INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE ESTADO-MAIOR CONJUNTO

2013-2014

TII

UTILIZAÇÃO DE EQUIPAMENTOS INFORMÁTICOS PARTICULARES NAS REDES CORPORATIVAS NAS FORÇAS ARMADAS

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

UTILIZAÇÃO DE EQUIPAMENTOS INFORMÁTICOS PARTICULARES NAS REDES CORPORATIVAS NAS FORÇAS ARMADAS

MAJ INF Hugo Miguel da Silva Rodrigues

Trabalho de Investigação Individual do CEMC 2013/2014

Pedrouços 2014

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

UTILIZAÇÃO DE EQUIPAMENTOS PARTICULARES NAS REDES CORPORATIVAS NAS FORÇAS ARMADAS

MAJ INF Hugo Miguel da Silva Rodrigues

Trabalho de Investigação Individual do CEMC 2013/2014

Orientador: MAj ADMIL Carlos Alberto Pires Ferreira

Pedrouços 2014

Agradecimentos

Ao Instituto de Estudos Superiores Militares pela excelente colaboração e permanente predisposição face às solicitações exigidas na realização deste trabalho.

Ao Tenente-Coronel Barros, expresso o meu sincero e leal agradecimento, pela disponibilidade, elevado profissionalismo e extraordinária partilha de conhecimento, originando uma dinâmica alicerçada de ideias valiosas.

Ao Tenente-Coronel Nunes agradeço o seu enriquecedor contributo, pelos criteriosos pareceres e inegáveis conhecimentos na área, contribuindo para o enriquecimento do conteúdo do mesmo.

Ao Major Ferreira pela profissional e gratificante orientação em todo o processo de elaboração do trabalho, ultrapassando as barreiras geográficas que se nos depararam mas nunca em circunstância alguma se tornaram um obstáculo.

Ao Major Vinagreiro pela permanente disponibilidade e assertividade nos seus comentários e inegáveis conhecimentos técnicos na área, por demais enriquecedores em todo o processo de elaboração do trabalho.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

Atualmente, numa sociedade de informação, o indivíduo refugia-se cada vez mais em equipamentos tecnológicos que o auxiliam nas suas tarefas diárias. A utilização destes equipamentos tornou-se comum, acompanhando o indivíduo para qualquer local.

As empresas começam a apostar cada vez mais na utilização de equipamentos informáticos particulares no local de trabalho, facilitando e maximizando os recursos disponíveis de forma a alcançar os objetivos da organização. Existe assim uma tendência da qual as organizações militares não se podem dissociar- a tendência do *Bring Your Own Device*.

O tema central abordado neste trabalho foi a aplicação do conceito *Bring Your Own Device* nas redes das Forças Armadas (FA), permitindo a maximização de recursos e uma maior flexibilidade essencial na prossecução dos objetivos das organizações militares.

O modelo de análise aplicado foi o método hipotético-dedutivo, assentando num percurso metodológico baseado em fontes e numa pesquisa bibliográfica e documental, salientando-se a importância dos manuais doutrinários específicos de cada ramo das Forças Armadas.

Concretizaram-se na feitura do trabalho considerações finais, desafios futuros face a uma implementação do conceito *BYOD* nas redes corporativas das Forças Armadas, tendo sido elencadas possíveis propostas a considerar, concluindo-se que a implementação do conceito *Bring Your Own Device* está dependente da resolução de diversas variáveis, nomeadamente a variável da segurança.

Abstract

Nowadays, in the information society, the individual takes refuge in increasingly technological equipment to assist him in his daily tasks. The use of these devices have become commonplace, accompanying people to every location.

Companies are increasingly beginning to focus on the use of private computer equipment in the workplace, facilitating and maximizing available resources to achieve the organization's goals. The military organization is therefore before a tendency that cannot dissociate itself from the Bring Your Own Device trend.

The central issue addressed in this investigation is the application of the Bring Your Own Device concept to the Armed Forces (AF) networks, allowing maximization of resources and greater flexibility essential in achieving the military organizations goals.

The analysis model applied was the hypothetical- deductive method, relying on a methodological approach based on sources and a bibliographical and documentary research, emphasizing the different doctrinal manuals of each specific military service.

