direction générale du numérique et des systèmes d'information et de communication*

DINSIC	*Direction interministérielle du numérique et du système d'information et de communication de l'Etat*
DIRCSI	Direção de Comunicações e Sistemas de Informação
DIRISI	*Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information de la Défense*
DITIC	Direção de Tecnologias de Informação e Comunicações
DN	Defesa Nacional
DoD	*Department of Defense*
DOTMLPII	Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade
DSSI	Direção de Serviços dos Sistemas de Informação

E

EB	*Exabyte*
EMGFA	Estado-Maior-General das Forças Armadas
ENISA	*European Union Agency for Cybersecurity*
EUA	Estados Unidos da América

F

FA	Força Aérea
FFAA	Forças Armadas
FMN	*Federated Mission Networking*

G

GB	*Gigabyte*
GNS	Gabinete Nacional de Segurança
GPTIC	Grupo de Projeto para as Tecnologias de Informação e Comunicação

H

HQ	*HeadQuarters*

I

IA	Inteligência Artificial

IaaS	*Infrastructure as a Service*
IBM	*International Business Machines Corporation*
ISACA	*Information Systems Audit and Control Association*
IUM	Instituto Universitário Militar

J

JEDI	*Joint Enterprise Defense Infrastructure*

K

KB	*Kilobyte*

L

LPM	Lei de Programação Militar

M

MB	*Megabyte*
MDN	Ministério da Defesa Nacional
Minarm	*Ministère des Armées*

N

NATO	*North Atlantic Treaty Organization*
NCIA	*NATO Communications and Information Agency*
NCS	*NATO Command Structure*
NFS	*NATO Force Structure*
NIST	*National Institute of Standards and Technology*

O

OE	Objetivo Específico
OG	Objetivo Geral

P

PaaS	*Platform as a Service*
PB	*Petabyte*

POCEAD	*Plateforme d'Ouverture, de Centralisation, d'Exposition et d'Analyse des Données*
PS3	*Portuguese Sky Sentinel System*

Q

QC	Questão Central
QD	Questão Derivada

R

RCM	Resolução do Conselho de Ministros
RH	Recursos Humanos

S

SaaS	*Software as a Service*
SAMA	Sistema de Apoio à Modernização Administrativa
SGMDN	Secretaria-Geral do Ministério da Defesa Nacional
SIGDN	Sistema Integrado de Gestão da Defesa Nacional
SLA	*Service-Level Agreement*
SI	Sistema de Informação

T

TB	*Terabyte*
TIC	Tecnologias de Informação e Comunicação

U

UE	União Europeia
USDoD	*United States Department of Defence*

Y

YB	*Yottabyte*

Z

ZB	*Zettabyte*

1. Introdução

O desenvolvimento das Tecnologias de Informação e Comunicação (TIC) permitiu que as organizações alterassem a forma como desenvolvem os seus processos, transformando-as, gradualmente, em organizações digitais (*North Atlantic Treaty Organization* [NATO], 2019b). Os dados assumem-se como um elemento estratégico, a par dos recursos materiais e humanos, tornando premente a existência de tecnologias e estruturas organizacionais que permitam o seu eficaz tratamento e utilização (Cavanillas, Curry, & Wahlster, 2016).

A NATO categoriza a informação como um recurso corporativo, que deve ser gerido, através de organização e controlo, ao longo de todo o seu ciclo de vida, independentemente do meio e formato de suporte, de forma a apoiar as missões, os processos de consulta, a tomada de decisão e os requisitos operacionais por si estabelecidos (NATO, 2007, p. 1-1).

A União Europeia (UE), reconhecendo o potencial residente na correta utilização dos dados em áreas como a saúde, o ambiente, os mercados, os serviços públicos e a governação, publicou, em fevereiro de 2020, "Uma estratégia europeia para os Dados", com um conjunto de medidas para os cinco anos seguintes, que permitam "[…] o desenvolvimento da economia dos dados" (Comissão Europeia [CE], 2020, p. 2).

O volume de dados produzidos tem-se multiplicado rapidamente nos últimos anos, resultado da proliferação de fontes (em número e em diversidade), e estima-se que continue a crescer, situando-se o fator comum das previsões na ordem de grandeza do *Zettabyte* (ZB)[1] (Espinosa, Kaisler, Armour, & Money, 2019).

Em 2018, a Corporação Internacional de Dados[2] (2018, cit. por CE, 2020) estimava que, em 2025, o total de dados produzidos e armazenados no mundo atingiria o volume de 175ZB, contrastando com os 33ZB então existentes, colocando em causa os modelos de armazenamento de dados tradicionais implementados pelas organizações, e apresentando novos desafios relativamente à disponibilidade de recursos (El-Seoud, El-Sofany, Abdelfattah, & Mohamed, 2017).

A reformulação das infraestruturas de armazenamento e processamento de dados no Estado Português é um desiderato desde 2011, aquando do início do processo de racionalização e redução de custos com as TIC na Administração Pública (AP) do Estado

[1] A medição do volume de dados é efetuada de acordo com as seguintes ordens de grandeza (*Data Storage Solutions Review*, 2020): *bit*; *Byte* (B), 8*bits*; *Kilobyte* (KB), 1024B; *Megabyte* (MB), 1024KB; *Gigabyte* (GB), 1024MB; *Terabyte* (TB), 1024GB; *Petabyte* (PB), 1024TB; *Exabyte* (EB), 1024PB; *Zettabyte* (ZB), 1024EB; *Yottabyte* (YB), 1024ZB.

[2] Tradução da UE de *International Data Corporation*.

(Resolução do Conselho de Ministros [RCM] n.º 46/2011, de 27 de outubro). Neste enquadramento, a redução do número de centros de dados (CD), a racionalização de serviços e a adoção de serviços na *cloud* constam em diversas iniciativas encetadas em 2012, através do "Plano Global Estratégico de Racionalização e Redução de custos nas TIC, na AP*"* (RCM n.º 12/2012, de 12 de janeiro).

A "Estratégia *Cloud* para a AP em Portugal", recentemente aprovada, veio apresentar um conjunto de medidas a implementar na AP, tendentes à utilização de serviços *cloud*, assentes na visão da "adoção de *cloud* pública, sempre que possível, em modelo inteligente, seguro e eficiente" (Agência para a Modernização Administrativa [AMA], 2020, p. 4).

No universo da Defesa Nacional (DN), os princípios de racionalização de recursos e rentabilização de meios, já plasmados no Conceito Estratégico de Defesa Nacional (RCM n.º 19/2013, de 21 de março), foram ainda reforçados na determinação da reforma estrutural na DN e nas Forças Armadas (FFAA) (RCM n.º 26/2013, de 11 de abril), bem como no Conceito Estratégico Militar (CEM) (Ministério da Defesa Nacional [MDN], 2014).

Atualmente, as entidades consideradas neste estudo, são detentoras de infraestruturas de armazenamento e processamento de dados próprias, que exploram autonomamente, desde a conceção da arquitetura de sistemas e serviços, ao processo aquisitivo de *hardware* e *software*, à sustentação, à exploração de sistemas e à continuidade de serviços (Ferreira, 2020).

Esta investigação assume, assim, particular relevância, no sentido de tornar compatível o modo como os dados são armazenados e processados na DN com modelos mais adequados aos fluxos de produção e acesso aos dados e às necessidades de informação para apoio à tomada de decisão.

O presente estudo tem então por objeto o armazenamento e processamento de dados e foi delimitado (Santos & Lima, 2019):

- Temporalmente, à atualidade (período 2020-2021), considerando o percurso evolutivo anterior em termos de legislação, normativos e tecnologias;

- Espacialmente, às FFAA e ao MDN (serviços centrais e entidades na sua dependência), dado que a Secretaria-Geral do MDN (SGMDN) é responsável por diversos sistemas em exploração de forma transversal na Defesa;

- Em conteúdo, à adequabilidade da adoção de novos modelos de armazenamento e processamento de dados, designadamente o modelo *cloud computing*, e da sua possível integração na arquitetura de serviços TIC da Defesa, incorporando os requisitos associados a sistemas que tratam *Big Data*.

Neste enquadramento, esta investigação tem como objetivos geral (OG) *Propor contributos para otimizar o modelo de armazenamento e processamento de dados nas FFAA na era do Big Data*, e específicos (OE):

OE1: Analisar o modelo de armazenamento e processamento de dados nas FFAA na era do *Big Data*;

OE2: Analisar a estratégia em matéria de armazenamento e processamento de dados de entidades congéneres na era do *Big Data*.

A questão central (QC) de investigação *Como contribuir para otimizar o modelo de armazenamento e processamento de dados nas FFAA na era do Big Data?* encontra-se alinhada com estes objetivos.

Estruturalmente, este documento encontra-se organizado em sete capítulos. Este primeiro, que introduz o tema. Um segundo, respeitante à revisão da literatura e apresentação do modelo de análise proposto. O terceiro, concernente à metodologia e ao método utilizados. Os quarto, quinto e sexto, relativos à análise dos dados, discussão dos resultados e resposta às questões de investigação. O sétimo, e último, ancorado nas conclusões, contributos para o conhecimento, limitações, proposta de estudos futuros e recomendações de ordem prática.

2. Enquadramento teórico e concetual

Neste capítulo são estudados, em termos de revisão da literatura, os conceitos estruturantes para o trabalho e apresentado o modelo de análise adotado.

2.1 Estado da arte e conceitos estruturantes

2.1.1 Armazenamento e processamento de dados

Tomando em consideração os objetivos estabelecidos para a investigação, o conceito de armazenamento e processamento de dados será analisado na perspetiva do modelo de implementação na *cloud*, por oposição ao modelo de implementação tradicional.

Por modelo tradicional entende-se aquele em que os recursos de computação e armazenamento são escalados de forma vertical, aumentando a capacidade de processamento e/ou armazenamento ao *hardware* existente (*National Institute of Standards and Technology* [NIST], 2015), dimensionando o sistema com recursos que poderão não ser utilizados durante períodos consideráveis, e em que a organização, por norma, é proprietária e responsável pelos recursos, ao longo do seu ciclo de vida (aquisição, instalação, configuração e gestão), em instalações próprias, *on-premises* (*International Business Machines Corporation* [IBM], 2020).

Por outro lado, *cloud computing* traduz um modelo que permite o acesso a um conjunto de recursos de computação (redes, servidores, armazenamento, aplicações e serviços), em rede, a pedido, sendo a atribuição e libertação de recursos realizada de forma dinâmica e com uma muito reduzida intervenção do prestador de serviços (*Cloud Service Provider* – CSP) (NIST, 2011).

O modelo *cloud* é caracterizado (IBM, 2020; NIST, 2011):

- Pela disponibilização automática de recursos, nomeadamente capacidade de processamento e/ou armazenamento, mediante a necessidade do utilizador;

- Pelo acesso a uma *pool* de recursos disponíveis em rede. O utilizador abstrai-se da implementação física dos recursos, podendo, contudo, ter determinado nível de controlo sobre os mesmos (por exemplo, o país, a região, ou até o CD onde estão implementados);

- Pela rápida escalabilidade e elasticidade, permitindo ao utilizador dispor dos recursos quando necessita e libertá-los quando já não são necessários. Esta característica permite às organizações evitar investimento em recursos que se mantêm por utilizar durante períodos consideráveis;

- Pelo controlo e monitorização da utilização de recursos, permitindo às organizações uma visão clara dos custos relacionados com os serviços, que são cobrados de acordo com a utilização.

No modelo *cloud*, o armazenamento e processamento de dados pode ser efetuado utilizando quatro modelos de implementação (IBM, 2020; NIST, 2011):

- O privado, em que a infraestrutura de suporte e todos os recursos associados à *cloud* são dedicados a uma única entidade. Pode ser implementado em instalações próprias, em instalações do CSP ou em instalações de terceiros contratualizadas para o efeito, e os recursos humanos (RH) envolvidos podem ser exclusivamente da organização, pertencentes a parceiros da área TIC ou ambos;

- O comunitário, caracterizado por disponibilizar serviços a um conjunto de organizações com propósitos afins. O conceito de propriedade e gestão de recursos é semelhante ao do modelo privado, mas com uma ou mais organizações envolvidas a disponibilizar instalações ou RH;

- O público, implementado com recurso a prestadores de serviços, em *clouds* públicas. O CSP é responsável por toda a infraestrutura de suporte ao armazenamento e/ou computação, e por vezes pela disponibilização de ligações com elevada largura de banda, de forma a cumprir com níveis de serviço pré-estabelecidos. A infraestrutura de uma *cloud* pública é partilhada por diversos clientes, designados por inquilinos (*tenants*);

- O híbrido, que resulta de uma composição dos modelos anteriores, envolvendo duas ou mais infraestruturas *cloud*. A articulação é efetuada através de uma camada de orquestração de serviços, que permite efetuar trocas de dados e balancear a carga de processamento de acordo com as necessidades da organização.

Em matéria de modelos de serviços disponibilizados sobre a *cloud*, e conforme esquematizado na Figura 1, os três principais são (IBM, 2020; NIST, 2011):

- *Infrastructure as a Service* (IaaS), que consiste em disponibilizar ao utilizador recursos de processamento, armazenamento e *networking*, residentes em infraestruturas propriedade do CSP. Estes recursos são atribuídos mediante necessidade (*on-demand*), e a sua utilização taxada em função do consumo (o denominado *pay-as-you-go*). O consumidor gere os sistemas operativos, aplicações e serviços que instala na infraestrutura, e pode controlar o armazenamento e alguns elementos de gestão de rede. Por forma a incrementar a resiliência do serviço prestado e a evitar pontos únicos de falha, alguns CSP implementam regras na forma como os recursos são física e geograficamente distribuídos,

nomeadamente através da constituição de regiões e, dentro destas, de zonas de disponibilidade. A categorização por regiões e zonas é feita em função da autonomia de capacidades como o fornecimento de energia e infraestrutura de rede. Esta característica torna o modelo *cloud* adequado à implementação das capacidades de *backup* e *disaster recovery* (conforme Apêndice A). O IaaS está ainda vocacionado para a disponibilização de ambientes de desenvolvimento e teste aplicacionais, processamento de dados em contexto analítico e armazenamento de dados;

- *Platform as a Service* (PaaS), adicionalmente à camada IaaS, o PaaS disponibiliza as ferramentas necessárias ao desenvolvimento de aplicações, nomeadamente *middleware*, gestão de bases de dados, sistemas operativos e ferramentas de desenvolvimento suportadas pelo CSP. O consumidor tem apenas acesso ao ambiente de desenvolvimento de aplicações, e à configuração do seu ambiente de exploração;

- *Software as a Service* (SaaS), contempla a entrega de aplicações como um serviço, sendo a infraestrutura a montante irrelevante para o utilizador, que tem sempre ao seu dispor a versão mais atualizada da aplicação.

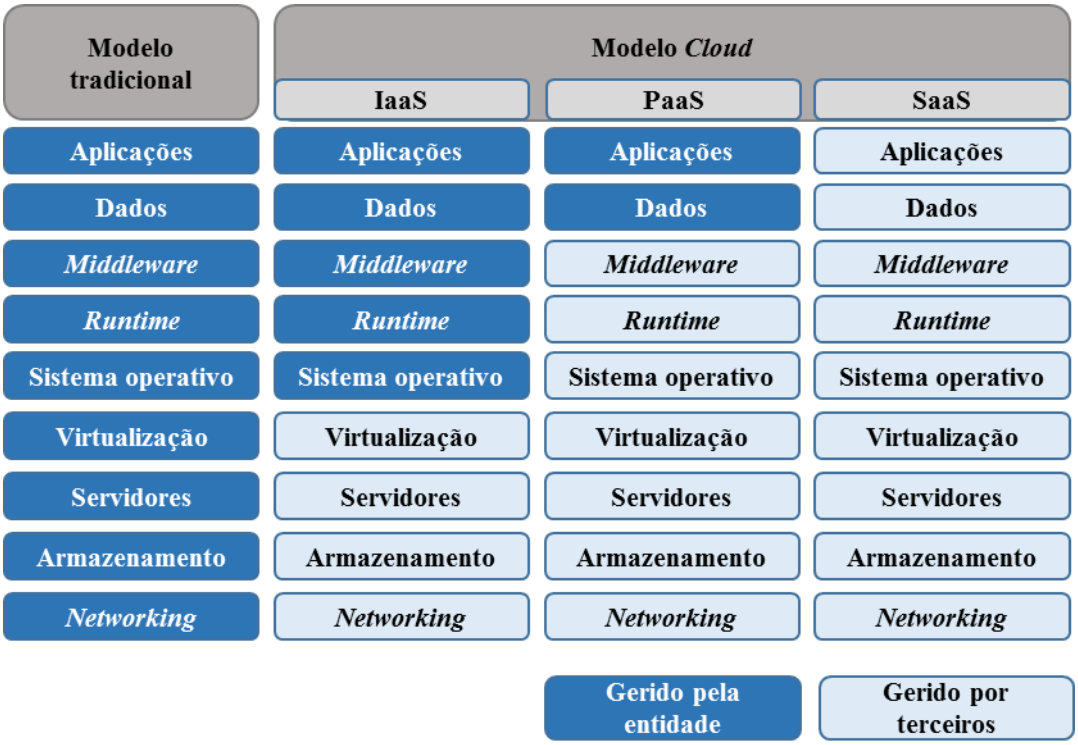


Figura 1 – Modelos de disponibilização de serviços
Fonte: Adaptado de AMA (2020).

A segurança é uma das principais preocupações manifestadas relativamente à adoção de um modelo público de *cloud*, existindo neste domínio várias medidas específicas a considerar, designadamente (IBM, 2020):

- Definição clara do proprietário dos dados;

- Encriptação de dados em trânsito, em utilização e em descanso, com governação dos mecanismos de encriptação pelo cliente;

- Total visibilidade sobre os mecanismos de autenticação e controlo de acesso;

- Governação e conhecimento de todos os mecanismos regulatórios aplicáveis aos dados, destacando-se o Regulamento Geral sobre a Proteção de Dados, "relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" (Regulamento do Parlamento Europeu e do Conselho n.º 679/2016, de 27 de abril, p. 1), bem como de troca de dados internos e com entidades externas.

Tendo em vista o incremento da cibersegurança e da ciber resiliência, a UE estipulou, em 2019 (Regulamento do Parlamento Europeu e do Conselho n.º 881/2019, de 17 de abril, p. 32), os objetivos e funções da Agência da União Europeia para a Cibersegurança (*European Union Agency for Cybersecurity* – ENISA), bem como

> […] um enquadramento para a criação de sistemas europeus de certificação da cibersegurança com o objetivo de assegurar um nível adequado de cibersegurança para os produtos, os serviços e os processos de TIC na União e de evitar a fragmentação do mercado interno no que toca aos sistemas de certificação da cibersegurança na União.

Em termos de implementação física, o número de CD disponibilizados pelos CSP mais relevantes, sobretudo junto das maiores economias mundiais, tem vindo a crescer na última década, com um elevado número de instalações localizadas na Europa (Maurer & Hinck, 2020, pp. 13-14), sendo que apenas uma reduzida quota deste mercado é detida por operadores estabelecidos na UE (CE, 2020). Considerando que a soberania e a jurisdição sobre os dados são fatores a tomar em consideração na adoção de serviços de *clouds* públicas, a falta de prestadores de serviços europeus condiciona a adoção deste tipo de serviços por entidades do setor público na Europa (Cavanillas et al., 2016).