This work concludes that Bring Your Own Device concept implementation in the corporate networks of the Armed Forces faces considerable challenges. This concept implementation depends on setting of several issues, specially the security component.

Palavras-chave

Bring Your Own Device, *Digital Citizenship*, *Mobile Security*, Redes.

Lista de Abreviaturas

BYOC	*Bring Your Own Cloud*
BYOD	*Bring Your Own Device*
C2	Comando e Controlo
COMPUSEC	Segurança dos Computadores/Informática
COMSEC	Segurança das Comunicações
CSI	Comunicações e Sistemas de Informação
DCGS-A	*Distributed Common Ground System-Army*
DLA	*Defense Logistics Agency*
DOS	*Denial of Service*
EMFA	Estado-Maior da Força Aérea
EMGFA	Estado-Maior-General das Forças Armadas
EUA	Estados Unidos da América
FA	Forças Armadas
FAP	Força Aérea Portuguesa
GI	Gestão de Informação
Hip	Hipótese
IESM	Instituto de Estudos Superiores Militares
INFOSEC	Segurança de Sistemas de Informação e Comunicação
MMHS	*Military Message Handling System*
OBJ	Objetivo específico
PA	Pontos de Acesso
PD	Pergunta derivada
PDA	*Personal Digital Assistant*

PDSIFA	Plano Diretor de Sistemas de Informação da Força Aérea
PP	Pegunta de partida
RFCM	Rede Fixa de Comunicações Militares
SAD	Sistemas de Apoio à Decisão
SC	Sistemas Comunicação
SCom	Subsistema de Comunicações
SG	Subsistema de Gestão
SI	Sistemas de Informação
SIC	Sistemas de Informação e Comunicação
SICA	Sistemas de Informação e Comunicação Automatizados
SICAM	Sistemas de Informação e Comunicação Automatizados da Marinha
SICCE	Sistema Integrado de Comando e Controlo do Exército
SIC-OP	Sistema de Informação e Comunicações Operacional
SIC-T	Sistema de Informação e Comunicações Tático
SSegI	Subsistema de Segurança da Informação
SSI	Subsistema de Informação
TIC	Tecnologias de Informação e de Comunicação
TII	Trabalho de Investigação Individual
RDE	Rede de Dados do Exército

Introdução

"Redes, sistemas e serviços de informação assumem um papel vital na sociedade"
(*European Commission*, 2013, p. 11)

a. Introdução ao tema e definição do contexto de investigação

O tema abordado neste trabalho denominado de "Utilização de equipamentos informáticos particulares nas redes corporativas nas Forças Armadas" constitui-se como um assunto atual, cada vez mais presente na exploração de sistemas informáticos e tecnologias de informação[1]. Este tema está inerentemente associado ao conceito *Bring Your Own Device* (*BYOD*) e a todas as vicissitudes que daí advêm.

Antigamente era usual as empresas de tecnologias de informação providenciarem todo o equipamento considerado necessário, aquando a nova entrada de qualquer funcionário para o interior da organização empresarial. Estas ferramentas identificadas e aprovadas, com programas específicos empresariais, materializavam-se em computadores, fossem eles de secretária ou portáteis.

Com a massificação da adoção das tecnologias de informação por parte da população em geral, a adoção e implementação do conceito *BYOD*, aliado a uma exponencial venda de equipamentos informáticos particulares, tornou-se uma inevitável tendência emergente (WatchGuard, 2013, p. 2).

A crescente venda de equipamentos informáticos causou uma mudança na média de números de dispositivos por indivíduo e, logicamente, impulsionou o conceito de *BYOD*. Nos tempos atuais, um indivíduo detém na sua posse três dispositivos móveis, sejam estes computadores ou simples equipamentos portáteis de entretenimento, contribuindo para que o *BYOD* seja um fenómeno de âmbito global, com tendência a aumentar, sendo a maximização de produtividade, um dos seus maiores atrativos, entre outros (Canal Tech Corporate, 2013).