Por outro lado, os prestadores de serviço com sede fora da UE poderão estar sujeitos à legislação de países terceiros, não conforme com a legislação europeia em matéria de proteção de dados, subsistindo preocupações no que respeita ao acesso aos dados, como

sucede, por exemplo, com "várias leis chinesas relacionadas com a cibersegurança e os serviços nacionais de informações", e com a Lei CLOUD norte-americana, cujo fundamento se relaciona com o acesso a dados no âmbito de investigações criminais, mas que suscita preocupações na sua compatibilização com a regulamentação (CE, 2020, p. 9).

Alinhado com a Estratégia Europeia para os dados, e tomando como foco a soberania, o governo alemão lançou em 2019 o projeto GAIA-X, com o objetivo de criar uma infraestrutura europeia de dados e de *cloud*, aberta, federada, confiável e segura, uma iniciativa que congrega atualmente esforços de mais de 300 entidades europeias (*Federal Ministry for Economic Affairs and Energy*, 2020, 2021).

A nível nacional, a Estratégia para a AP preconiza a seleção de "localização da jurisdição de um tribunal nacional ou da comunidade europeia e em, pelo menos, dois locais geográficos redundantes" (AMA, 2020). Recentemente foi anunciada a futura disponibilização de serviços de *cloud* pública de um dos principais CSP, com alojamento de dados em território nacional (Jornal Económico, 2021), bem como a implementação de um CD de grandes dimensões em Sines, até 2025, destinado a diversas aplicações comerciais e a serviços de armazenagem e processamento de dados (Governo da República Portuguesa, 2021).

2.1.2 *Big Data*

Big Data refere-se a conjuntos de dados extensos – nomeadamente em termos de volume, velocidade, variedade e/ou variabilidade (os frequentemente designados 4 V´s do *Big Data*) – cujo armazenamento, processamento e análise requerem uma arquitetura escalável e eficiente (NIST, 2015), não suprível pelos sistemas tradicionais (El-Seoud et al., 2017).

Mais detalhadamente, o volume refere-se ao crescimento exponencial de dados que se tem verificado nos últimos anos, identificando-se, a título de exemplo, a produção de 40 TB de dados/hora por uma aeronave Rafale (*Ministère des Armées*, 2019). A velocidade reporta-se às elevadas taxas de atualização e transmissão de dados (Mazumdar, Seybold, Kritikos, & Verginadis, 2019). A variedade respeita aos diferentes formatos de dados produzidos (vídeo, mensagens de texto, áudio, registos de sensores e de *logs*), a partir de uma variedade de fontes (sensores, aplicações, Internet) (NIST, 2018). A variabilidade, para finalizar, refere-se à alteração dos dados ao longo do tempo (NIST, 2015).

Alguns exemplos de áreas de aplicabilidade de *Big Data* são a medicina (extensos volumes de registos e exames médicos, que devem estar disponíveis para apoio à tomada

de decisão), as empresas fornecedoras de redes sociais e a indústria, onde sistemas de alarmística e de predição, alimentados por inúmeros sensores, permitem otimizar a gestão do ciclo de vida das máquinas (Tawalbeh & Saldamli, 2019).

Em ambiente militar, nomeadamente ao nível tático, a proliferação de sensores presentes no terreno, associada a informação disponibilizada por fontes civis, pode traduzir-se em grandes conjuntos de dados que, tratados de forma adequada, promoverão um incremento da *situational awareness* (Johnsen, 2019).

O ciclo de vida de *Big Data* apresenta especificidades que o distinguem do modelo habitual de ciclo de vida dos dados nas organizações, residindo a diferença substancial no momento do ciclo em que os dados são armazenados de forma persistente (El-Seoud et al., 2017). O desenho de um sistema *Big Data* dependerá essencialmente da tipologia de dados a tratar (em descanso – armazenados, ou em movimento – os dados são tratados à medida que são injetados) e da premência do seu tratamento, existindo aplicações em que a velocidade é fator preponderante (caso da alarmística) e outras em que a ênfase está no volume (El-Seoud et al., 2017). Num sistema tradicional, os dados são armazenados em conformidade com a forma como são inseridos no sistema ou processados (El-Seoud et al., 2017).

A finalidade do tratamento dos dados determina também a forma temporal como os mesmos são processados e disponibilizados: mediante pedido ou em intervalos regulares de processamento (Tawalbeh & Saldamli, 2019).

O volume de dados a processar e a armazenar, e as tecnologias de análise associadas a *Big Data* não são, frequentemente, compatíveis com as estruturas existentes nas organizações (Cavanillas et al., 2016). Tendo em conta a exigência de recursos de processamento e armazenamento, as soluções disponibilizadas através de *cloud computing*, pelas suas características intrínsecas, afiguram-se adequadas a sistemas *Big Data*, permitindo às organizações utilizar, mas ao mesmo tempo abstrair-se da infraestrutura computacional e de armazenamento (El-Seoud et al., 2017).

Alguns prestadores de serviços na *cloud* disponibilizam já um conjunto de ferramentas dedicadas ao processamento de *Big Data* (NIST, 2018), designado de forma genérica por *Big Data Analytics* (Tawalbeh & Saldamli, 2019).

Do ponto de vista dos RH, o relatório publicado pelo *World Economic Forum* (2020), relativo ao futuro das profissões, estimou que, até 2025, as tecnologias associadas a *cloud computing* e *Big Data Analytics* são as que apresentam maior probabilidade de

adoção por parte das organizações, incrementando a procura em profissões correspondentes, nomeadamente analistas e cientistas de dados, ao que acresce o expectável preenchimento das profissões associadas a *cloud computing* com indivíduos que transitam de outras áreas das TIC.

2.2 Modelo de análise

Esta investigação foi desenvolvida conforme o modelo apresentado no Apêndice B.

3. Metodologia e método

Este estudo enquadra-se nas Ciências Militares, designadamente na área de Técnicas e Tecnologias Militares, subárea de Comando, Controlo, Comunicações, Computadores e Informação, apresentando-se neste capítulo a metodologia e o método que o nortearam.

3.1 Metodologia

Seguiu-se um raciocínio indutivo, associado a uma estratégia de investigação qualitativa e a um desenho da pesquisa do tipo de estudo de caso (Santos & Lima, 2019).

3.2 Método

3.2.1 Participantes e procedimento

Participantes. Integraram esta investigação 13[3] *experts*: 12 militares e 1 civil, conforme Apêndice C.

Procedimento. As entidades entrevistadas foram previamente contactadas por telefone ou *email*, para averiguar da sua disponibilidade para integrar o estudo. Após confirmação, foi agendada a entrevista (presencialmente, por *email*, vídeo ou audioconferência, conforme disponibilidade e restrições associados à situação de pandemia vigente). Foram asseguradas as garantias de anonimato e confidencialidade da informação prestada, da qual todas as entidades abdicaram.

3.2.2 Instrumento(s) de recolha de dados

Foram construídos três guiões de entrevistas semiestruturadas (Apêndices D, E e F) destinados a entidades: da DN, para aferir a situação atual relativa ao armazenamento e processamento de dados, e o seu posicionamento quanto a requisitos *Big Data* e adoção de *cloud computing*; do Gabinete Nacional de Segurança (GNS), enquanto Autoridade Nacional de Segurança; associadas à investigação e ensino, de forma a apreciar possíveis contributos destas áreas para o processo de implementação de *cloud computing* nas FFAA.

3.2.3 Técnicas de tratamento dos dados

Foi efetuada uma análise qualitativa do conteúdo das entrevistas, cujo resultado foi conjugado com a análise documental e revisão da literatura de forma a permitir responder às questões de investigação.

[3] Quantitativo bem enquadrado, inclusivamente de forma superior, na dimensão (N=12) definida para "[…] grupo de informantes relativamente homogéneo" (Rego, Cunha, & Meyer Jr., 2019, p. 53).

4. Modelo de armazenamento e processamento de dados nas Forças Armadas na era do *Big Data*

Neste capítulo, e a fim de responder à Questão Derivada (QD) 1, é necessário começar por examinar o enquadramento nacional (do Estado Português) concernente a esta matéria, e apresentar a *Estratégia cloud para a AP em Portugal*, recentemente aprovada (AMA, 2020).

4.1 Enquadramento nacional

A *Estratégia cloud para a AP em Portugal* decorreu do estudo conduzido pelo Conselho para as TIC na AP, relativo à adoção de tecnologias e serviços *cloud* na AP, na sequência do qual foram evidenciadas as mais-valias que se antecipam com a adoção daqueles serviços, designadamente, a não-dispersão de RH e materiais, a centralização na aquisição de serviços e a racionalização de infraestruturas (RCM n.º 84/2020, de 1 de outubro).

Assente na visão "Adoção de *cloud* pública, sempre que possível, em modelo inteligente, seguro e eficiente", a estratégia segue os seguintes princípios orientadores (AMA, 2020, pp. 4-5):

- A segurança e soberania da informação e dos dados são requisitos críticos *ab initio*, que podem condicionar a adoção e tipo de serviços *cloud*;
- As organizações do Estado devem desenvolver as soluções recorrendo, prioritariamente, a serviços em *cloud* pública, de acordo com uma *framework* de adoção;
- Devem ser adotadas soluções de mercado e privilegiar serviços *cloud* conforme disponibilizados pelos fornecedores, minimizando customizações;
- Deve ser monitorizado detalhadamente o consumo e qualidade dos serviços *cloud*;
- Deve ser definida à partida uma estratégia operacional de saída de cada serviço *cloud*, com vista a evitar o fenómeno do *vendor lockin*[4].

Tendo em vista a sua implementação e agilização, deverão ser desenvolvidos, previsivelmente num prazo de dois anos, um conjunto de mecanismos, normativos e processos, nomeadamente um modelo de *governance*, uma *framework* de adoção de

[4] No contexto de *cloud computing*, *vendor lockin* refere-se ao fenómeno em que os clientes ficam dependentes da tecnologia disponibilizada por um CSP, sujeitando-se a questões financeiras e legais ou incompatibilidades tecnológicas no caso de pretenderem mudar para um CSP diferente (Michael et al., 2010, cit. por Opara-Martins, Sahandi, & Tian, 2016).

serviços que suporte o processo de implementação de novos serviços ou de evolução/migração de serviços já existentes, a alteração do edifício legislativo e do enquadramento processual de suporte à contratação, um plano de qualificação de RH necessários ao desenvolvimento, exploração e contratação de serviços *cloud*, a "disponibilização de peças concursais" padrão para agilização dos processos de contratação, a criação de uma ferramenta de suporte aos processos de tomada de decisão e gestão de contratos e a criação de "um modelo de partilha de recursos e conhecimento" (AMA, 2020, pp. 5-6).

Como resultado do processo de identificação de sistemas candidatos a implementação no modelo *cloud*, da análise de viabilidade do mesmo e do risco da informação processada, será proposta a implementação, de acordo com uma análise de risco, num dos seguintes modelos (AMA, 2020, pp. 30-31): "Risco elevado, *on premises* em modelo não *cloud* ou num modelo *cloud* alojado em CD geridos pela AP; Risco moderado, *cloud* híbrida com componentes mais críticas alojadas em CD geridos pela AP; Risco baixo, *cloud* pública".

4.2 Situação atual nas Forças Armadas

A análise aos modelos de armazenamento e processamento de dados em exploração nas FFAA, seguidamente apresentada, está estruturada de acordo com os vetores de edificação de capacidades militares (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade - DOTMLPII) (MDN, 2014).

Doutrina. Nenhuma das cinco entidades tem formalizadas as estratégias de armazenamento e processamento de dados em vigor, estando de forma geral implícitas em documentos estratégicos da entidade, ou concretizadas a jusante em documentos técnicos. Na SGMDN, para os projetos de *Business Intelligence* (BI) (incluindo *Big Data*), essa estratégia está "[…] implícita no Plano Estratégico [e], integra duma forma mais executiva, tal como outras, o Plano de Atividades/Gestão" (R.M. Francisco, entrevista por videoconferência, 9 de fevereiro de 2021). Na Marinha, deduz-se da Diretiva Estratégica da Marinha e de outros documentos setoriais (J.P. Roque, entrevista por videoconferência, 4 de fevereiro de 2021).

Relativamente à implementação de modelos *cloud*, não existem orientações estratégicas formalizadas, tendo apenas a Marinha referido a existência de normativos ao nível do utilizador (J.P. Roque, *op. cit.*). A atual utilização de *cloud computing* nas FFAA é constituída por iniciativas isoladas, quer de utilização de serviços SaaS (SGMDN, Estado-

Maior-General das Forças Armadas [EMGFA] e Marinha), nomeadamente ferramentas de produtividade e colaborativas (R.M. Francisco, *op. cit.*, J.A. Rocha, entrevista por *email*, 13 de abril de 2021, J.P. Roque, *op. cit.*), quer de implementação de projetos internos em modelos privados (Exército) (L.F. Camelo, entrevista por *email*, 25 de fevereiro de 2021). Na Marinha, a utilização deste tipo de serviços foi impulsionada pela situação resultante da pandemia COVID-19, a partir de março de 2020 (J.P. Roque, *op. cit.*).

Organização e Liderança. Todas as entidades compreendem, na sua estrutura organizacional, uma área responsável pela gestão do ciclo de vida da respetiva infraestrutura TIC:

- SGMDN: Direção de Serviços dos Sistemas de Informação (DSSI) e Direção de Serviços do Centro de Dados da Defesa (CDD);

- EMGFA: Direção de Comunicações e Sistemas de Informação (DIRCSI);

- Marinha: Superintendência das Tecnologias de Informação, que engloba o Centro de Documentação de Informação e Arquivo Central da Marinha, a Direção de Tecnologias de Informação e Comunicações (DITIC) e a Direção de Análise e Gestão da Informação (DAGI);

- Exército: Direção de Comunicações e Sistemas de Informação (DCSI) e administradores de redes locais nas Unidades;

- Força Aérea (FA): DCSI.

A importância desta capacidade é reconhecida pelas chefias.

Material. O *hardware* e *software* afetos ao armazenamento e processamento de dados são adquiridos e geridos de forma autónoma por cada uma das entidades, com financiamento proveniente do Orçamento do Estado e da Lei de Programação Militar (LPM) e, no caso da SGMDN, de fundos provenientes do Sistema de Apoio à Modernização Administrativa (SAMA). Foram identificadas limitações no financiamento desta capacidade face ao necessário para garantir a sua atualização.

As entidades encontram-se em estádios de maturidade distintos quanto à aplicação de ferramentas e metodologias para exploração e tratamento de dados, e à adequação das infraestruturas TIC de suporte.

No caso da SGMDN, o desenvolvimento de *dashboards* para apoio à decisão utilizando ferramentas de BI acompanhou a evolução dos módulos do Sistema Integrado de Gestão da Defesa Nacional (SIGDN), tendo, mais recentemente, um projeto de disponibilização de dados de RH, permitido avançar para um novo modelo tecnológico de

extração e preparação de dados (C.M. Passos, entrevista por videoconferência, 9 de novembro de 2020). A capacidade de armazenamento existente é adequada às necessidades atuais e contempla crescimento, na ordem das dezenas de TB, nomeadamente para adequação aos projetos de BI que serão desenvolvidos, e a de processamento irá sofrer um processo de renovação (R.M. Francisco, *op. cit.*).

A capacidade existente no EMGFA apresenta "limitações na escalabilidade e flexibilidade", estando desadequada para requisitos *Big Data* que venham a surgir (J.A. Rocha, *op. cit.*). Atualmente é disponibilizado um *dashboard* de Gestão Estratégica com recurso a ferramentas de BI (H.J. Guerreiro, entrevista presencial, 3 de dezembro de 2020).

Na Marinha, a DAGI implementa *dashboards* com recurso a ferramentas de BI para apoio a todas as áreas funcionais, sendo reconhecidamente "já problemática a escalabilidade quando é necessário aceder a novas fontes […] necessárias ao conhecimento situacional marítimo" (J.P. Roque, *op. cit.*). Está previsto o desenvolvimento, a partir do corrente ano, do projeto do Sistema de Apoio ao Planeamento, Execução e Controlo da Atividade de Fiscalização Marítima no âmbito do Sistema de Fiscalização e Controlo das Atividades de Pesca (APEC-SIFICAP), que incluirá uma componente de processamento e armazenamento *Big Data*, destinada ao tratamento de diversas fontes e formatos de informação (J.P. Roque, *op. cit.*).

O Exército detém capacidade própria de desenvolvimento de *dashboards* para apoio à decisão com ferramentas de BI (F.J. Soares, entrevista presencial, 16 de novembro de 2020), sendo que a expansão da capacidade de armazenamento e processamento, em curso, contempla futuros requisitos para o tratamento de *Big Data* (L.F. Camelo, *op. cit.*).

A FA não utiliza ainda ferramentas/metodologias dedicadas à análise e à exploração de dados (J.M. Mendes, entrevista presencial, 3 de dezembro de 2020). Pese embora o *hardware* e *software* afetos a esta capacidade serem atuais e garantidos por contrato de manutenção robusto, o "conjunto de fontes de dados […] ainda não é explorado de forma conjunta, na medida em que não existem ferramentas que consigam lidar com grandes volumes de dados, pelo que o modelo atual não está adaptado" a requisitos *Big Data* (T.D. Lopes, entrevista por *email*, 5 de abril de 2021). A plataforma de Comando e Controlo (C2) *Portuguese Sky Sentinel System* (PS3), desenvolvida no âmbito do Dispositivo Especial de Combate a Incêndios Rurais previu, na sua evolução, a inclusão de fontes externas, bem como "capacidade de análise de dados, baseados em algoritmos de análise em tempo real, apoiando assim efetivamente as operações militares" (T.D. Lopes, *op. cit.*).

Infraestruturas. Todas as entidades dispõem de CD próprios, implementados em infraestruturas proprietárias, *on-premises*. A constituição de capacidade alternativa, destinada a *backup* e *disaster recovery*, também em instalações próprias, encontra-se em diferentes estágios de implementação.

Pessoal e treino. A gestão do ciclo de vida da infraestrutura de armazenamento e processamento de dados é efetuada por elementos internos das entidades, por vezes em acumulação com outras funções da área TIC. No caso da SGMDN, os RH englobam militares colocados pelos Ramos, bem como funcionários civis da AP. Existe recurso a elementos de entidades externas, em reforço da capacidade interna ou para prover serviços especializados.

As limitações de RH, em quantidade e qualificados na área TIC, são generalizadas. J.P. Roque (*op. cit.*) estima que a DITIC tenha atualmente 66% da sua lotação preenchida, sendo problemática a sustentação das capacidades atuais. Na SGMDN, esta escassez "[…] entre outros fatores, […], poderá obrigar à externalização de alguns serviços, a fim de garantir a qualidade de serviço necessária" (R.M. Francisco, *op. cit.*).

Verificam-se "períodos de retenção em funções incompatíveis com os ciclos de formação e treino" (J.A. Rocha, *op. cit.*), bem como algum desajuste entre as necessidades existentes e a regulamentação associada às nomeações e colocação de pessoal, e à progressão na carreira militar, tornando necessária "uma política de retenção que garanta a permanência dos militares nesta área [eminentemente técnica] por elevados períodos" (L.F. Camelo, *op. cit.*). A atratividade por parte do mercado de trabalho civil, na área das TIC, é atualmente também fator de preocupação (J.P. Roque, *op. cit.*).

A formação e qualificação do pessoal são percecionadas de formas distintas: na SGMDN é efetuada quando necessário, sendo inclusivamente disponibilizada formação a elementos de outras entidades da DN em circunstâncias específicas (R.M. Francisco, *op. cit.*); em algumas entidades, a formação existente é ministrada em contexto de trabalho, frequentemente pelo fabricante (T.D. Lopes, L.F. Camelo, *op. cit.*). T.D. Lopes e J.P. Roque (*op. cit.*) referiram, ainda, a realização de treino com regularidade, nomeadamente de forma conjunta e sob coordenação do EMGFA, sobretudo na área de ciberdefesa.

Interoperabilidade. As entidades encontram-se ligadas através das diferentes redes de comunicações, sendo estabelecidas relações de confiança entre domínios, com partilha de informação limitada (J.P. Roque, *op. cit.*). O SIGDN é explorado transversalmente, introduzindo interoperabilidade ao nível dos Sistemas de Informação (SI) de gestão,

prevendo-se que "para além do BI, talvez a maior aposta estratégica TIC dos próximos anos da DN seja precisamente na área da interoperabilidade dos Dados e Serviços" (R.M. Francisco, *op. cit.*).

4.3 Adequabilidade de modelos *cloud computing* às Forças Armadas

A adoção de serviços em *clouds* públicas afigura-se, de forma geral, vantajosa em termos de *custos*, na medida em que dispensa o investimento na aquisição, sustentação e modernização da infraestrutura TIC de suporte e das respetivas capacidades de *backup e disaster recovery*. Contudo, T.D. Lopes (*op. cit.*) advertiu para o facto do "desinvestimento interno em capacidades próprias [colocar] o Ramo numa posição vulnerável, pois aquando de eventuais cortes orçamentais […], o valor a investir visando a recuperação de capacidades será muito maior", acrescendo ainda que a necessidade de financiamento plurianual poderá ser um obstáculo, face ao modelo de disponibilização de verbas em vigor.

Respeitante ao *processo aquisitivo*, "a contratação pública não está ainda adequada para esta transição [provisionamento dinâmico da capacidade], na medida em que investimentos tipicamente em ativo imobilizado transitariam para investimentos em serviços de consumo, que não geram imobilizado" (J.A. Rocha, *op. cit.*).

Os desafios associados ao processo de contratação de serviços *cloud*, seja pela duração máxima permitida para os contratos (por norma, 3 anos), que condiciona os decisores pelo risco de terem que mudar de prestador de serviço ao fim daquele período, seja pela transição de investimento em equipamento para aquisição de serviços, encontram-se identificados na Estratégia para a AP, e serão alvo de desenvolvimento de medidas específicas (AMA, 2020).

São consensuais as potenciais vantagens em termos de *escalabilidade* e *flexibilidade de recursos*, providos mediante necessidade, e tendencialmente consensuais (80%; n=4) as de *disponibilidade*, face às taxas elevadas apresentadas pelos CSP. De acordo com J.P. Roque (*op. cit.*), a disponibilidade tem a ver com "a confiança no *Service Provider*", sendo que, no caso da Marinha, o contrato de prestação de serviços estabelecido com a Microsoft contempla um *Service-Level Agreement* (SLA) H24. Contudo, 60% (n=3) das entidades da DN manifestaram reservas quanto à dependência de um CSP civil, pelo facto de não conseguirem ter controlo da estrutura, do seu estado, das avarias e das prioridades a atribuir em caso de indisponibilidade, ou porque "em situações de crise, são as

organizações militares que se encontram preparadas para garantir a disponibilidade, [não tendo] os CSP […] forma de [tal] garantir" (R.M. Francisco, *op. cit.*).

Neste âmbito, J.M. Tribolet (entrevista por *email*, 6 de fevereiro de 2021) realçou a necessidade de se implementarem, de forma sistémica, "mecanismos de testes da integridade quer da funcionalidade aplicacional instalada nas *clouds*, quer dos dados aí residentes", efetuados num registo contínuo e "[…] independente do fornecedor de serviços". Referiu ainda, no caso específico de *Big Data*, a necessidade de garantias de redundância, assegurando a "capacidade de acesso e reposição dos recursos *Big Data* existentes na *Cloud*, em cenários de disrupção extrema que ponham em causa o acesso em tempo útil a esses recursos" (J.M. Tribolet, *op. cit.*).

Do ponto de vista dos *RH* das organizações, foi reconhecido, consensualmente, que a adoção de serviços em *clouds* públicas, nomeadamente serviços relacionados com SI de gestão, acarreta vantagens, como sejam a diminuição da necessidade de formação e qualificação em determinadas áreas, e a libertação de indivíduos de tarefas de gestão da infraestrutura TIC, para outras tarefas associadas a sistemas operacionais. Realocação que poderá ser vantajosa, considerando as dificuldades atuais referentes a RH e às previsões anteriormente referidas relativas à disponibilidade futura de profissionais na área TIC. A inexistência de conhecimento interno para sustentar a capacidade em situação de crise pode, contudo, constituir uma vulnerabilidade (L.F. Camelo, *op. cit.*).

Respeitante à *segurança* de *clouds* públicas, a perceção das entidades da DN entrevistadas divergiu. Apesar de 60% (n=3) ter reconhecido que os CSP implementam mecanismos conducentes à segurança dos dados, tais como a disponibilização contínua de atualizações de segurança de *software* e o duplo fator de autenticação de utilizadores, os seus posicionamentos relativos à adoção do modelo foram diversos.

A.G. Marques (entrevista por videoconferência, 10 de fevereiro de 2021) referiu como exemplo de informação que não deve ser transposta para a *cloud* do Estado, caso não existam áreas específicas compatíveis com a sua criticidade,

> […] dados cujo eventual comprometimento permita inferir as capacidades das FFAA em todas as suas componentes [e que,] se exfiltrados, poderiam permitir conhecer, de forma vertical e transversal […] as competências, prontidão e estado sanitário do pessoal das FFAA, bem como dados dos seus sistemas de armas.

Considerou, contudo, existir um conjunto de serviços e dados que poderiam ser geridos e disponibilizados em modelos IaaS e PaaS na *cloud* do Estado (A.G. Marques, *op. cit.*). O GNS já certificou alguns serviços da plataforma *Microsoft Azure* na marca NACIONAL RESERVADO, tendo já outros CSP abordado aquele Gabinete no sentido de proceder à certificação dos seus serviços e plataformas (A.G. Marques, *op. cit.*). J.P. Roque (*op. cit.*) realçou, a este propósito, que os postos de trabalho e os canais de comunicação não se encontram ainda devidamente credenciados para processar aquela marca.

Também não reuniu consenso o grau de classificação de segurança da informação a processar em *cloud* pública.

Ainda concernente à segurança, C.J. Páscoa (entrevista por *email*, 12 de fevereiro de 2021) estabeleceu como objetivos, para utilização da *cloud* e, especificamente para *Big Data*, o cumprimento dos requisitos de confidencialidade, integridade e disponibilidade.

Como vantagens adicionais à adoção deste modelo, foram ainda elencadas "a maior interoperabilidade, por normalização de sistemas, menor consumo de energia, diminuição da pegada ecológica" (A.G. Marques, *op. cit.*), e "a partilha de informação e o contributo para a desmaterialização e a associação ao programa Simplex e aos planos nacionais para a simplificação, descarbonização e digitalização" (C.J. Páscoa, *op. cit.*).

Na perspetiva da implementação de uma cloud privada da DN, e apesar dos *custos* mais elevados relativamente à utilização de um modelo público (porque obriga à implementação de uma infraestrutura própria para garantia de *backups*, bem como à disponibilidade de verbas para a atualização de *hardware* e *software*), T.D. Lopes (*op. cit.*) enfatizou a obtenção de economias de escala e rentabilização de recursos, dispensando cada entidade de investimentos próprios na capacidade. Contudo, enquanto infraestrutura partilhada no seio da DN, L.F. Camelo (*op. cit.*) manifestou preocupação relativa às necessidades específicas de cada entidade, porque "agrupar estruturas com culturas organizacionais diversas e com modos próprios de trabalhar, poderia dificultar o entendimento entre as diversas entidades e o investimento a realizar".

Neste modelo, a *escalabilidade* seria "proporcional ao planeamento e à precisão dos dados fornecidos pelas entidades participantes em relação à necessidade dos seus utilizadores "[implicando] a concordância de todas as entidades para alterações na estrutura e capacidade da *cloud*" (L.F. Camelo, *op. cit.*).

A *disponibilidade* neste modelo seria semelhante à de uma *cloud* pública, em situações normais, desde que existam os recursos financeiros para materializar a

capacidade, e os RH, devidamente formados e qualificados para a explorar, uma vez que o controlo da infraestrutura TIC é de responsabilidade interna (L.F. Camelo, *op. cit.*). Em situações de exceção, "as FFAA, como último baluarte e garante da Nação, [deverão] ter capacidade própria para operar quando tudo o resto estiver inoperacional ou fortemente degradado, tendo essa capacidade de ser criada e treinada em tempo de paz" (L.F. Camelo, *op. cit.*), porque numa "situação de crise ou guerra, estados de intervenção naturais das FFAA e para os quais se preparam, o modelo privado, *a priori*, dá mais garantias de segurança e disponibilidade do que o modelo público" (R.M. Francisco, *op. cit.*).

Neste modelo, apesar da perspetiva de centralização de *RH* afetos à capacidade, racionalizando recursos, seriam expectáveis algumas limitações já verificadas nesta área em termos de número e qualificações de indivíduos (R.M. Francisco, *op. cit.*).

Em termos de *segurança* é um modelo percebido como vantajoso pela maioria dos entrevistados da DN (80%; n=4), que relevam a segurança física das instalações, o controlo das plataformas exploradas (fatores que ganham maior realce em situações de crise ou de guerra), e a maior adequabilidade para armazenamento e processamento de informação classificada.

A adoção de *cloud computing* na DN, independentemente do modelo, constitui um desafio cultural, sendo necessária uma liderança efetiva no processo, através da identificação de "um líder na DN, ao mais alto nível, que promova a confiança nesta solução, e que lidere o processo de identificação de serviços e de prioridades [de implementação]" (A.G. Marques, *op. cit.*), ou, por outras palavras, uma mudança na "[…] cultura das organizações que compõem a DN, para poderem aceitar o desafio de ter dados na *cloud* e poderem confiar no sistema"(C.J. Páscoa, *op. cit.*), sendo necessária uma governação sistémica da utilização da *cloud*, ao nível da DN, abrangendo "todas as dimensões relevantes da atuação" e não limitada aos aspetos tecnológicos (J.M. Tribolet, *op. cit.*).

Neste âmbito,

> […] o principal e mais difícil desafio reside na capacitação das entidades e do sistema de DN para conceptualizar as arquiteturas aplicacional, de informação, de processos, de controlo e de auditoria a serem implementadas nas *clouds* que pretender vir a usar, sejam elas públicas ou privadas. (J.M. Tribolet, *op. cit.*)

Refere ainda J.M. Tribolet (*op. cit.*) que "a prestação de serviços de *clouds* públicas deve ser acompanhada permanentemente por equipas especializadas ao mais alto nível sistémico da DN".

A adoção de serviços *cloud* pela DN, independentemente do modelo adotado, pode ser potenciada pela criação de sinergias e de relações de cooperação com entidades académicas, de investigação e da indústria TIC, seja no desenvolvimento de capacidades (exemplo do projeto de desenvolvimento de máquinas de cifra, em curso – A.G. Marques [*op. cit.*]), seja "no estudo e definição dos modelos a adotar, […] das capacidades de testes […], na capacitação dos meios humanos da DN […], nomeadamente desenhando e executando programas de formação à medida, adequados às necessidades e objetivos da DN" (J.M. Tribolet, *op. cit.*), seja ainda como "parceiras essenciais e catalisadores para o processo de criação de valor e de transformação das organizações, até no domínio da investigação e desenvolvimento e das candidaturas a programas de financiamento" (C.J. Páscoa, *op. cit.*).

Com a adoção de modelos *cloud* pela DN, consideram-se reunidas as condições para a adoção de

> […] práticas de sensorização e recolha de dados generalizadas [tornando necessárias] políticas relativas a todo o ciclo de vida dos dados, nomeadamente quanto à recolha, validação, limpeza, acesso, segurança e processamento desses dados […]. A governação dos dados / informação deve ser assumida ao mais alto nível organizacional e numa perspetiva multidimensional […] fundada nas necessidades reais das operações […]". (J.M. Tribolet, *op. cit.*)

4.4 Síntese conclusiva e resposta à Questão Derivada 1

Da análise efetuada, conjugada com os quadros comparativos apresentados nos Apêndices G e H, e em resposta à QD1, *Qual é o modelo de armazenamento e processamento de dados nas FFAA na era do Big Data?*, conclui-se não existir um modelo único em vigor, mas sim diferentes modelos independentes, repercutidos em reduzidas sinergias.

À luz de uma análise conforme com os vetores de edificação de capacidades militares DOTMLPII, infere-se que a atual capacidade de armazenamento e processamento de dados, efetuada, na sua quase totalidade, de acordo com o modelo tradicional, traduz-se na(o): ausência de *doutrina* formal; existência de áreas organizacionais com funções específicas para assegurar a capacidade, suportadas por uma liderança que reconhece a sua

importância (*organização* e *liderança*); utilização de *hardware* e *software* adquiridos, desenvolvidos e geridos de forma autónoma, apresentando ferramentas e metodologias de exploração de dados em diferentes estádios de maturidade, e inadequadas para o tratamento de *Big Data* (*material*); uso de *infraestruturas* próprias; emprego de RH maioritariamente internos e insuficientes em quantidade e em qualificações para as tarefas, cuja formação é efetuada, em alguns casos, em contexto de trabalho, pelo fabricante (*pessoal e treino*); SI de gestão, nomeadamente o SIGDN, e ligações entre as respetivas redes de comunicações, como mecanismos de troca de dados entre as entidades (*interoperabilidade*).

Ademais, conclui-se a inexistência de uma exploração de sinergias ao nível dos processos aquisitivos, existindo restrições de financiamento para manutenção da capacidade permanentemente atualizada, e a transversalidade das dificuldades em deter e em reter os RH internos necessários, por períodos de tempo compatíveis com a aquisição e o exercício de *expertise* na matéria.

A adoção de serviços *cloud*, independentemente do modelo, é composta por iniciativas reduzidas e isoladas, não existindo uma abordagem estruturada na DN sobre a matéria, o que, em certa medida, associa-se ao facto da estratégia do Estado Português para a *cloud*, aplicável a toda a AP e assente numa lógica *cloud first*, ser ainda recente e, consequentemente, com diversos normativos e mecanismos ainda por estabelecer.

Por último, constatou-se que o posicionamento relativo à adoção destes modelos, públicos e privados, é divergente, evidenciando-se preocupações ao nível da disponibilidade e da segurança de dados e serviços, condições fulcrais para as FFAA, mas reconhecendo, de forma geral, as mais-valias em termos de economias de escala, racionalização de recursos, nomeadamente RH, e interoperabilidade.

5. Estratégia em matéria de armazenamento e processamento de dados em entidades congéneres na era do *Big Data*

Neste capítulo analisam-se – tal como no capítulo anterior, à luz de vetores de edificação de capacidades militares DOTMLPII – as estratégias adotadas pela NATO, e pelas áreas da Defesa de França e dos Estados Unidos da América (EUA) em matéria de armazenamento e processamento de dados com recurso a modelos *cloud*, e responde-se à QD2.

5.1 *North Atlantic Treaty Organization*

Doutrina. Enquadrada na sua estratégia de disponibilização de serviços TIC, a NATO estabeleceu uma política para a implementação de serviços na *cloud*, a *NATO Cloud Computing Policy* (NATO, 2016), onde todas as soluções TIC a implementar por entidades NATO devem considerar prioritariamente o modelo *cloud* (*cloud first*), em detrimento de infraestruturas específicas/isoladas/desagregadas, e considerou a infraestrutura como uma "shared commodity that is accessed as a service" (p. 1).

Pese embora o objetivo seja a obtenção de uma infraestrutura TIC única, destinada a processar todos os tipos de informação (até à classificação NATO SECRET, inclusive), até que seja tecnicamente viável garantir todos os princípios da segurança da informação, serão implementadas duas arquiteturas, lógica e fisicamente distintas (NATO, 2016), destinadas, designadamente, ao processamento de informação classificada com o grau:

- NATO CONFIDENTIAL ou superior, implementada numa *cloud* privada propriedade da Aliança ou de uma nação aliada;

- NATO RESTRICTED ou inferior, que poderá ser disponibilizada de acordo com o modelo comunitário, híbrido ou público, desde que garantidos todos os princípios da segurança da informação.

Apesar da supradita premissa *cloud first*, a opção entre o modelo *cloud* e as arquiteturas tradicionais para a implementação de um novo serviço, ou para a transição de um já existente, deverá ser efetuada com base em critérios, como sejam a sensibilidade dos dados (associada à segurança da informação ou soberania dos dados), os tempos de resposta (fatores como a latência da rede, aquando do acesso a serviços remotos na *cloud*, podem tornar a opção desadequada em aplicações *near real-time* ou *real-time*), a garantia de continuidade de negócio durante o processo de migração, a integração e dependência com outras aplicações que não serão migradas, e/ou a análise custo-benefício entretanto efetuada (NATO, 2020).

Organização e Liderança. A doutrina NATO referente à adoção de um modelo *cloud computing* aplica-se à *NATO Enterprise*[5], implementado sob a supervisão do *Consultation, Command and Control Board* (C3B), sendo que a Aliança encoraja as Nações a seguirem, nos seus ecossistemas TIC, o modelo que norteia a transição de uma arquitetura tradicional para uma arquitetura *cloud*, plasmado na *NATO Cloud Computing Directive* (NATO, 2020).

Para permitir uma governação dos serviços *cloud* ao longo do seu ciclo de vida, foi implementada uma estrutura de governação, que contempla diferentes perfis (Figura 2), segundo um modelo de responsabilidades partilhadas entre o CSP e o cliente (Figura 3) (NATO, 2020).

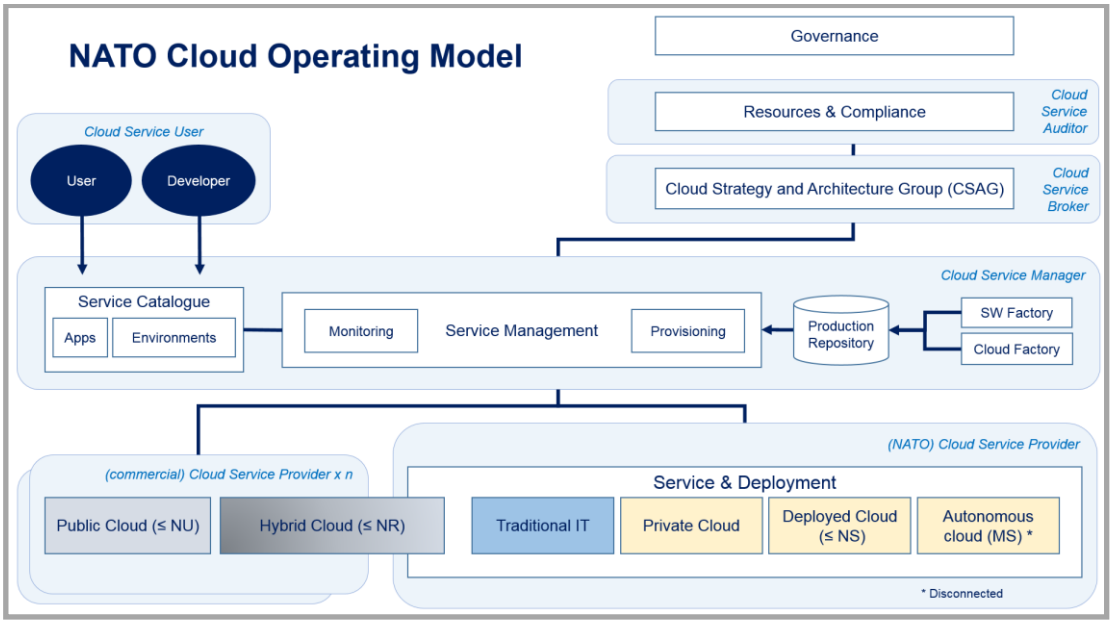


Figura 2 – Modelo operacional da nuvem NATO
Fonte: NATO (2020).