[1] "Conjunto de ciências aplicadas que lidam com operações sobre dados e informação (teoria da informação, operações aritméticas e lógicas, organização, representação, transferência, troca e processamento de dados, operação, tecnologia relativa a equipamentos, desenvolvimento e sustentação de sistemas, segurança, interoperabilidade, *office automation*, inteligência artificial, multimédia e hipermédia) " [ISO/IEC 2382-01: 1993]

Este trabalho pretende dar contributos para a pertinência da adoção do conceito *Bring Your Own Device* nas redes corporativas das Forças Armadas (FA) e identificar as suas vantagens e possíveis restrições na inclusão deste conceito.

b. Justificação do estudo

A utilidade e a versatilidade da adoção do conceito de *BYOD* e consequente implementação deste, dissimulam em certa medida algumas das preocupações sobre os riscos implícitos para as redes corporativas, ao facultarem o acesso de equipamentos informáticos particulares a sistemas detentores de informações classificadas.

A implementação e supervisão de contra medidas de segurança em diversos equipamentos, os múltiplos utilizadores e diferentes plataformas, reveste-se como um exercício de extrema dificuldade, na sua abrangência, seja esta ao nível humano, físico e organizacional. As organizações necessitam de adotar uma política de implementação ativa de forma a habilitar estas com ferramentas capazes de mitigar possíveis ameaças.

As organizações militares estão despertas e sensibilizadas para a implementação do conceito *BYOD* nas suas redes corporativas. Exemplo desta sensibilização e preocupação é o caso do Exército dos Estados Unidos da América (EUA), onde as redes informáticas estão-se a transformar à mesma velocidade que o Exército vai evoluindo de forma a ficar mais ligeiro, cada vez mais móvel, com caraterísticas modulares e com imediata capacidade de resposta estratégica (US Army, 2009, p. 99). O caso do Corpo de Fuzileiros Navais (*Marines Corps)* acompanha esta tendência e é analisado neste trabalho, devido à sua pertinência, atualidade e contribuição para melhor compreensão da problemática analisada.

c. Objeto de estudo e sua delimitação

O objeto de estudo deste Trabalho de Investigação Individual (TII) centra-se no conceito *BYOD* e sua implementação em redes corporativas de uma organização, tendo sido delimitada a investigação às redes dos diferentes ramos das Forças Armadas Portuguesas e Estado-Maior-General das Forças Armadas (EMGFA) em tempo de paz, contendo estas redes corporativas, informação classificada e informação não classificada.

d. Objetivos da investigação

O objetivo geral deste trabalho é identificar quais as possibilidades existentes nas Forças Armadas para a implementação do conceito *Bring Your Own Device.*

Deste objetivo geral decorrem os seguintes objetivos específicos: **(OBJ1)** Verificar quais os equipamentos informáticos particulares que se integram no conceito *Bring Your*

Own Device, na ligação às redes corporativas das FA **(OBJ2)** Quais as atuais limitações que as redes corporativas classificadas das FA têm na adoção e implementação do conceito *Bring Your Own Device*, **(OBJ3)** Identificar as características das redes corporativas não classificadas das FA, na implementação do conceito *Bring Your Own Device*, **(OBJ4)** Verificar quais as ameaças à segurança militar, na ligação de dispositivos às redes corporativas das FA, aplicáveis ao conceito *Bring Your Own Device*.

e. Procedimento metodológico

Na fase inicial da investigação e considerando o atrás apresentado, designadamente no que à limitação do tema diz respeito, foi definida a pergunta de partida (PP) que orientou o desenvolvimento do presente trabalho e permitiu ser o fio condutor de toda a estrutura deste. Assim, a PP definida foi:

PP – "Que possibilidades as redes corporativas das Forças Armadas oferecem na implementação do conceito *Bring Your Own Device*?"

No sentido de operacionalizar a execução do trabalho e mais facilmente inferir a resposta à PP, identificámos as seguintes hipóteses (Hip) de resposta, às perguntas derivadas (PD) elencadas:

PD 1 – "Quais os equipamentos informáticos particulares que se integram no conceito *Bring Your Own Device*, na ligação às redes corporativas das Forças Armadas?"