[5] A *NATO Enterprise* compreende os *NATO Headquarters* (HQ) (*International Staff*, *International Military Staff* e pontos de presença nas missões e delegações nacionais nos HQ), a *NATO Command Structure* (NCS) e pontos de presença nas representações nacionais naquela estrutura de comando, os elementos específicos da *NATO Force Structure* (NFS), os elementos da NCS e da NFS destacados e embarcados em apoio direto a operações e missões da Aliança, agências NATO, instalações de formação e treino NATO e os pontos de presença nas nações para ligação a sistemas de informação e comunicações nacionais (NATO, 2015).

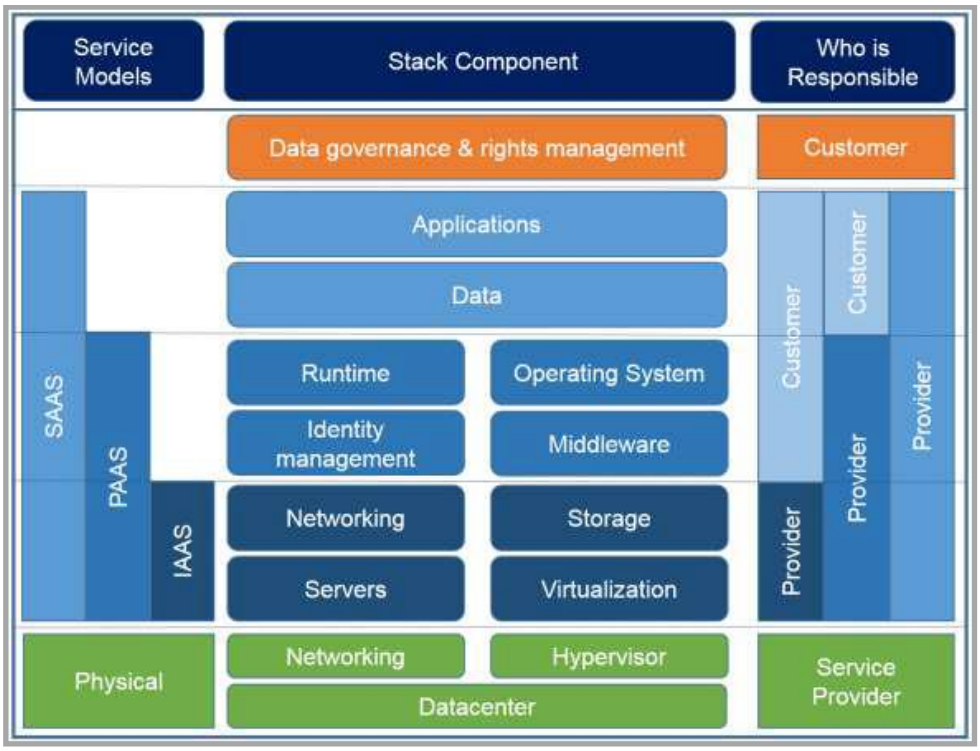


Figura 3 – Modelo de responsabilidades partilhadas
Fonte: NATO (2019a).

Material. A NATO reconhece as vantagens da utilização de *clouds* nacionais e públicas, que, concorrendo para economias de escala e minimizando custos de investimento e sustentação de infraestruturas, permitem direcionar o investimento para sistemas operacionais (NATO, 2020).

Infraestruturas. Respeitante à implementação de *clouds* privadas, a Aliança desenvolveu na última década um programa de modernização da sua infraestrutura tecnológica, cuja primeira fase, formalmente iniciada em 2017, foi dedicada à renovação das infraestruturas *core* de processamento e armazenamento, e contemplou a instalação de dois CD com soluções tecnológicas baseadas em *cloud computing*, em localizações geográficas distintas (Bélgica e Itália) (*NATO Communications and Information Agency* [NCIA], 2017). Adicionalmente, o programa inclui nós geograficamente dispersos em Itália, Turquia, Inglaterra e EUA para o alojamento de sistemas que, pelas suas características, não poderão ser centralizados, preconizando-se a expansão da arquitetura através de um terceiro nó central, localizado no NATO HQ, bem como de novos nós deslocalizados (NCIA, 2017).

Para os serviços a implementar em *clouds* públicas, a NATO (2020) estabeleceu que os dados deverão ser alojados em CD localizados em nações NATO, selecionadas pela Aliança, só sendo sujeitos a alteração com consentimento prévio. Para o desenho e a

acreditação da arquitetura de segurança de serviços a implementar neste modelo, a Aliança definiu um conjunto de recomendações de alto nível, que orientam os mecanismos de controlo a integrar no SLA a estabelecer com o CSP, para além das já mencionadas restrições respeitantes à localização dos CD (NATO, 2019a).

São inequívocos, na política *cloud* da NATO, a necessidade de cumprir com as políticas e diretivas próprias já estabelecidas respeitantes à segurança da informação, o respeito pela privacidade dos dados, tomando em consideração a legislação e regulamentação específicas de cada nação, bem como o requisito de total controlo, por parte da Aliança, do acesso, alteração, arquivo e eliminação de dados (NATO, 2016).

No caso específico de informação NATO RESTRICTED, não é possível ainda implementar soluções destinadas ao seu processamento em *clouds* públicas, até que sejam desenvolvidos normativos de segurança compatíveis com este requisito, tarefa que se encontra em curso (NATO, 2019a, 2019c). Os normativos em vigor assentavam no pressuposto de que tal informação seria tratada em infraestruturas propriedade exclusiva da NATO (NATO, 2019a).

Os diversos modelos *cloud computing* são considerados soluções adequadas e comuns para sistemas baseados em tecnologias como Inteligência Artificial (IA) e *machine learning* destinados ao tratamento de *Big Data* (NATO, 2021).

Pessoal e Treino. Quanto aos RH envolvidos, não sendo necessários indivíduos para efetuar a gestão do ciclo de vida de *hardware*, nas situações em que os serviços migrem para *clouds* públicas, serão, contudo, fundamentais, elementos para a gestão daqueles serviços, tendo a NCIA criado novas posições organizacionais para o efeito, nomeadamente para monitorizar e estimar custos de consumo (NCIA, 2019). O treino em tecnologias e ferramentas de administração *cloud* encontra-se previsto (NATO, 2020).

Interoperabilidade. A interoperabilidade de serviços *cloud* será garantida através da utilização de *standards* NATO e *standards* abertos no seu desenvolvimento (NATO, 2016), sendo potenciada pela abrangência de implementação da respetiva política (*NATO Enterprise*).

5.2 França

Doutrina. Enquadrado no processo de transformação digital do Estado, o Ministério das Forças Armadas francês (Minarm [*Ministère des Armées*]) apresentou em 2017 a sua estratégia setorial, *Ambition Numérique du Ministère des Armées*, e em 2018, o plano para a sua operacionalização (Minarm, 2017b, 2018), criando a marca *Défense Connect* para

alcançar visibilidade para o processo de transformação digital junto de entidades governamentais e civis (nomeadamente escolas e empresas) (Minarm, 2020).

O *Big Data* e a IA surgem como novas tecnologias de tratamento de dados, potenciadoras de melhoria nos sistemas militares, mas também noutras áreas como a gestão de RH, a consolidação financeira e gestão administrativa e a manutenção, considerando o modelo *cloud* como a solução tecnológica adequada (Minarm, 2017b, p. 21, 2018, p. 7).

Neste enquadramento, o governo francês publicou em 2018 uma estratégia para a utilização da *cloud* (*Direction interministérielle du numérique et du système d'information et de communication de l'Etat* [DINSIC], 2018), assente no desenvolvimento e utilização de uma *cloud* híbrida, com uma estrutura pautada por três níveis concêntricos e distintos, de acordo com a sensibilidade dos dados, refletida na orientação do Minarm para a *cloud* da Defesa, que será composta pelas componentes (Minarm, 2020):

- Interna, exclusiva das FFAA, dedicada às operações e situada *on-premises*;

- Dedicada, alojada em instalações de parceiros de confiança, garantindo os requisitos de autonomia e soberania, e hospedando a maioria dos sistemas do Ministério, cuja segurança será da responsabilidade da respetiva área de cibersegurança, em conformidade com a Agência Nacional de Cibersegurança Francesa;

- Externa, que prevê, para dados não-sensíveis, serviços publicados em catálogo acessível na *Internet*, alojados em prestadores de serviços públicos (DINSIC, 2018).

Organização e Liderança. O Minarm integra uma entidade responsável pela condução e coordenação do processo de transformação digital dentro das FFAA, reforçando a governação da área de Comunicações e Sistemas de Informação (CSI), a *Direction générale du numérique et des systèmes d'information et de communication* (DGNUM), criada em 2018, diretamente dependente do ministro e em coordenação estreita com outras entidades, nomeadamente o Chefe do Estado-Maior-General das FFAA e a Agência para a Inovação do Estado (Minarm, 2020). A implementação tecnológica dos projetos, bem como a gestão dos dados e aplicações do ministério, encontram-se a cargo da *Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information de la Défense* (DIRISI) (Minarm, 2017a).

Material. Assente no modelo *cloud* para o desenho da respetiva arquitetura, foi implementada a *Plateforme d'Ouverture, de Centralisation, d'Exposition et d'Analyse des Données* (POCEAD), tendo em vista o armazenamento de dados de acordo com modelos

consonantes com *Big Data* e a exposição e partilha de dados na *Intranet* da Defesa (Minarm, 2020). Este projeto é o precursor da *Architecture de Traitement et d'Exploitation Massive de l'Information multi-Sources* (ARTEMIS), atualmente em curso, que visa a criação de uma plataforma *Big Data*, destinada ao ministério das FFAA, que permitirá o armazenamento, processamento e exploração massiva de dados, com recurso a técnicas de IA e *machine learning* (Global Newswire, 2019). O projeto é desenvolvido por um consórcio de empresas com sede na Europa (Atos, *Cap Gemini* e *Commissariat à l'énergie atomique et aux énergies alternatives*) e integra outros parceiros franceses, nomeadamente académicos, médias empresas e *startups* (Global Newswire, 2019).

O *Chief Information Officer* (CIO) da Defesa, diretor da DGNUM, considera viável a migração de aplicações de suporte logístico e recrutamento, entre outras, para a *cloud* privada do Estado, no modelo SaaS, reconhecendo a vantagem de suprimir o suporte dedicado àqueles sistemas (CIO, 2020).

Infraestruturas. Conforme com a estratégia apresentada para o Estado, a utilização da *cloud*, considerada prioritária no processo de transformação digital do Estado, poderá contemplar o alojamento de dados fora do território nacional (DINSIC, 2018).

Contudo, a implementação de serviços e disponibilização de dados em nuvem, imprescindível para o tratamento massivo de dados associados a novas tecnologias como IA e *Big Data*, é considerada uma questão de soberania pelas FFAA francesas (Minarm, 2020). Assim, os dados do ministério devem ser alojados internamente ou num CSP exclusivamente ao abrigo da legislação nacional, em conformidade com diretivas internas, uma vez que a sua segurança não se prende apenas com questões tecnológicas e organizacionais, mas também com legislação extraterritorial, de que é exemplo o *Cloud Act* norte-americano (Minarm, 2020). O facto do mercado de prestadores de serviços na *cloud* ser dominado por firmas norte-americanas (*Google*, *Microsoft* e *Amazon*) constitui, assim, um fator de preocupação (Minarm, 2019).

De acordo com o CIO (2020), a Defesa não é um ministério como os outros, não tendo muita aplicabilidade a sua integração na *cloud* pública do Estado. Em alternativa, deve ser entendido como o mais resiliente e independente de serviços externos, sobretudo estrangeiros, pese embora poderem ser utilizadas tecnologias estrangeiras (CIO, 2020).

Pelo referido, e a fim de disponibilizar capacidade *on-premises*, foi efetuada na última década uma racionalização de serviços TIC na Defesa francesa, tendo-se centralizado a capacidade própria de alojamento de dados e serviços em quatro CD

localizados na área metropolitana, que constituem o núcleo da denominada *Cloud Défense* (Minarm, 2017a).

Pessoal e Treino. Para acompanhar o processo de transformação digital, o *Ministère des Armées* deveria disponibilizar condições para recrutar RH com competências em áreas de especialização específicas (já existentes ou novas), a fim de garantir a sua sustentabilidade nesta área, antecipando-se, assim, um aumento da necessidade deste tipo de recursos (civis e militares) até 2025 (Minarm, 2020). Refira-se que os objetivos de recrutamento de civis foram cumpridos, com abertura de novos concursos e alterações salariais, estando em curso a elaboração de um plano de ação para os militares (Minarm, 2020). Esta necessidade tem-se refletido, por outro lado, no imperativo de equacionar uma reforma das carreiras militares e civis nas TIC, nomeadamente no que respeita a recrutamento e retenção, aculturação, formação CSI e treino totalmente digital para todos os indivíduos (Minarm, 2020).

No âmbito do treino, o ministério lançou em 2019 o projeto Academia Digital (*Académie du Numérique*), que abrange áreas de formação diversas como o desenvolvimento de sistemas, IA, cibersegurança, redes e sistemas de comunicações (Minarm, 2020).

Interoperabilidade. De acordo com a estratégia enunciada, as diferentes componentes que integram a *cloud* híbrida formam "círculos concêntricos", promovendo sinergias e articulação de código entre eles (Minarm, 2019, p. 14). Ao nível dos dados armazenados pelo Minarm, a interoperabilidade encontra-se subjacente aos projetos de desenvolvimento das plataformas POCEAD e ARTEMIS, já referidas (Global Newswire, 2019; Minarm, 2020).

5.3 Estados Unidos da América

Doutrina. A estratégia do Departamento de Defesa dos Estados Unidos (*United States Department of Defense* – USDoD) para a *cloud* (*DoD Cloud Strategy*) resultou da necessidade de abranger e normalizar um conjunto de implementações anteriores de modelos *cloud*, desconexas e isoladas, de entidades integrantes da Defesa (USDoD, 2018). Esta estratégia, publicada em 2018, apresentou o conceito *Enterprise DoD Cloud*, que abrange todos os níveis de decisão (tático, operacional e estratégico) e todos os graus de classificação de segurança, e a ser implementado de forma privilegiada (*cloud first*), em detrimento do modelo tradicional, com recurso a diversas arquiteturas *cloud* (*multi-cloud*), providenciadas por diferentes prestadores de serviços (*multi-vendor*) (USDoD, 2018).

Adicionalmente, e em publicação de 2019, a estratégia para a modernização digital do DoD apresentou a *Enterprise cloud* como um objetivo estratégico, que permitirá a organização, tratamento e acesso a volumes massivos de dados, criando condições para o desenvolvimento de soluções baseadas em IA e *machine learning* para apoio à tomada de decisão (USDoD, 2019). Igual enfoque atribuído pela estratégia daquele departamento para os dados, de 2020, que refere que a arquitetura de dados deverá ser "potenciada pela *enterprise cloud*" (DoD, 2020, p. 4), possibilitando a sua utilização à escala e velocidade necessárias para garantir eficiência e superioridade operacional (DoD, 2020, p. 2).

O processo de implementação da *Enterprise cloud*, representado na Figura 4, preconiza (USDoD, 2018, 2021):

- Uma componente transversal e genérica (*General Purpose*), denominada *Joint Enterprise Defense Infrastructure* (JEDI), prevalente, que permita disponibilizar serviços IaaS e PaaS, por parte de um CSP, com ambientes distintos para todos os níveis de classificação, incluindo desde funcionalidades centralizadas a serviços ao nível tático, e potenciando tecnologias como a IA e *machine learning*;

- Componentes dedicadas (*Fit for Purpose*), para as situações em que os requisitos não sejam suportados pela componente *General Purpose;*

- Avaliação e migração das arquiteturas *cloud* preexistentes em organizações que integram o DoD para o ambiente JEDI ou, mediante a especificidade dos respetivos requisitos e após aprovação, transformação em arquiteturas *Fit for Purpose*.

Organização e Liderança. Ao CIO da Defesa incumbe a responsabilidade pela implementação do referido ecossistema *cloud*, e pela promoção da criação de uma estrutura organizacional, com liderança estabelecida e fóruns de governação, para garantir que os objetivos estabelecidos serão alcançados através da execução dos planos delineados (USDoD, 2018). A estratégia para a modernização digital aprovada em 2019 reforçou esta prioridade (USDoD, 2019, p. 15).

Material. Fazendo uso das vantagens intrínsecas ao ambiente *cloud*, é objetivo do DoD focar os recursos orgânicos nos sistemas operacionais, bem como manter uma arquitetura "*evergreen*"[6], quer em termos tecnológicos, quer em termos de segurança, com responsabilidades partilhadas, caso-a-caso, entre o CSP e o dono do sistema, mediante a arquitetura de cibersegurança determinada pelo CIO (USDoD, 2018).

[6] Refere-se à permanente atualização de serviços disponibilizados ao utilizador, bem como da infraestrutura tecnológica que os suporta (*Microsoft Corporation*, 2020).

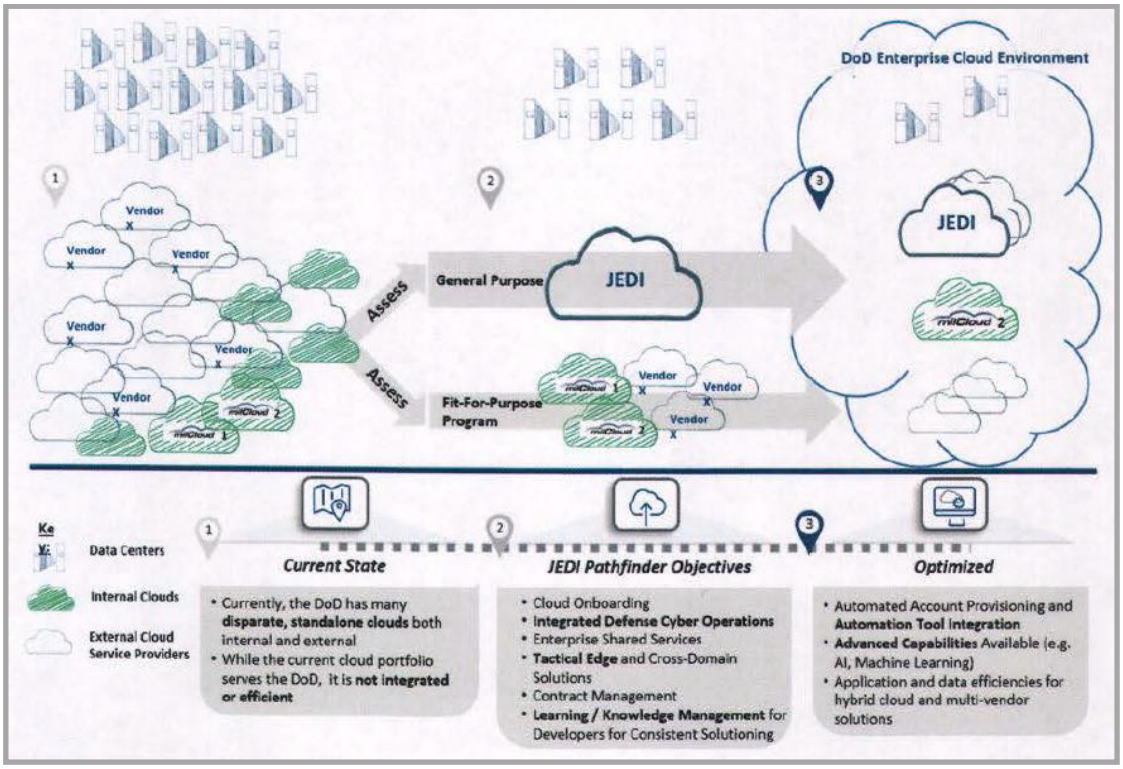


Figura 4 – Percurso do DoD para ambientes *cloud* híbridos e *multi-vendor*
Fonte: USDoD (2018).

Infraestruturas. A política suprarreferida reconhece as valências de utilizar serviços *cloud* públicos, através de infraestruturas disponibilizadas por CSP, nomeadamente das características *multi-region* e *multi-availability zone* que permitem incrementar resiliência, garantir a continuidade de serviço e a recuperação de falhas, por oposição à realização de investimento interno em recursos que periodicamente ficam desatualizados e que podem não suprir as necessidades (USDoD, 2018).

Ainda relativamente a prestadores de serviços, é clara na política enunciada a necessidade de potenciar a indústria nacional, maximizando a competição entre prestadores de serviços, e diversificando os contratos, evitando fenómenos de *vendor-lockin* (USDoD, 2018).

As aplicações e sistemas que não serão implementados numa arquitetura *cloud*, após respetiva análise de adequabilidade, ficarão residentes em CD *on-premises*, dedicados, que serão racionalizados e reduzidos em número (USDoD, 2018). Nas situações em que o ambiente *General Purpose* não providenciar as valências necessárias para os requisitos apresentados, serão criadas soluções *Fit for Purpose*, *on-premises* (caso do ambiente *milCloud* 2.0, orientado para a missão, implementado numa *cloud* privada em dois CD da

Defence Information Systems Agency), ou em ambiente comercial, caso do *Defense Enterprise Office Solution*, que visa proporcionar um conjunto de ferramentas de produtividade, de troca de mensagens, colaborativas e de gestão de conteúdos de forma transversal a todo o DoD, de acordo com o modelo SaaS (USDoD, 2018, 2021).

Pessoal e Treino. A este nível, foi enfatizada a aquisição de *know-how* interno – para avaliar a adequabilidade da transição de serviços e sistemas para o modelo *cloud*, e para desenvolver, manter e explorar os serviços, através da inclusão de cláusulas de assistência e treino especializado nos contratos a estabelecer com os prestadores de serviços (UsDoD, 2018).

Interoperabilidade. Ao nível da estratégia foi preconizada a interoperabilidade do ambiente *General Purpose* com as diferentes implementações *Fit for Purpose*, aplicando-se ao nível dos dados a utilização de *standards* para catalogação, processamento, acesso e armazenamento (UsDoD, 2018).

5.4 Síntese conclusiva e resposta à Questão Derivada 2

Decorrente da análise efetuada, e sintetizada no Quadro comparativo elencado no Apêndice I, em resposta à QD2, *Qual é a estratégia em matéria de armazenamento e processamento de dados de entidades congéneres na era do Big Data?*, conclui-se que as estratégias das três realidades estudadas comungam um encetar, na última década, por processos de modernização e transformação digital, preconizando para o armazenamento e processamento de dados, mediante uma avaliação prévia de viabilidade, a adoção de serviços *cloud*, em detrimento de arquiteturas tradicionais (*cloud first*). Uma realidade inclusivamente mandatória nos casos da NATO e dos EUA, e encorajada no francês.

Transversal também às três congéneres estudadas é o facto de estar prevista a utilização de modelos híbridos, em que a componente de dados mais sensíveis será alojada em *clouds* privadas, *on-premises*, enquanto a de dados menos sensíveis passará pela utilização (nunca esquecendo a soberania e segurança de dados) de *clouds* públicas. Uma *praxis* associada a uma racionalização e redução de CD das respetivas entidades.

Com estratégias claramente definidas para o seu país, em geral, e para a Defesa, em particular, todas as congéneres consideraram o modelo *cloud* como uma base de trabalho adequada para o desenvolvimento de projetos com recurso a novas tecnologias de tratamento de dados, como IA ou *machine learning*, permitindo o tratamento de *Big Data*.

Conclui-se, por último, que a estratégia de armazenamento e processamento de dados nas três entidades, estudada de acordo com os vetores de edificação de capacidades

militares DOTMLPII, traduz-se, em matéria de: *doutrina*, na existência de orientações de nível estratégico; *organização* e *liderança*, em modelos de governação delineados ou previstos, com estruturas lideradas por entidades com posicionamento na estrutura superior das organizações; *material*, na redução de investimento em capacidades internas, direcionando o foco dos recursos para serviços operacionais; *infraestruturas*, na adoção de modelos de implementação híbridos, com recurso a *clouds* públicas e implementando *clouds* privadas em CD proprietários; *pessoal* e *treino*, na identificação da necessidade de deter RH devidamente qualificados para o desenvolvimento e administração de serviços *cloud*; *interoperabilidade*, na adoção de *standards* e nas trocas de dados entre os diversos modelos *cloud*.

6. Proposta de otimização do modelo de armazenamento e processamento de dados nas Forças Armadas, e resposta à Questão Central

Pelo até aqui analisado, e em resposta à QC, *Como contribuir para otimizar o modelo de armazenamento e processamento de dados nas Forças Armadas na era do Big Data*?, apresenta-se, na Figura 5, a proposta para um modelo de gestão da capacidade de armazenamento e processamento de dados, organizada de acordo com os vetores DOTMLPII, refletindo a adoção de serviços *cloud*.

Doutrina

Implementar cloud first em modelo híbrido

- Estabelecer enquadramento doutrinário para a capacidade, ao nível da DN, em alinhamento com a Estratégia *cloud* para a AP;
- Estabelecer política de Gestão da Informação ao nível da DN;
- Verificar a adequabilidade do modelo *cloud* na implementação de novos sistemas ou serviços, bem como na migração ou evolução de existentes;
- Implementar o modelo híbrido:
  - *Cloud* pública. Tendencialmente ferramentas SaaS de produtividade, ferramentas colaborativas, SI de gestão, e outra informação não classificada;
  - *Cloud* privada da DN. Informação cujo armazenamento e processamento em infraestruturas civis não seja considerado adequado, e informação classificada, de forma segregada; pode abranger uma *cloud* comunitária e *clouds* privadas das entidades, destinadas a serviços orgânicos de teor operacional.
  - Modelo tradicional, centralizado, para serviços e sistemas centrais que não sejam considerados adequados para implementação em modelo *cloud*, ou nas entidades, para serviços e sistemas orgânicos de teor operacional.

Organização

Estabelecer CIO e estrutura de governação da DN

- Criar posição de CIO ao nível da DN;
- Criar estrutura de governação TIC da DN, liderada pelo CIO e composta por representantes do MDN, EMGFA e Ramos, com responsabilidades específicas na gestão da capacidade de armazenamento e processamento de dados, na gestão de dados e da Informação, e na segurança.

Treino

Capacitar pessoal de forma contínua

- Formar e qualificar RH afetos à capacidade de forma centralizada;
- Formar e qualificar RH de forma autónoma para sistemas e serviços específicos em exploração nas entidades;
- Estabelecer parcerias com entidades de ensino, visando a criação de módulos de formação adequados à exploração da capacidade;
- Criar módulos de formação em áreas emergentes (*data science*, IA, *cloud computing*, *machine learning*);
- Explorar modelos de formação e de partilha de recursos e de conhecimento, em matéria de serviços *cloud*, a desenvolver pela AP.

[Cont.]

Material

Centralizar recursos e normalizar processos

- Centralizar processos aquisitivos de *hardware* e de licenciamento de *software*;
- Centralizar processos de contratação de serviços *cloud*, alinhados com os mecanismos em desenvolvimento no âmbito da AP;
- Centralizar verbas, atualmente atribuídas às entidades, para a gestão do ciclo de vida dos serviços que passarem a ser geridos conjuntamente;
- Definir *framework* para o processo de atualização de *hardware* e *software*, visando um ambiente tendencialmente "*evergreen*";
- Definir uma matriz de adequabilidade para adoção de serviços *cloud*, alinhada com a *framework* da AP, mais restritiva e conforme com requisitos especificamente militares;
- Definir requisitos técnicos a incorporar nos SLA associados aos contratos a estabelecer com CSP, e alinhados com os requisitos a estabelecer pela AP, mais restritivos e conformes com especificidades militares (p.ex. segurança, localização, infraestrutura de transporte, latência da rede);
- Definir *framework* de testes de conformidade dos serviços de *clouds* públicas, a desenvolver de forma independente do CSP;
- Definir mecanismos de monitorização e previsão de custos dos serviços *cloud* contratados;
- Definir estratégias operacionais de saída de serviços *cloud*;
- Identificar a capacidade mínima resiliente alternativa aos serviços adotados em *clouds* públicas, a explorar em situações disruptivas;
- Estabelecer parcerias com universidades e com a indústria nacional com o objetivo de potenciar a investigação e desenvolvimento, vocacionado para o setor militar, nas áreas de *data science*, IA, *cloud computing* e *machine learning*.

Liderança

CIO transversal à DN

- Estabelecer liderança efetiva da capacidade, através da criação de CIO ao nível da DN e da estrutura de governação TIC.

Pessoal

Manter RH adequados em número e qualificação

- Centralizar RH afetos à capacidade, garantindo em cada entidade capacidade própria autónoma para gestão dos serviços orgânicos;
- Definir mecanismos de recrutamento, seleção e retenção específicos para as funções associadas à área, dentro das limitações inerentes à condição militar, e às regras de movimentação de pessoal e progressão na carreira;
- Analisar mecanismos de contratação de pessoal civil para complementar possíveis, e muito específicas/cirúrgicas necessidades da área.

Infraestruturas

Racionalizar e adequar CD à capacidade de forma resiliente

- Implementar *cloud* privada da DN em CD *on-premises*, selecionados de entre os CD existentes, de acordo com critérios a estabelecer pela estrutura de governação;
- Racionalizar capacidades existentes nos restantes CD, afetas a sistemas *Fit for Purpose* (*clouds* privadas e modelo tradicional);
- Criar resiliência, com implementação de mecanismos de *backup* e *disaster recovery*.

[Cont.]

Interoperabilidade

Normalizar serviços e trocas de dados

- Estabelecer mecanismos de interoperabilidade entre as componentes públicas e privadas, quando garantidos os requisitos de segurança definidos pelas entidades competentes;
- Identificar *standards* e protocolos universais para trocas de dados entre entidades da DN e entre estas e entidades externas;
- Identificar serviços transversais a centralizar.

Figura 5 – Armazenamento e processamento de dados de acordo com os vetores DOTMLPII

7. Conclusões

O desenvolvimento tecnológico verificado nos últimos anos potenciou uma transformação substancial na forma como são recolhidos e processados dados. Proliferam sensores de diversas tipologias, recolhendo dados em volumes e formatos diferentes, cujo tratamento deve ser efetuado em tempo quase real, ou em momentos temporais estipulados, consoante a finalidade a que se destinam.

É sobre os dados que assentam, cada vez mais, os processos de tomada de decisão das organizações, pelo que o impedimento de acesso aos mesmos poderá paralisá-las. A existência de estruturas de armazenamento e processamento de dados fiáveis, seguras e resilientes é, assim, fulcral.

Organizações como a NATO e a UE têm vindo a debruçar-se sobre esta matéria, colocando o foco nas componentes tecnológica (na segurança das infraestruturas físicas sobre a qual residem os dados e nos processos a eles associados), legislativa e processual, e debatendo questões como as potenciais áreas de exploração dos dados e a soberania.

O desenvolvimento do modelo *cloud computing*, que permite uma abstração dos recursos físicos sobre os quais os dados, serviços e aplicações assentam, veio alterar o paradigma associado à detenção, pelas organizações, de infraestruturas próprias, obrigando a investimentos substanciais e a uma capacidade própria de gestão das mesmas, bem como à atribuição rígida de recursos a serviços e sistemas, sem fazer deles uma exploração eficiente. Pelas suas características de escalabilidade e flexibilidade de recursos, o *cloud computing* é um modelo adequado ao processamento de *Big Data*, conceito que surge associado aos dados na forma, volume e tratamento já referidos.

Portugal, e a DN em particular, não são alheios a esta evolução, tendo-se desenvolvido, na última década, um processo de racionalização dos recursos associados às TIC do Estado, ao mesmo tempo que se davam passos na análise e adoção de modelos *cloud*, que culminaram, em 2020, na apresentação da Estratégia da AP para a *cloud*.

Neste enquadramento, afigurou-se importante aferir a forma desta estratégia ser aplicada nas FFAA, a par da adequabilidade e viabilidade daquele tipo de modelos face à atual situação das estruturas de armazenamento e processamento de dados e aos requisitos genéticos de uma organização militar.

Este estudo teve, então, como objeto o armazenamento e processamento de dados, e foi delimitado: temporalmente, ao período 2020-2021; espacialmente, às FFAA e ao MDN (serviços centrais e entidades na sua dependência); em termos de conteúdo, à

adequabilidade da adoção de novos modelos de armazenamento e processamento de dados, nomeadamente *cloud computing*, considerando os requisitos emergentes de sistemas que tratam *Big Data*.

Assim, relativamente ao OE1, *Analisar o modelo de armazenamento e processamento de dados nas Forças Armadas na era do Big Data*, e em resposta à correspondente QD1 – estudada com base na análise de conteúdo das entrevistas conduzidas a 13 *experts* das entidades da DN em estudo, do GNS e das áreas de investigação e ensino –, concluiu-se existirem diferentes modelos independentes, apresentando reduzidas sinergias. A análise à capacidade de armazenamento e processamento de dados das entidades em estudo, efetuada de acordo com os vetores de edificação de capacidades militares (DOTMLPII), permitiu concluir pela existência de áreas organizacionais com funções específicas nesta matéria, ancoradas numa liderança das chefias mas sem doutrina formalizada. A exploração e gestão de *hardware* e *software* são efetuadas de forma autónoma, ao longo do seu ciclo de vida, existindo ferramentas e metodologias de exploração de dados em diferentes estádios de maturidade, de uma forma geral não suportando o tratamento de *Big Data*, com uma interoperabilidade quase restrita ao nível dos SI de gestão. Esta exploração é efetuada em infraestruturas próprias, com RH maioritariamente internos, com diferentes práticas de formação, insuficientes em número e qualificações e com períodos de permanência incompatíveis com a *expertise* necessária. À semelhança dos modelos distintos existentes, que restringem sinergias entre entidades, nomeadamente ao nível de processos aquisitivos, as iniciativas de adoção de serviços *cloud* são reduzidas e isoladas. Apesar das reconhecidas mais-valias destes modelos quanto a economias de escala, racionalização de recursos, nomeadamente RH, e interoperabilidade, destacam-se preocupações ao nível da disponibilidade e da segurança de dados e serviços, fulcrais para as FFAA. A estratégia do Estado Português para a *cloud*, assente no princípio *cloud first* e aplicável a toda a AP é recente, existindo ainda diversos normativos e mecanismos por desenvolver, o que concorre para a inexistência de uma estratégia subsidiária na DN que dite uma abordagem estruturada e uniforme.

Quanto ao OE2, *Analisar a estratégia em matéria de armazenamento e processamento de dados de entidades congéneres na era do Big Data*, e resposta à associada QD2 – com recurso a análise documental –, concluiu-se que as estratégias adotadas nesta matéria pelas entidades congéneres estudadas (NATO e áreas da Defesa de França e dos EUA), preconizam a adoção de serviços *cloud* em detrimento de arquiteturas

tradicionais (*cloud first*), mediante avaliação prévia de viabilidade e políticas claramente estabelecidas. A sua concretização é efetuada em modelos de implementação híbridos, que contemplam o tratamento de dados mais sensíveis em *clouds* privadas, *on-premises*, em CD proprietários, e o de dados menos sensíveis em *clouds* públicas, sujeito a restrições associadas à segurança e soberania dos dados, estabelecendo-se interoperabilidade ao nível da adoção de *standards* e das trocas de dados entre os diversos modelos *cloud*. Este modelo permite direcionar recursos para serviços operacionais, reduzindo investimento em capacidades internas. A gestão da capacidade é efetuada através de estruturas organizacionais dedicadas ou com funções afins, com uma liderança de topo efetiva, tendo sido identificada a necessidade de recrutar e qualificar RH para explorar a capacidade. O modelo é considerado adequado para o desenvolvimento de projetos associados a *Big Data*, permitindo o recurso a tecnologias como IA, ou *machine learning.*

Face ao exposto, de forma a responder ao OG, *Propor contributos para otimizar o modelo de armazenamento e processamento de dados nas Forças Armadas na era do Big Data*, e à respetiva QC, concluiu-se que a otimização da forma como as FFAA gerem o armazenamento e processamento de dados, passará por, ao nível do vetor de edificação de capacidades: *doutrina*, implementar serviços *cloud* em modelo híbrido, de acordo com a premissa *cloud first*; *organização*, estabelecer a posição de CIO ao nível da DN, liderando uma estrutura organizacional a criar para a governação das TIC da DN; *treino*, capacitar o pessoal afeto às TIC e garantir a sua qualificação de forma contínua; *material*, centralizar recursos (*hardware* e *software*) e verbas necessárias à sustentação da capacidade (centralizada), bem como estabelecer um conjunto de ferramentas necessárias à normalização de processos; *liderança*, garantir uma liderança contínua da capacidade através do CIO; *pessoal*, desenvolver os mecanismos necessários à manutenção de pessoal, em número e qualificações, para a gestão da capacidade; *infraestruturas*, racionalizar e adequar os CD existentes na DN para a implementação, de forma resiliente, da capacidade; *interoperabilidade*, normalizar serviços e trocas de dados entre entidades internas e com entidades externas à DN.

Decorrentes deste estudo, assinala-se como principal **contributo para o conhecimento** a identificação de um conjunto de evidências metodológica e cientificamente validadas para otimizar o tratamento e armazenamento de dados na realidade da DN.

Identifica-se como **limitação** a este estudo, que lhe é alheia e não condicionou as conclusões apresentadas, a condição ainda pouco maturada da Estratégia *Cloud* para a AP, refletida em mecanismos, ferramentas e normativos ainda parcamente desenvolvidos e menos sintónicos com uma aprofundada análise.

Concernente a **estudos futuros**, afigura-se pertinente analisar o tratamento diferenciado de informação classificada, quer em modelos *cloud* públicos, quer privados, bem como abordar a presente temática na perspetiva das redes de comunicações e dos RH.

Como **recomendações de ordem prática**, sugere-se ao MDN, conjuntamente com o EMGFA, a adoção do modelo híbrido proposto, através da implementação das medidas apresentadas no presente estudo.

Referências bibliográficas

Agência para a Modernização Administrativa. (2020, novembro). *Estratégia Cloud para a Administração Pública em Portugal*. Retirado de https://tic.gov.pt/web/tic/-/estrategia-cloud-da-administracao-publica

Berryhill, J., Heang, K., Clogher, R., & McBride, K. (2019). Hello, World: Artificial intelligence and its use in the public sector. *OECD Working Papers on Public Governance, 36, OECD Publishing*. Paris. doi: https://doi.org/10.1787/726fd39d-en

Cavanillas, J., Curry, E., & Wahlster, W. (2016). *New Horizons for a Data-Driven Economy*. SpringerOpen.