Hip 1 – Os equipamentos informáticos particulares que integram o conceito *Bring Your Own Device*, na ligação às redes corporativas das Forças Armadas, são portáteis e seguros.

PD 2 – "Quais as atuais limitações que as redes corporativas classificadas das Forças Armadas têm na adoção e implementação do conceito *Bring Your Own Device*?"

Hip 2 – As atuais redes corporativas classificadas das Forças Armadas não permitem a aplicação do conceito *Bring Your Own Device*.

PD 3 – "Quais as características das redes corporativas não classificadas das Forças Armadas, na implementação do conceito *Bring Your Own Device?*"

Hip 3 – As redes corporativas não classificadas das Forças Armadas, na adoção do conceito *Bring Your Own Device*, são interoperáveis, seguras e flexíveis.

PD 4 – "Quais as ameaças à segurança militar, na ligação de dispositivos às redes corporativas das Forças Armadas, aplicáveis ao conceito *Bring Your Own Device?*"

Hip 4 – As contra medidas, face à exploração das vulnerabilidades pelas ameaças existentes, conseguem ser mitigadas, na adoção do conceito *Bring Your Own Device*, nas redes corporativas das Forças Armadas.

Para a condução desta investigação será utilizado o procedimento metodológico definido por Raymond Quivy e Luc Van Campenhoudt (2008) conforme previsto na NEP/ACA-010[2] do Instituto de Estudos Superiores Militares (IESM). As três fases[3] previstas neste procedimento (a rutura, a construção e a verificação) não são independentes nem estanques ao longo de toda a análise contemplada no trabalho.

No Apêndice 1 a este trabalho encontra-se a versão do processo metodológico aplicado e quais os diversos procedimentos que ocorreram na sua elaboração. No Apêndice 2 encontram-se definidos os conceitos, dimensões, indicadores e instrumentos de observação que permitiram validar ao longo do trabalho os objetivos previamente identificados e anteriormente referenciados. Estes instrumentos de observação foram abordados na forma de observação direta, procedendo diretamente à recolha da informação e incidindo sobre os indicadores identificados.

f. Estrutura do estudo

Na primeira fase da investigação, foi identificado o conceito de *BYOD*, sua definição e aplicabilidade atual, tendo sido analisados casos de implementação do conceito em instituições académicas de relevo. Foram analisados os domínios operacionais das redes corporativas das FA, seguindo-se a identificação das características e requisitos operacionais necessárias à implementação do conceito *BYOD,* e ainda analisadas segundo o conteúdo da classificação de segurança da informação.

Abordámos o conceito *BYOD* de forma a edificar os requisitos necessários para que um equipamento informático individual possa ser aplicado neste conceito, quais as suas propriedades e inerentes caraterísticas.

Após a caraterização dos domínios operacionais nos diversos ramos das FA, identificados que estão os requisitos necessários e as características que deverão existir nos equipamentos informáticos particulares para a sua interação com as redes corporativas, transversais aos diversos ramos das FA, analisámos as vulnerabilidades e as ameaças à segurança da informação e das organizações, aos níveis dos equipamentos e das redes.

Após a conclusão das diferentes fases, abordamos o caso de estudo da *Huawei Technologies co., LTD,* tendo este sido um caso de sucesso e de referência da implementação do conceito *BYOD* numa organização empresarial. Apresentaram-se contributos para o conhecimento e foram identificadas algumas considerações de ordem

[2] NEP/ACA-010 Trabalhos de Investigação, de 18Fev13.

[3] Identificadas na publicação em questão por "atos".

prática de possível adoção da aplicação do *BYOD* nas redes corporativas das FA.

Na conclusão do trabalho procurou-se fazer uma retrospetiva dos fatores tomados como essenciais de todo o procedimento, as vantagens e restrições existentes na implementação do conceito *BYOD* nas redes corporativas das FA.

De forma a caracterizar os equipamentos informáticos particulares, redes corporativas das FA e ameaças internas e externas (passos da metodologia apresentada no Apêndice 1 – Processo metodológico), este trabalho aplicou um modelo de investigação, tendo por base conceitos, dimensões e indicadores (Quivy & Campenhoudt, 2008). A obtenção de dados foi feita recorrendo a oferta bibliográfica nacional e estrangeira sobre o tema, documentos doutrinários nacionais, estrangeiros e documentos estruturantes de conceitos abordados pelo assunto em análise e apoiada pelos instrumentos de observação reconhecidos no Apêndice 2 – Modelo concetual da investigação.