CIO. (2020, 2 de janeiro). *Arnaud Coustillière (directeur de la DGNUM, Ministère des Armées) élu Stratège IT de l'année 2019* [Página *online*]. Retirado de https://www.cio-online.com/actualites/lire-arnaud-coustilliere-directeur-de-la-dgnum-ministere-des-armees-elu-strategе-it-de-l-annee-2019-11794.html

Comissão Europeia. (2020, 19 de fevereiro). *Uma estratégia europeia para os dados*. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1593073685620&uri=CELEX%3A52020CD0066

Data Storage Solutions Review. (2020, 24 de janeiro). *Data Storage Units of Measurement Chart from Smallest to Largest* [Página *online*]. Retirado de https://solutionsreview.com/data-storage/data-storage-units-of-measurement-chart-from-smallest-to-largest/

Direction interministérielle du numérique et du système d'information et de communication de l'Etat. (2018, 3 de julho). *Le gouvernement annonce sa stratégie en matière de cloud*. Retirado de https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-en-matiere-de-cloud

El-Seoud, S., El-Sofany, H., Abdelfattah, M., & Mohamed, R. (2017). Big Data and Cloud Computing: Trends and Challenges. *International Journal Of Interactive Mobile Technologies (IJIM), 11*(2), 34-52. doi:http://dx.doi.org/10.3991/ijim.v11i2.6561

Espinosa, J., Kaisler, S., Armour, F., & Money, W. (2019). Big Data Redux: New Issues and Challenges Moving Forward. *Proceedings of the 52nd Hawaii International Conference on System Sciences*. Maui, Hawai. doi:10.24251/HICSS.2019.131

Federal Ministry for Economic Affairs and Energy. (2020, maio). *GAIA-X: A Pitch Towards Europe - Status Report on User Ecosystems and Requirements*. Retirado de https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

Federal Ministry for Economic Affairs and Energy. (2021, 19 de abril). *GAIA-X: A Federated Data Infrastructure for Europe* [Página *online*]. Retirado de https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

Ferreira, R. (2020). *Implementação de uma rede de dados única na Defesa*. (Trabalho de Investigação Individual CPOG 2019/20). Lisboa: Instituto Universitário Militar.

Global Newswire. (2019, 23 de maio). *The French Defense Procurement Agency selects the consortium led by Atos for Project Artemis, phase II*. Retirado de https://www.globenewswire.com/news-release/2019/05/23/1841354/0/en/The-French-Defense-Procurement-Agency-selects-the-consortium-led-by-Atos-for-Project-Artemis-phase-II.html

Governo da República Portuguesa (2021, 23 de abril). *Sines receberá o maior investimento estrangeiro das últimas décadas* [Página *online*]. Retirado de https://www.portugal.gov.pt/pt/gc22/comunicacao/noticia?i=sines-recebera-o-maior-investimento-estrangeiro-das-ultimas-decadas

IBM. (2020, 25 de novembro). *Cloud computing* [Página *online*]. Retirado de https://www.ibm.com/cloud/learn/cloud-computing

Information Systems Audit and Control Association. (2015). *ISACA Glossary of Terms - Portuguese* (3*rd Edition*). Information Systems Audit and Control Association. Retirado de https://www.isaca.org/resources/glossary

Johnsen, F. (2019, 10 de outubro). *Towards Big Data in the Tactical Domain*. NATO Science and Technology Organization.

Jornal Económico. (2021, 14 de abril). *Altice, Microsoft e HPE formam parceria. Centro de dados da Covilhã acolhe oferta de cloud "híbrida" inédita em Portugal* [Página *online*]. Retirado de https://jornaleconomico.sapo.pt/noticias/altice-microsoft-e-hp-firmam-parceria-centro-de-dados-da-covilha-acolhe-oferta-de-cloud-hibrida-inedita-em-portugal-726397

Maurer, T., & Hinck, G. (2020, agosto). *Cloud security – a primer for policy makers*. Carnegie Endowment for International Peace. Retirado de https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597

Mazumdar, S., Seybold, S., Kritikos, D., & Verginadis, Y. (2019). A survey on data storage and placement methodologies for Cloud-Big Data ecosystem. *Journal of Big Data*, *6*(15). Retirado de https://doi.org/10.1186/s40537-019-0178-3

Microsoft Corporation. (2020). *Accelerating Modern Workplace Productivity Adoption*. Retirado de https://adoption.microsoft.com/enabling-modern-collaboration/

Ministère des Armées. (2017a, 10 de maio). *Du Cloud Défense à la transformation digitale*. Retirado de https://www.defense.gouv.fr/english/ema/transformation/actualites/du-cloud-defense-a-la-transformation-digitale

Ministère des Armées. (2017b, dezembro). *Ambition Numérique - Ministère des Armées*. Retirado de https://www.defense.gouv.fr/defenseconnect/documents-de-reference/ambition-numerique-du-ministere-des-armees

Ministère des Armées. (2018, 19 de abril). *Schéma directeur de la transformation numérique*. Retirado de https://www.defense.gouv.fr/defenseconnect/documents-de-reference

Ministère des Armées. (2019, setembro). *Artificial Intelligence in support of Defence*. Retirado de https://www.defense.gouv.fr/salle-de-presse/communiques/communique_publication-du-rapport-du-ministere-des-armees-sur-l-intelligence-artificielle

Ministère des Armées. (2020). *La Transformation numérique du ministère des Armées – concepts clés*. Retirado de https://www.defense.gouv.fr/defenseconnect/actualites/journee-d-echanges-autour-de-la-transformation-numerique-du-ministere-des-armees

Ministério da Defesa Nacional. (2014). *Conceito Estratégico Militar – CEM 2014. Aprovado pelo Ministro da Defesa Nacional em 22 de julho de 2014. Confirmado em Conselho Superior de Defesa Nacional de 30 de julho de 2014*. Lisboa: Autor.

National Institute of Standards and Technology. (2011, setembro). *The NIST definition of Cloud Computing. Special Publication 800-145*. Gaithersburg: Autor.

National Institute of Standards and Technology. (2015, setembro). *NIST Big Data Interoperability Framework: Volume 1 - Definitions*. Retirado de doi: http://dx.doi.org/10.6028/NIST.SP.1500-1

National Institute of Standards and Technology. (2018, junho). *NIST Big Data Interoperability Framework: Volume 6 - Reference Architecture*. NIST.SP.1500-6r1. Retirado de https://doi.org/10.6028/NIST.SP.1500-6r1

NATO Communications and Information Agency. (2017, 30 de março). *NATO signs milestone contract for IT modernization*. Retirado de

https://www.ncia.nato.int/about-us/newsroom/nato-signs-milestone-contract-for-it-modernization.html

NATO Communications and Information Agency. (2019, 13 de maio). *NCI Agency races to the cloud for unclassified portals*. Retirado de https://www.ncia.nato.int/about-us/newsroom/nci-agency-races-to-the-cloud-for-unclassified-portals.html

North Atlantic Treaty Organization. (2007, 11 de dezembro). *NATO Information Management Policy*. C-M(2007)0118. Bruxelas: North Atlantic Council.

North Atlantic Treaty Organization. (2015, 14 de dezembro). *The NATO Enterprise approach for the delivery of C3 capabilities and the provision of ict services*. AC/322-D(2015)0014-REV3. Bruxelas: North Atlantic Council.

North Atlantic Treaty Organization. (2016, 7 de janeiro). *NATO Cloud Computing Policy*. AC/322-D(2016)0001. Bruxelas: North Atlantic Council.

North Atlantic Treaty Organization. (2019a, 3 de janeiro). *Supporting document for the protection of NATO information within public cloud-based Communication and Information Systems (CIS)*. AC/35-D/1050, AC/322-D(2019)0001. Bruxelas: North Atlantic Council.

North Atlantic Treaty Organization. (2019b, 13 de fevereiro). *NATO Chief Information Officer (CIO)*. AC/322-D(2019)0008(INV). Bruxelas: North Atlantic Council.

North Atlantic Treaty Organization. (2019c, 3 de maio). *New Task for the Cyber Defence Capability Team (CD CaT): Cloud Security Technical Directive*. AC/322(CP/4)N(2019)0011-REV2 (INV). Bruxelas: North Atlantic Council.

North Atlantic Treaty Organization. (2020, 12 de março). *NATO Cloud Computing Directive*. AC/322-D(2019)0032-REV2 (INV). Bruxelas: North Atlantic Council.

North Atlantic Treaty Organization. (2021, 8 de janeiro). *NIAG study on Emerging and Disruptive Technologies, in the context of Emerging Powers - Final report*. AC/259-D(2021)0001 NIAG-D(2021)0004. Bruxelas: North Atlantic Council.

Opara-Martins, J., Sahandi, R., & Tian, F. (2016) Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *J Cloud Comp 5, 4*. Retirado de https://doi.org/10.1186/s13677-016-0054-z

Rego, A., Cunha, M. P., & Meyer Jr., V. (2019). Quantos participantes são necessários para um estudo qualitativo? Linhas práticas de orientação. *Revista De Gestão Dos Países de Língua Portuguesa, 17*(2), 43-57. https://doi.org/10.12660/rgplp.v17n2.2018.78224

Regulamento do Parlamento Europeu e do Conselho n.º 679/2016, de 27 de abril (2016). *Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0679

Regulamento do Parlamento Europeu e do Conselho n.º 881/2019, de 17 de abril (2019). *Relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n. o 526/2013 (Regulamento Cibersegurança).* Retirado de https://op.europa.eu/en/publication-detail/-/publication/35e93bb4-8905-11e9-9369-01aa75ed71a1/language-pt

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, 596-605. 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, 1981-1995. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 26/2013, de 11 de abril (2013). *Aprova as linhas de orientação para a execução da reforma estrutural da Defesa Nacional e das Forças Armadas, designada por Reforma «Defesa 2020»*. Diário da República 1.ª Série, 77, 2285-2289 . Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 46/2011, de 27 de outubro (2011). *Cria o Grupo de Projecto para as Tecnologias de Informação e Comunicação*. Diário da República, 1.ª Série, 218, 4848. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 84/2020, de 1 de outubro (2020). *Prorroga o mandato do grupo de projeto «Conselho para as Tecnologias de Informação e Comunicação na Administração Pública»*. Diário da República, 1.ª Série, 197, 6-8. Lisboa: Presidência do Conselho de Ministros.

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

Tawalbeh, L., & Saldamli, G. (2019). Reconsidering big data security and privacy in cloud and mobile cloud systems. *Journal of King Saud University – Computer and Information Sciences*. Retirado de https://doi.org/10.1016/j.jksuci.2019.05.007

United States Departament of Defense. (2018, dezembro). *DoD Cloud Strategy*. Retirado de https://dodcio.defense.gov/Library/

United States Departament of Defense. (2019, 12 de julho). *DoD Digital Modernization Strategy*. Retirado de https://dodcio.defense.gov/Library/

United States Departament of Defense. (2020, setembro). *DoD Data Strategy*. Retirado de https://dodcio.defense.gov/Library/

United States Departament of Defense. (2021, 7 de fevereiro). *Enterprise Cloud* [Página *online*]. Retirado de https://www.cloud.mil/

World Economic Forum. (2020, outubro). *The future of Jobs Report 2020*. Retirado de https://www.weforum.org/reports

Apêndice A — Corpo de Conceitos

Ciclo de vida da informação – Planeamento, recolha, criação ou geração de informação, organização, recuperação, utilização, acessibilidade, transmissão, armazenamento, proteção e disposição (NATO, 2007).

Continuidade de Negócio – Processo de uma organização para fazer face a uma disrupção de serviços, envolvendo atividades de prevenção, de mitigação e de recuperação (*Information Systems Audit and Control Association* [ISACA], 2015). Depende diretamente do *disaster recovery plan* para a reposição de serviços críticos (ISACA, 2015).

***Data Science* –** Extração de conhecimento diretamente a partir de dados, através de um processo de descoberta, hipótese e teste da hipótese (tradução direta a partir de NIST, 2015).

***Disaster recovery* –** Implementação de um conjunto de atividades e processos que visam repor as atividades de negócio críticas de uma organização, após uma falha ou interrupção de serviços (ISACA, 2015).

Informação – Qualquer comunicação ou representação de conhecimento (factos, dados ou opiniões) utilizando qualquer meio ou forma (audiovisual, narrativa, cartográfica, numérica, gráfica, textual) (NATO, 2007).

Infraestrutura *cloud* - Todos os recursos de *hardware* e *software* que permitem disponibilizar serviços de acordo com as características do modelo *cloud* (NIST, 2011). Compreende uma camada física, que engloba servidores e componentes de armazenamento e de rede, e uma camada de abstração, composta por *software* implementado sobre a componente física (NIST, 2011).

Infraestrutura TIC – Conjunto de recursos de *hardware*, *software* e *networking* que permitem a uma organização disponibilizar soluções de tecnologias de informação e comunicações aos seus utilizadores (NATO, 2016).

Inteligência Artificial – Termo genérico associado a computadores, máquinas ou sistemas que parecem ter a capacidade de imitar o raciocínio humano, utilizado para descrever quer uma tecnologia quer uma área de pesquisa, abrangendo o desenho de sistemas inteligentes e o desenvolvimento de métodos e técnicas associadas (Berryhill, Heang, Clogher, & McBride, 2019). São abrangidas nesta área de pesquisa considerações de ordem ética e de impacto social dos referidos sistemas (Berryhill et al., 2019).

Machine learning – Conjunto de técnicas que permitem uma aprendizagem automatizada, sem intervenção humana, por parte de máquinas, com base em padrões e inferências, que

pode ser efetuada através de treino, fornecendo à máquina um conjunto de situações corretas para assimilação, ou por situações de tentativa/erro, interpretando regras fornecidas (Berryhill et al., 2019). É considerada uma subárea da IA (Berryhill et al., 2019).

Resiliência – Capacidade de um sistema recuperar rapidamente de uma disrupção ou de resistir a uma falha, com efeitos mínimos associados (ISACA, 2015).

Apêndice B — Modelo de análise

<table>
<tr><td>Objetivo Geral</td><td colspan="4">Propor contributos para otimizar o modelo de armazenamento e processamento de dados nas Forças Armadas na era do Big Data</td></tr>
<tr><td rowspan="2">Objetivos Específicos</td><td>Questão Central</td><td colspan="3">Como contribuir para otimizar o modelo de armazenamento e processamento de dados nas Forças Armadas na era do Big Data?</td></tr>
<tr><td colspan="2">Questões Derivadas</td><td>Conceitos</td><td>Dimensões</td><td>Técnicas de recolha de dados</td></tr>
<tr><td rowspan="10">OE1
Analisar o modelo de armazenamento e processamento de dados nas Forças Armadas na era do Big Data</td><td colspan="2" rowspan="10">QD1
Qual é o modelo de armazenamento e processamento de dados nas Forças Armadas na era do Big Data?</td><td rowspan="8">Armazenamento e processamento de dados</td><td>Doutrina</td><td rowspan="18">Análise documental e entrevistas semiestruturadas</td></tr>
<tr><td>Organização</td></tr>
<tr><td>Treino</td></tr>
<tr><td>Material</td></tr>
<tr><td>Liderança</td></tr>
<tr><td>Pessoal</td></tr>
<tr><td>Infraestruturas</td></tr>
<tr><td>Interoperabilidade</td></tr>
<tr><td rowspan="3">Big Data</td><td>Doutrina</td></tr>
<tr><td>Segurança</td></tr>
<tr><td>Infraestruturas</td></tr>
<tr><td rowspan="10">OE2
Analisar a estratégia em matéria de armazenamento e processamento de dados de entidades congéneres na era do Big Data</td><td colspan="2" rowspan="10">QD2
Qual é a estratégia em matéria de armazenamento e processamento de dados de entidades congéneres na era do Big Data?</td><td rowspan="8">Armazenamento e processamento de dados</td><td>Doutrina</td></tr>
<tr><td>Organização</td></tr>
<tr><td>Treino</td></tr>
<tr><td>Material</td></tr>
<tr><td>Liderança</td></tr>
<tr><td>Pessoal</td></tr>
<tr><td>Infraestruturas</td></tr>
<tr><td>Interoperabilidade</td></tr>
<tr><td rowspan="3">Big Data</td><td>Doutrina</td></tr>
<tr><td>Segurança</td></tr>
<tr><td>Infraestruturas</td></tr>
</table>

Apêndice C — Identificação dos entrevistados

Cargo	Titular	Fase		Área de *expertise*
		E	C	
Diretor-Geral do GNS	Contra-almirante Gameiro Marques		✓	GNS
Subchefe do Estado-Maior da FA, Diretor de Informação da FA	Major-general Teodorico Lopes		✓	FA
Secretário-Geral Adjunto do MDN	Comodoro Alves Francisco		✓	MDN
Superintendente das Tecnologias da Informação da Marinha	Comodoro Cancela Roque	✓	✓	Marinha
Ex-Diretor da DCSI do Exército	Brigadeiro-general Francisco Soares	✓		Exército
Diretor da DIRCSI do EMGFA	Brigadeiro-general João Rocha	✓	✓	EMGFA
Diretor da DCSI do Exército	Brigadeiro-general Luís Camelo		✓	Exército
Diretor dos Sistemas de Informação da DSSI da SGMDN	Coronel Carlos Passos	✓		MDN
Ex-Docente de Engenharia Organizacional na Academia da Força Aérea	Coronel Carlos Páscoa		✓	Investigação e ensino
Chefe da Repartição de Sistemas e Tecnologias de Informação da DIRCSI do EMGFA e ex-Adjunto da FA para aquela função	Coronel Helder Guerreiro	✓		EMGFA
Subdiretor da DCSI da FA e ex-Chefe da Repartição de Tecnologias de Informação da DCSI	Coronel José Mendes	✓		FA
Representante nacional no Secretariado do programa *Federated Mission Networking* (FMN) na NATO	Tenente-coronel António Valente	✓		EMGFA-FMN
Professor Catedrático Distinto Jubilado do Instituto Superior Técnico, e Fundador e Investigador Emérito do Instituto de Engenharia de Sistemas e Computadores	Professor Doutor José Tribolet		✓	Investigação e ensino

Legenda: Entrevista conduzida numa fase exploratória (E) ou numa fase de "campo", propriamente dito (C).

Apêndice D — Guião de entrevista semiestruturada a entidades da Defesa Nacional

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE PROMOÇÃO A OFICIAL GENERAL
2020/2021

ENTREVISTA SEMIESTRUTURADA

O presente guião de entrevista semiestruturada foi elaborado no âmbito do Trabalho de Investigação Individual do Curso de Promoção a Oficial General 2021/21 pela Coronel Engenheira Informática Ana Cristina Domingos de Oliveira Rodrigues Telha, e pretende analisar o modelo de armazenamento e processamento de dados nas Forças Armadas na era do *Big Data*.

Atualmente, face ao volume de dados produzidos, fruto da proliferação de fontes, quer em número, quer em diversidade, é requerido às organizações que disponham de modelos de processamento e armazenamento de dados ágeis, escaláveis, flexíveis e seguros. Aos conjuntos de dados cujo tratamento, pelas suas características (dimensão, variedade, velocidade de atualização e transmissão ou variabilidade, entre outras), seja inviável com recurso aos tradicionais modelos, dá-se o nome de *Big Data*.

O modelo *cloud computing* afigura-se como uma possível solução para fazer face aos desafios indicados, apresentando diversas arquiteturas de implementação e disponibilização de serviços.

Através da presente investigação, pretende-se, por um lado, aferir de que forma se encontra organizado o armazenamento e processamento de dados nas Forças Armadas, e qual a sua capacidade de incorporação dos novos requisitos já mencionados e, por outro, identificar propostas de otimização, com base na análise do modelo *cloud computing*.

Face ao anteriormente exposto, o contributo de V/ Exa. constitui-se como uma mais-valia para a investigação em curso e, consequentemente, para a qualidade das conclusões a alcançar e das recomendações a efetuar.

Neste sentido, solicito autorização para que as suas respostas, ou excertos das mesmas, devidamente contextualizados, sejam citados e identificados. Caso, em alternativa, não deseje ser identificado, será assegurada a salvaguarda do anonimato e confidencialidade das respostas prestadas.

Ressalva-se, para os devidos efeitos, que os resultados da investigação terão o grau de classificação de segurança NÃO CLASSIFICADO.

Muito obrigada pela colaboração.

1 - Caracterização da situação atual

Por modelo de armazenamento e processamento de dados entende-se o conjunto de recursos (infraestruturas, *hardware* e *software*) utilizados para processar e armazenar os dados de uma Organização ao longo do seu ciclo de vida.

Como caracteriza o modelo de armazenamento e processamento de dados da sua Organização, numa análise efetuada de acordo com os diversos vetores de edificação de uma capacidade militar:

1.1 (D)outrina (Estratégias, planos, diretivas, normas de execução)

1.2 (O)rganização (Área Organizacional responsável pela implementação, exploração e sustentação da capacidade)

1.3 (T)reino (Formação, qualificação, treino e exercícios)

1.4 (M)aterial (*Hardware*, *software* e respetivos financiamento e processos aquisitivos)

1.5 (L)iderança (Determinação da exploração da capacidade pelas chefias)

1.6 (P)essoal (Recursos humanos [internos/externos] envolvidos na implementação, exploração e sustentação da capacidade)

1.7 (I)nfraestruturas (Instalações onde se encontra instalada a capacidade)

1.8 (I)nteroperabilidade (Relacionamento inter-entidades [Ministério da Defesa Nacional, Estado-Maior-General das Forças Armadas, Ramos])

2 – *Big Data*

2.1 - Face ao descrito em 1., considera que o atual modelo de armazenamento e processamento de dados da sua Organização se encontra adequado aos requisitos impostos na abordagem a *Big Data*, nomeadamente no que respeita a disponibilidade de recursos (humanos e materiais), escalabilidade, flexibilidade e segurança?

2.2 – Existem, ou encontram-se previstos, na sua Organização, requisitos para a implementação de sistemas que se enquadrem neste âmbito?

3 – O modelo *cloud computing*

O modelo *cloud computing* tem vindo a ser adotado por diversas organizações, públicas e privadas, bem como por organizações militares, substituindo ou complementando o tradicional modelo em que os recursos são adquiridos, implementados e geridos pela Organização, em instalações próprias, dimensionados para o valor máximo de utilização e escalados de forma vertical mediante necessidade.

Este modelo é caracterizado pela rápida flexibilidade e escalabilidade, pelo acesso a um conjunto de recursos disponíveis em rede, mediante solicitação, pela abstração da implementação física do modelo e pelo controlo e monitorização dos serviços consumidos, permitindo uma gestão dos custos associados aos serviços, taxados mediante utilização. Abrange diversas modalidades de disponibilização de serviços (desde a infraestrutura física ao serviço ou sistema de informação), podendo ser implementado em infraestruturas próprias da organização ou em infraestruturas de prestadores de serviços externos, de acordo com um modelo privado, comunitário, híbrido ou público.

A arquitetura de armazenamento e processamento de dados de uma Organização pode resultar da composição de diversos modelos de disponibilização de serviços e de implementação.

3.1 – Existem, ou estão previstas, implementações de modelos *cloud computing* na sua Organização?

3.2 – Existe na sua Organização um enquadramento doutrinário relativo a esta matéria?

3.3 – Considera adequada a utilização de serviços de *clouds* públicas pela sua Organização? Se sim, qual o grau de classificação de segurança da informação a tratar por estes serviços?

3.4 – Que vantagens/desvantagens encontra no modelo de utilização de serviços de *clouds* públicas, no que concerne a:

3.4.1 – Custos, considerando que neste modelo serão cobrados os recursos utilizados (*pay as you use*), contrapondo com o investimento necessário à aquisição, sustentação e gestão de recursos próprios (consequente transição de orçamento *Capital Expenditure – CapEx*, para *Operational Expenditure – OpEx*)

3.4.2 – Flexibilidade e escalabilidade de recursos

3.4.3 - Disponibilidade

3.4.4 – Segurança

3.4.5 – Recursos humanos (incluindo formação e qualificação)

3.5 - Considera adequada a implementação de *clouds* privadas que sirvam a Defesa Nacional, em modelo a determinar (privado, comunitário), que permitam o processamento de informação classificada e não classificada?

3.6 – Que vantagens/desvantagens encontra no modelo de utilização de serviços de *clouds* privadas, no que concerne a:

3.6.1 – Custos, considerando que os recursos utilizados serão da responsabilidade das entidades que implementam a *cloud*.

3.6.2 – Flexibilidade e escalabilidade de recursos

3.6.3 - Disponibilidade

3.6.4 – Segurança

3.6.5 – Recursos humanos (incluindo formação e qualificação)

Apêndice E — Guião de entrevista semiestruturada ao Gabinete Nacional de Segurança

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE PROMOÇÃO A OFICIAL GENERAL
2020/2021

ENTREVISTA SEMIESTRUTURADA

O presente guião de entrevista semiestruturada foi elaborado no âmbito do Trabalho de Investigação Individual do Curso de Promoção a Oficial General 2021/21 pela Coronel Engenheira Informática Ana Cristina Domingos de Oliveira Rodrigues Telha, e pretende analisar o modelo de armazenamento e processamento de dados nas Forças Armadas na era do *Big Data*.

Atualmente, face ao volume de dados produzidos, fruto da proliferação de fontes, quer em número, quer em diversidade, é requerido às organizações que disponham de modelos de processamento e armazenamento de dados ágeis, escaláveis, flexíveis e seguros. Aos conjuntos de dados cujo tratamento, pelas suas características (dimensão, variedade, velocidade de atualização e transmissão ou variabilidade, entre outras), seja inviável com recurso aos tradicionais modelos, dá-se o nome de *Big Data*.

O modelo *cloud computing* afigura-se como uma possível solução para fazer face aos desafios indicados, apresentando diversas arquiteturas de implementação e disponibilização de serviços.

Através da presente investigação, pretende-se, por um lado, aferir de que forma se encontra organizado o armazenamento e processamento de dados nas Forças Armadas, e qual a sua capacidade de incorporação dos novos requisitos já mencionados e, por outro, identificar propostas de otimização, com base na análise do modelo *cloud computing*.

Face ao anteriormente exposto, o contributo de V/ Exa. constitui-se como uma mais-valia para a investigação em curso e, consequentemente, para a qualidade das conclusões a alcançar e das recomendações a efetuar.

Neste sentido, solicito autorização para que as suas respostas, ou excertos das mesmas, devidamente contextualizados, sejam citados e identificados. Caso, em alternativa, não deseje ser identificado, será assegurada a salvaguarda do anonimato e confidencialidade das respostas prestadas.

Ressalva-se, para os devidos efeitos, que os resultados da investigação terão o grau de classificação de segurança NÃO CLASSIFICADO.

Muito obrigada pela colaboração.

1 – A *North Atlantic Treaty Organization* (NATO) preconiza a implementação de uma infraestrutura de Tecnologias de Informação e Comunicações (TIC) baseada no modelo *cloud*, que permita o tratamento de todos os níveis de segurança de informação até *NATO SECRET* (NATO *Cloud Computing Policy*, janeiro de 2016). Para a informação com os graus *NATO CONFIDENTIAL* e acima deverá ser utilizado o modelo de implementação privado, enquanto que, para a informação com graus de classificação *NATO RESTRICTED* e inferior, poderão ser utilizados modelos comunitários, híbridos ou públicos. Considera viável a aplicação de um modelo similar às entidades da Defesa Nacional (DN)?

2 - Alinhada com os trabalhos desenvolvidos nos últimos anos no âmbito da implementação de serviços *cloud* na Administração Pública (AP), a Resolução do Conselho de Ministros n.º 84/2020 determinou a identificação e criação - por parte do Conselho para as Tecnologias de Informação e Comunicação na Administração Pública e do Gabinete Nacional de Segurança - de um conjunto de instrumentos que suportem o processo de adoção e aquisição daquele tipo de serviços. Quando estima serem disponibilizados os

referidos instrumentos, qual a sua abrangência e qual considera ser a penetração expectável deste tipo de serviços na AP?
3 – No que às entidades da DN (Estado-Maior-General das Forças Armadas, Ramos e Ministério da Defesa Nacional) respeita, que restrições poderão ser impostas na adoção de serviços de *clouds* públicas?
4 – Que vantagens/desvantagens identifica na adoção de serviços de *clouds* públicas por entidades da DN?
5 – Que desafios identifica na adoção de modelos *cloud* por entidades da DN?
6 – Na sua perceção, de que forma podem as entidades académicas, de investigação e a indústria TIC nacional proporcionar um apoio efetivo ao desenvolvimento de capacidades nacionais no âmbito da implementação de modelos *cloud*, nomeadamente na área da DN?
7 – No que respeita à abordagem a *Big Data*, considera existirem requisitos específicos, nomeadamente no domínio da segurança dos dados e dos sistemas, a serem endereçados?

Apêndice F — Guião de entrevista semiestruturada a entidades de investigação e ensino

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE PROMOÇÃO A OFICIAL GENERAL
2020/2021

ENTREVISTA SEMIESTRUTURADA

O presente guião de entrevista semiestruturada foi elaborado no âmbito do Trabalho de Investigação Individual do Curso de Promoção a Oficial General 2021/21 pela Coronel Engenheira Informática Ana Cristina Domingos de Oliveira Rodrigues Telha, e pretende analisar o modelo de armazenamento e processamento de dados nas Forças Armadas na era do *Big Data*.

Atualmente, face ao volume de dados produzidos, fruto da proliferação de fontes, quer em número, quer em diversidade, é requerido às organizações que disponham de modelos de processamento e armazenamento de dados ágeis, escaláveis, flexíveis e seguros. Aos conjuntos de dados cujo tratamento, pelas suas características (dimensão, variedade, velocidade de atualização e transmissão ou variabilidade, entre outras), seja inviável com recurso aos tradicionais modelos, dá-se o nome de *Big Data*.

O modelo *cloud computing* afigura-se como uma possível solução para fazer face aos desafios indicados, apresentando diversas arquiteturas de implementação e disponibilização de serviços.

Através da presente investigação, pretende-se, por um lado, aferir de que forma se encontra organizado o armazenamento e processamento de dados nas Forças Armadas, e qual a sua capacidade de incorporação dos novos requisitos já mencionados e, por outro, identificar propostas de otimização, com base na análise do modelo *cloud computing*.

Face ao anteriormente exposto, o contributo de V/ Exa. constitui-se como uma mais-valia para a investigação em curso e, consequentemente, para a qualidade das conclusões a alcançar e das recomendações a efetuar.

Neste sentido, solicito autorização para que as suas respostas, ou excertos das mesmas, devidamente contextualizados, sejam citados e identificados. Caso, em alternativa, não deseje ser identificado, será assegurada a salvaguarda do anonimato e confidencialidade das respostas prestadas.

Ressalva-se, para os devidos efeitos, que os resultados da investigação terão o grau de classificação de segurança NÃO CLASSIFICADO.

Muito obrigada pela colaboração.

1 – A *North Atlantic Treaty Organization* (NATO) preconiza a implementação de uma infraestrutura de Tecnologias de Informação e Comunicações (TIC) baseada no modelo *cloud*, que permita o tratamento de todos os níveis de segurança de informação até *NATO SECRET* (NATO *Cloud Computing Policy*, janeiro de 2016). Para a informação com os graus *NATO CONFIDENTIAL* e acima deverá ser utilizado o modelo de implementação privado, enquanto que, para a informação com graus de classificação *NATO RESTRICTED* e inferior, poderão ser utilizados modelos comunitários, híbridos ou públicos. Considera viável a aplicação de um modelo similar às entidades da Defesa Nacional (DN)?

2 - Alinhada com os trabalhos desenvolvidos nos últimos anos no âmbito da implementação de serviços *cloud* na Administração Pública (AP), a Resolução do Conselho de Ministros n.º 84/2020 determinou a identificação e criação - por parte do Conselho para as Tecnologias de Informação e Comunicação na Administração Pública e do Gabinete Nacional de Segurança - de um conjunto de instrumentos que suportem o processo de adoção e aquisição daquele tipo de serviços. No que às entidades da DN (Estado-Maior-General das Forças Armadas, Ramos e Ministério da Defesa Nacional) respeita, que restrições considera que deverão ser efetuadas na adoção de serviços de *clouds* públicas?

3 – Que vantagens/desvantagens identifica na adoção de serviços de *clouds* públicas por entidades da DN?

4 – Que desafios identifica na adoção de modelos *cloud* por entidades da DN?
5 – Na sua perceção, de que forma podem as entidades académicas, de investigação e a indústria TIC nacional proporcionar um apoio efetivo ao desenvolvimento de capacidades nacionais no âmbito da implementação de modelos *cloud*, nomeadamente na área da DN?
6 – No que respeita à abordagem a *Big Data*, considera existirem requisitos específicos a serem endereçados numa implementação num modelo *cloud*?

Apêndice G — Análise comparativa dos modelos *cloud* pelas entidades da Defesa Nacional

***Cloud* Pública**		
Custos	SGMDN	✓ Diminui necessidade de investimento na aquisição e modernização da infraestrutura subjacente, nomeadamente para SI de Gestão – modelo PaaS.
	EMGFA	✓ Possível "[…] exploração mais otimizada e, consequentemente mais eficiente" × "[…] contratação pública não está ainda adequada para esta transição [provisionamento dinâmico]".
	Marinha	✓ "…não obriga à gestão do ciclo de vida da capacidade".
	Exército	✓ "[Desnecessários] com a estrutura para efetuar *backup* (embora esteja naturalmente diluídos no custo do serviço)"; ✓ "A vantagem de crescimento garantida pelo modelo "pay as you use""… × …é desvanecida pela falta de disciplina e formação dos principais utilizadores"; × "O investimento constante não é adequado para o modelo de financiamento e aquisição do Exército".
	FA	✓ "Alívio no investimento na aquisição e manutenção, não só do serviço (SW) como da plataforma de base (HW), contudo…"; × "…o desinvestimento interno em capacidades próprias colocará o Ramo numa posição vulnerável, pois aquando de eventuais cortes orçamentais, será difícil recuperar, dado que o valor a investir visando a recuperação de capacidades será muito maior"; × Necessidade de financiamento plurianual;
Flexibilidade e Escalabilidade de recursos	SGMDN	✓ Solução muito vantajosa; ✓ Mais capacidade de disponibilizar serviços quer relativamente ao modelo privado, quer à situação atual.
	EMGFA	✓ "Resposta de escalabilidade mais dinâmica quer para o provisionamento, quer para desaprovisionamento".
	Marinha	✓ "Permite crescer consoante as necessidades".
	Exército	✓ "A capacidade e estrutura públicas não são da responsabilidade do utilizador e o crescimento é garantido pelo fornecedor do serviço".
	FA	✓ Vantajoso.
Disponibilidade	SGMDN	✓ Solução vantajosa; × Não existem garantias em situação de crise.
	EMGFA	✸ Estabelecimento de "SLA contratuais dinâmicos em função das necessidades, normalmente incluindo alta-disponibilidade e redundância física e geográfica".
	Marinha	✓ O *service provider* (no caso já existente na Marinha, a Microsoft) disponibiliza suporte H24, mediante o SLA estabelecido; ✓ A disponibilidade tem que ver com a confiança no *Service Provider*.
	Exército	✓ "A utilização de recursos tem uma disponibilidade garantida pelo fornecedor e mantida em valores bastante elevados, mas…"; × "…não existe controlo da estrutura, do estado e das avarias. Não é possível dar prioridades em caso de indisponibilidade".
	FA	✓ Solução vantajosa, contudo… × …dependência da prestação de serviço de uma entidade civil (CSP).
RH	SGMDN	✓ Solução vantajosa; ✓ Diminui necessidade de RH especialistas em Administração de Sistemas na AP e nas FFAA, para os SI de Gestão – modelo PaaS, visto não ser uma área *core* da DN.
	EMGFA	✓ "Nível de exigência ao nível dos RH, quer na quantidade quer nas competências, será inferior".
	Marinha	✓ "São libertados recursos de tarefas de rotina"; ✓ Se o serviço não for prestado *on-premises*, o RH é libertado desta tarefa.

	Exército	✓ "A formação e qualificação é necessária apenas do ponto de vista de utilização da estrutura e alguma gestão para garantir os requisitos e uma correta distribuição […]"; × "[…] não permite a passagem de *know how* em termos de gestão de uma plataforma de armazenagem de informação para os RH do Exército, o que se torna gravoso nos casos em que será necessário atuar sem ter acesso a essa funcionalidade, quer por essa se encontrar inoperacional (caso de catástrofe, p. ex.), quer por o Exército ter de operar em ambientes onde não estão disponíveis estes recursos (teatros de operação fora do território nacional)".
	FA	✓ Libertação de RH qualificados para outras tarefas, convergindo para a simplificação e agilização de processos da organização; ✓ Contribui para "a mobilidade dos militares, a reformulação de processos intersectoriais, bem como a concentração dos RH qualificados em áreas estratégicas, mitigando assim vulnerabilidades"; ✓ Redução de custos em formação inicial.
Segurança	SGMDN	✓ Vantajoso, desde que garantidos todos os requisitos de credenciação ("desde que o *Service Provider* seja certificado pelo GNS, o grau de classificação poderá ir, teoricamente, até CONFIDENCIAL"); ✓ Vantajoso do ponto de vista aplicacional, "nomeadamente pela disponibilização contínua de atualizações de segurança de *software"*. ✸ Necessidade de acautelar "fatores como a nacionalidade do *Service Provider*, bem como a localização dos centros de dados onde os serviços ficarão alojados".
	EMGFA	✸ Necessidade de "certificações de segurança e de proteção de informação adequadas, de acordo com os normativos emitidos pelas entidades nacionais e internacionais competentes".
	Marinha	✓ "O CSP tem mecanismos de segurança implementados, que garantem que os dados se encontram seguros. No caso […] foi implementado duplo fator de autenticação dos utilizadores". × Os canais de comunicação e os postos de trabalho não estão credenciados para informação Reservada, apesar de já existir um CSP (Microsoft Azure) credenciado pelo GNS;
	Exército	✓ "Garantida e mantida pelo fornecedor de forma transparente e inacessível ao utilizador final, […]"; × …mas o modelo "não é adequado para as necessidades de segurança do Exército".
	FA	× Informação classificada – modelo não apropriado, "face às ameaças cibernéticas atuais e emergentes, bem como à necessária cultura de segurança por parte dos prestadores de serviços civis"; × Informação classificada – impõe cláusulas de confidencialidade com o prestador de serviços, bem como um processo complexo junto das entidades envolvidas (NATO, UE, GNS), acarretando custos elevados; ✸ Necessidade de acautelar localização dos CD;

Legenda: ✓-Vantagem; ×-Desvantagem; ✸ – Fator a considerar.

Fonte: Construído a partir de L.F. Camelo (*op. cit.*), de R.A. Francisco (*op. cit.*), de T.D. Lopes (*op. cit.*), de J.A. Rocha (*op. cit.*) e de J.P. Roque (*op. cit.*).

***Cloud* Privada**		
Custos	SGMDN	× Mais elevados; ✓Centralização de massa crítica de RH e financeira/orçamental, que se encontra agora dispersa.
	EMGFA	✸ Necessária análise de casos para concluir se "possíveis custos de utilização serão mais racionais e eficientes".
	Marinha	✸ Não existe disponibilidade financeira para contratos anuais de sustentação de equipamentos. × Desvantajoso

	Exército	✓ "O modelo em uso é "pay as you grow", permitindo um controlo centralizado por parte do Exército na sua necessidade de armazenamento e reduzindo o CapEx [*Capital Expenditure*] por evitar a aquisição de capacidade sem dela ter real necessidade"; ✓ "(…) maximizar os resultados de investimento (…)"; ✓ "Economia de escala para conseguir reduzir os custos de implementação"; × "(…) ao agrupar estruturas com culturas organizacionais diversas e com modos próprios de trabalhar, poderia dificultar o entendimento entre as diversas entidades e o investimento a realizar [cloud única]"; × Custos com a estrutura para efetuar *backup* em paralelo que acresce ao custo da infraestrutura; × As atualizações da infraestrutura têm de ser garantidas com a existência de verbas destinadas a fazer face a esta necessidade.
	FA	✓ [cloud única] Dispensa de investimento em plataformas tecnológicas próprias; ✓ [cloud única] Sinergias e economias de escala; ✓ [cloud única] Redução de custos associados à infraestrutura, à qualificação de RH e à manutenção de sistemas.
Flexibilidade e Escalabilidade de recursos	SGMDN	× Menor relativamente ao modelo público…; ✓ …maior relativamente ao modelo atual.
	EMGFA	✓ "Resposta de escalabilidade mais dinâmica quer para o provisionamento, quer para desaprovisionamento".
	Marinha	× Menor relativamente ao modelo público…; ✓ …maior relativamente ao modelo tradicional.
	Exército	✓ "Existe grande flexibilidade no modelo "pay as you grow", de uma forma transparente para os utilizadores a todos os níveis"; × "[*cloud* única] …seria proporcional ao planeamento e à precisão dos dados fornecidos pelas entidades participantes em relação à necessidade dos seus utilizadores […] modelo previsivelmente mais rígido que o modelo de *clouds* individuais, pois implica a concordância de todas as entidades para alterações na estrutura e capacidade da *cloud*".
	FA	× Menor relativamente ao modelo público…; ✓ …maior relativamente ao modelo tradicional.
Disponibilidade	SGMDN	✓ "Controlo dos SI de gestão a todo o tempo, sem o que a capacidade militar das FFAA seria irremediavelmente afetada, bastando observar que o serviço *email* (serviço de gestão), por mais que seja difícil de aceitar, é talvez o serviço mais importante na coordenação operacional e militar, em estado de crise ou outros"; ✓ Mais garantias, *a priori*, que o modelo público em situação de crise ou guerra, "estados de intervenção naturais das FFAA e para os quais se preparam"; ✓ Vantajoso face ao atual modelo de armazenamento e processamento (CD tradicional).
	EMGFA	✸ Estabelecimento de "SLA contratuais dinâmicos em função das necessidades, normalmente incluindo alta-disponibilidade e redundância física e geográfica".
	Marinha	✓ Vantajoso
	Exército	✓ Idêntica à utilização de uma cloud pública,…; × …mas condicionada pelas limitações em termos de RH; × Necessidade de estrutura para efetuar *backup* em paralelo para garantir a disponibilidade.
	FA	✓ Vantajoso apenas no caso de estabelecimento de um contrato de prestação de serviço com suporte 24/7; × [cloud única] Em caso de redução orçamental, risco de a Força Aérea não deter infraestruturas que permitam manter os serviços.
RH	SGMDN	× Necessidade de RH disponíveis e devidamente qualificados; ✸ "Crescente escassez de RH especialistas em Administração de Sistemas na AP e nas FFAA"; ✓Centralização de massa crítica de RH e financeira/orçamental, que se

		encontra agora dispersa.
	EMGFA	✓ "Nível de exigência ao nível dos RH, quer na quantidade quer nas competências, será inferior".
	Marinha	× Desvantajoso relativamente ao modelo público
	Exército	× "Dependendo da forma como a gestão desta capacidade [criação de *clouds* privadas no âmbito da Defesa] seria feita, poderia ser uma desvantagem, tendo em conta as diferentes prioridades e a capacidade de RH entre os diversos intervenientes"; ✓ "A criação de uma estrutura única para administração dos recursos poderia colmatar esta desvantagem e seria uma forma de apoiar esta estrutura e outras da mesma natureza"; × "mais vulnerável à gestão de RH feita pelas diversas entidades e pelas políticas internas de cada entidade"; × "[…] os problemas referidos […] com os RH, nomeadamente a sua quantidade e permanência em funções, pode ser um fator muito limitativo"; × "[*cloud* única] necessária uma formação intensa, capacitando a gestão de toda a estrutura com RH próprios"; × "No caso de se evoluir a estrutura para uma plataforma diferente, apenas os conhecimentos conceptuais sobre o funcionamento da *cloud* se mantêm atuais, obrigando a nova formação e inutilizando o investimento feito em formações anteriores".
	FA	✓ Libertação de RH qualificados para outras tarefas; ✸ Falta de RH qualificados na área de cibersegurança.
Segurança	SGMDN	✓ Mais garantias, *a priori*, que no modelo público em situação de crise ou guerra, estados de intervenção naturais das FFAA e para os quais se preparam; ✓ Maior segurança relativamente à *cloud* pública e ao modelo atual, proporcionando também um maior "conforto psicológico"; (…) existem fatores estritamente militares que devem ser observados e avaliados; ✸ Segurança física das instalações - modelo mais adequado, contudo mais caro".
	EMGFA	✸ Necessidade de "certificações de segurança e de proteção de informação adequadas, de acordo com os normativos emitidos pelas entidades nacionais e internacionais competentes".
	Marinha	✓ "Modelo adequado, nomeadamente para informação classificada que impõe um conjunto de medidas de segurança mais restritas".
	Exército	✓ "O controlo é interno e garantido pelas plataformas da escolha da entidade, circulando a informação por meios inteiramente controlados pelas entidades da Defesa"; × Necessidade de garantir verbas para atualização da infraestrutura.
	FA	✓ Vantajoso, desde que assegurados os recursos humanos e financeiros necessários.

Legenda: ✓-Vantagem; ×-Desvantagem; ✸ – Fator a considerar.

Fonte: Construído a partir de L.F. Camelo (*op. cit.*), de R.A. Francisco (*op. cit.*), de T.D. Lopes (*op. cit.*), de J.A. Rocha (*op. cit.*) e de J.P. Roque (*op. cit.*).

Apêndice H — Análise comparativa de entidades da Defesa Nacional

	SGMDN	EMGFA	Marinha	Exército	Força Aérea
D	- Estratégia implícita - Plano estratégico e Planos de Atividades/Gestão da SGMDN; - Não existe doutrina para a *cloud.*	- Estratégia implícita; - Arquitetura tradicional.	-Estratégia implícita -Diretiva Estratégica da Marinha, documentos setoriais (menção às TIC), programas setoriais e programas intersectoriais; - Não existe doutrina para a *cloud*, existem normas de utilização.	- Estratégia implícita; - Norma de Autoridade Técnica para gestão; -Não existe doutrina para a *cloud.*	- Estratégia implícita; - Não existe doutrina para a *cloud.*
O	- DSSI e CDD.	- DIRCSI.	- STI.	- DCSI; - Administradores de redes locais (Unidades).	- DCSI.
T	-Formação a militares e civis, quando necessária; - Disponibilização de formação a outras entidades da DN.	- Custos de formação avultados; - Necessidade de manter os RH em funções tempo suficiente para garantir treino e proficiência.	- Treino e formação realizados com frequência; - Componente de Ciberdefesa - realizados diversos exercícios e ações de sensibilização.	- *On-the-job training.*	- Formação mínima obtida em contexto de trabalho por parte do fabricante; - Os militares participam, com alguma regularidade, em exercícios internos e em exercícios coordenados pelo EMGFA em ambiente conjunto.
M	- Capacidade de armazenamento adequada, contempla crescimento (dezenas de TB); - Capacidade de processamento em processo de renovação; - Requisitos para sistemas de BI, não *Big Data;* - Capacidades para BI adequadas e expansíveis mediante requisitos;	- Modelo implica aquisição para capacidades de crescimento futuras (*upfront* – CapEx); - Atualizações requerem investimentos em *hardware*, de forma a compatibilizar com versões de *software*; - Limitações na escalabilidade e flexibilidade da atual arquitetura e inadequação da capacidade a requisitos *Big*	- *Hardware* e *software* adquiridos pela Marinha; - Restrições de financiamento; - Capacidade existente insuficiente para requisitos *Big Data;* - Problema de escalabilidade na integração de novas fontes; - Requisitos para o projeto APEC-SIFICAP; - Implementação de *dashboards* com recurso a	- *Hardware* e s*oftware* adquiridos pelo Exército mediante especificações da DCSI; - Capacidade em crescimento tomando em consideração *Big Data*, apesar de não existirem ainda requisitos específicos; - Financiamento LPM e Orçamento do Exército.	- *Hardware* com contrato de manutenção robusto, permite assegurar a atualização permanente do *software* e a continuidade em caso de falha de algum componente do sistema; - Capacidade insuficiente para exploração de fontes de dados; - Requisitos para o projeto PS3;

	SGMDN	EMGFA	Marinha	Exército	Força Aérea
	- Financiamento do Orçamento de Estado e projetos SAMA (fundos europeus).	*Data*; - Não existem requisitos explícitos para *Big Data* – indícios referentes à exploração de sensores.	ferramentas BI para apoio a todas as áreas funcionais; - Financiamento para investimento - LPM e Orçamento de Estado - Marinha.		- Financiamento com verbas LPM e Orçamento da FA.
L	- Secretário-Geral Adjunto SGMDN – coordenação das TIC; - Promovida a modernização da gestão de forma transversal à DN, através da coordenação de projetos SIMPLEX e SAMA.	- Infraestruturas e organização de dados implementadas de acordo com orientações superiores.	- Intenções das chefias plasmadas nas diretivas setoriais.	- Superioridade da Informação – desígnio da chefia do Exército.	- Perceção da importância dos sistemas e alinhamento por parte das Chefias.
P	- Área de Gestão da Informação suprida; apoio de RH do parceiro tecnológico do CDD; - Necessário reforço com especialistas para os projetos SAMA; - Falta de pessoal TIC em quantidade e devidamente qualificado no CDD - transversal às FFAA e à AP; - Militares do CDD são providos pelos Ramos (limitações) e elementos civis da AP; - A falta de RH poderá obrigar à externalização de alguns serviços, a fim de garantir a qualidade de serviço necessária.	- RH insuficientes em quantidade e competências mínimas essenciais; - Períodos de retenção em funções incompatíveis com os ciclos de formação e treino; - Externalização de serviços especializados de forma a garantir a eficácia da exploração e sustentação da capacidade existente.	- Lotação da DITIC com preenchimento de 66%; - Grande atratividade por parte do mercado de trabalho civil; - Sustentação das capacidades atuais problemática.	- RH transversais à área TIC, internos, com suporte do gestor de informação; - Recurso a elementos externos quando excedida capacidade interna e na implementação dos CD principal e alternativo. - Falta de alinhamento com regras de colocação e progressão na carreira; - Capacidade desajustada.	- RH internos afetos à implementação, sustentação e operação do sistema; - Constrangimentos associados à necessidade de pessoal qualificado, à condição militar e à rotação nas funções.

	SGMDN	EMGFA	Marinha	Exército	Força Aérea
I	- CDD.	CD EMGFA.	- CD principal – Alfeite; - Capacidade alternativa – DITIC.	- CD principal – DCSI; - CD alternativo – Santa Margarida (em implementação); - Dados em servidores locais (em migração) com *backup* nos CD centrais.	- CD principal; - Redundância no CD alternativo (fase inicial de implementação) e nas unidades da FA identificadas para o efeito.
I	- Nos SI de gestão a interoperabilidade é garantida pelo facto de o SIGDN ser sistema único e transversal; - Desenvolvimento de *webservices* à medida *on-demand*; - Diversos projetos futuros para interoperabilidade de Dados e Serviços; - Limitações no processamento de informação classificada.	- Troca de informação entre entidades através da utilização partilhada de SI comuns.	- Estabelecidas relações de confiança com os restantes domínios da DN.	- Redes de comunicações MDN-EMGFA-Ramos interoperáveis; - Troca de dados limitada (SIGDN, informação operacional para C2 de forças em missão).	- Utilização, no âmbito do projeto SIGDN e do SIAMFA, entre outros, os recursos do CDD. - Ligação aos outros Ramos, EMGFA e SGMDN, com partilha de informação limitada.

Legenda: D-Doutrina; O-Organização; T-Treino; M-Material; L-Liderança; P-Pessoal; I-Infraestruturas; I-Interoperabilidade.

Fonte: Construído a partir de L.F. Camelo (*op. cit.*), de R.A. Francisco (*op. cit.*), de T.D. Lopes (*op. cit.*), de J.A. Rocha (*op. cit.*) e de J.P. Roque (*op. cit.*).

Apêndice I — Análise comparativa de entidades congéneres

	NATO	EUA	França
D	- *NATO Cloud Computing Policy;* - *NATO Cloud Computing Directive;* - *Supporting document for the protection of NATO information within public cloud-based Communication and Information Systems (CIS);* - *Cloud Security Technical Directive* (em desenvolvimento).	- *DOD Cloud Strategy;* - *DoD Digital Modernization Strategy;* - *DoD Data Strategy.*	- *Ambition Numérique du Ministère des Armées;* - *Schéma directeur de la transformation numérique* ; - Estratégia do Estado para a *cloud;* - *La Transformation numérique du ministère des Armées – concepts clés.*
O	- Modelo de governação definido no *Cloud Operating Mode*l, composto por indivíduos com responsabilidades diversas nas entidades da *NATO Enterprise.*	- CIO da Defesa responsável pela: implementação do ecossistema *cloud*, emissão de linhas orientadoras em termos de segurança e criação de uma estrutura organizacional e fóruns de governação dedicados.	- DIRISI. Entidade responsável pelos dados e aplicações do ministério e pelas iniciativas da transformação digital; - DGNUM. Entidade responsável pela condução do processo de transformação digital; - CIO da Defesa, diretor da DGNUM.
T	- Previsto treino em ferramentas tecnológicas e de administração de serviços *cloud computing.*	- Necessidade de adquirir *know-how* interno para a edificação da capacidade (p.ex., com inclusão de cláusulas de assistência e treino especializado nos contratos com os prestadores de serviços).	- Lançado projeto Academia Digital (*Académie du Numérique*) - formação de civis e militares na área de SIC; - Abrange diversas áreas (desenvolvimento de sistemas, IA, ciber, redes e sistemas de comunicações).
M	- Redução do investimento e sustentação em *hardware* e *software*; - Direcionamento de recursos para serviços e sistemas operacionais; - Implementação de mecanismos de controlo de segurança na adoção de *clouds* públicas.	- Foco dos recursos na vertente operacional; - Criação de uma arquitetura de cibersegurança *cloud* - manutenção de um ambiente "*evergreen*"; - Responsabilidades de segurança partilhadas entre o CSP e o dono do sistema, de acordo com as responsabilidades estabelecidas pelo CIO do DoD.	- Foco dos recursos na vertente operacional, transição de serviços administrativos para a rede do Estado; - Plataforma POCEAD para armazenamento e tratamento de dados de acordo com técnicas de IA e *machine learning*; - Plataforma *Big Data* (projeto ARTEMIS), que permitirá o armazenamento e processamento massivo de dados.
L	- "*Cloud First*" *approach* para a *NATO Enterprise;* -Supervisão do C3B.	- *"Cloud First"* para as entidades integrantes do DoD; - Coordenação do CIO do DoD.	- DGNUM depende diretamente do Ministro e coordena com outras entidades, nomeadamente o CEMGFA e a Agência para a Inovação da Defesa; - Criação da marca *Défense Connect.*

P	- Criação de novas posições para gestão de serviços *cloud* (independentemente do modelo de implementação).	- Necessidade de desenvolver capacidades orgânicas nos elementos do DoD para a transição, desenvolvimento e exploração de serviços *cloud*.	- Necessidade de RH para o processo de transformação digital, previsto aumento de necessidade de civis e militares na área CSI até 2025. - Reforma na carreira das TIC (pessoal civil e militar), nomeadamente: Recrutamento e retenção; Aculturação e formação CIS; Treino totalmente digital para todos os indivíduos.
I	- Infraestruturas distintas mediante classificação de segurança da informação: . Até NATO RESTRICTED: *cloud* pública, privada ou híbrida; . A partir de NATO CONFIDENTIAL: *cloud* privada. - *Clouds* privadas - Infraestruturas *core* NATO renovadas: 2+1 CD; - *Clouds* públicas - CD localizados em nações NATO, de acordo com legislação e regulamentação local relativa a privacidade de dados (segurança), no cumprimento de políticas e diretivas de segurança da Aliança para CSI; - Estabelecimento de mecanismos de controlo de segurança a verificar na adoção de *clouds* públicas; - Requisitos de segurança para NATO RESTRICTED em *cloud* pública ainda em estudo; - *Infrastructure as a shared commodity that is accessed as a service*.	- Estratégia *multi-cloud*, *multi-vendor*; - *Enterprise Cloud: General Purpose cloud + Fit for Purpose clouds*; - Utilização das *características multi-region* e *multi-availability* zone dos prestadores de serviços; - Racionalização e redução do número de CD *on premise*; - Criação de uma arquitetura de cibersegurança *cloud* - manutenção de um ambiente "*evergreen*"; - Responsabilidades de segurança partilhadas entre o CSP e o dono do sistema, de acordo com as responsabilidades estabelecidas pelo CIO do DoD.	- Implementação de 4 CD na zona metropolitana para suportar a denominada *Cloud Défense;* - *Cloud* interna – Dados do Ministério, *on-premises*; - *Cloud* dedicada - Instalações de parceiros de confiança, garantindo os requisitos de autonomia e soberania, hospedando a maioria dos sistemas do Ministério; - *Cloud* externa – prestadores de serviços públicos.
I	- Modelo aplicável à NATO *Enterprise;* - Aliança encoraja as nações Aliadas a adotar o modelo de transição para a arquitetura *cloud* proposto; - Desenvolvimento de serviços *cloud* de acordo com *standards* NATO e *standards* abertos.	- Preconizada interoperabilidade entre os ambientes *General Purpose* e as diferentes implementações *Fit for Purpose;* - Utilização de *standards* de dados para catalogar, processar, aceder e armazenar dados.	- Preconizadas sinergias e articulação entre os diversos níveis concêntricos da cloud híbrida; - Ao nível dos dados, subjacente aos projetos POCEAD e ARTEMIS.

Legenda: D-Doutrina; O-Organização; T-Treino; M-Material; L-Liderança; P-Pessoal; I-Infraestruturas; I-Interoperabilidade.

Fonte: Construído a partir de DINSIC (2018), de *Global Newswire* (2019), de Minarm (2017a, 2017b, 2018, 2020), da NATO (2016, 2019a, 2019c, 2020), da NCIA (2017, 2019) e do USDoD (2018, 2019, 2020).