Esta análise incidindo nesta variedade documental, materializou-se na frequência do aparecimento de certas caraterísticas de conteúdo ou ausência destas, constituindo-se como as duas categorias da análise de conteúdo: os métodos quantitativos e os métodos qualitativos. O modelo de análise seguido, ilustrando todas as fases anteriormente descritas, resume-se no Apêndice 3 – Modelo de Análise.

1. O Conceito *Bring Your Own Device* e o seu impacto global

"Uma nova tendência ganha preponderância em muitas empresas, o conceito de *Bring Your Own Device (BYOD) ".*

Dean Wiech, *Managing Director* na Tools4ever, 2014

O conceito *BYOD* define-se como sendo a possibilidade dos colaboradores de uma determinada organização levarem consigo, para os locais de trabalho, os seus equipamentos informáticos particulares[4], fazendo uso dos mesmos no acesso à informação digital da organização, como por exemplo *mails*, ficheiros e bases de dados, acedendo desta maneira aos recursos das redes corporativas das organizações (Hayes & Kotwica, 2013). Este conceito também aparece em diversos documentos como o fenómeno dos funcionários e *outsiders* trazerem equipamentos informáticos e ligarem-se às redes corporativas de uma organização (WatchGuard, 2013, p. 2).

Repentinamente, as organizações, maioritariamente empresariais, vêem-se confrontadas com um ambiente de trabalho, onde os funcionários trazem os seus telemóveis pessoais, equipamentos capazes de registar dados e conversações, recolher e armazenar fotografias ou outra qualquer informação interna, sensível e privada, para o seu interior. Através destes equipamentos, esta informação interna, sensível e privada, é rapidamente partilhada fora das "fronteiras" das próprias organizações, perdendo desta forma o controlo na informação privada interna, sua gestão e uso da mesma. Adicionalmente, os funcionários tornam-se cada vez mais dependentes da utilização de redes sociais[5]. Estas são avaliadas como fator de distração, uma perda de tempo e de produtividade, assumindo-se como um obstáculo ao sucesso de uma qualquer organização.

A implementação do conceito *BYOD* numa organização revelou, que a eficiência e a produtividade nas organizações empresariais que apoiavam esta implementação aumentavam, permitindo aos funcionários partilhar e comunicar de uma forma extremamente flexível e pacífica, face à rigidez do controlo por parte das empresas. O trabalho deixa de ser um local para onde o funcionário simplesmente se dirige, e passa a ser um local onde o funcionário tem algo objetivo e concreto para realizar (WatchGuard, 2013).

[4] *Smartphones*, *tablets* e computadores portáteis (Hayes & Kotwica, 2013).

[5] "O Facebook, com mais de 900 milhões de usuários, é a rede social com mais acessos dos últimos tempos, passando facilmente outras redes que costumavam ser líderes – como o Orkut" (Tailândia, 2012).

A utilização destes equipamentos informáticos está cada vez mais presente nas organizações empresariais. As pessoas estão "*tecno-dependentes"* querendo universalizar o uso dos seus *gadgets* incluindo o uso nos locais de trabalho de forma a ajudar o desempenho das tarefas (Unit, 2013). De acordo com um inquérito de janeiro de 2013, a 316 executivos, pela *Economist Intelligence Unit* (Unit, 2013, p. 3), 62% das empresas em todo o mundo autorizam o uso de equipamentos informáticos particulares aos seus elementos.

Walczak (2013) afirma que metade dos empregadores solicitarão aos futuros empregados que possuam equipamentos informáticos móveis, tais como portáteis, *smartphones*, *tablets*, que os tragam para os locais de trabalho. Os trabalhadores poderão trabalhar em qualquer local, a qualquer momento, tendo inclusive o conceito *Cloud Computing Technology*[6] *(Cloud)* começado a assumir preponderância face ao conceito *BYOD*.

Contudo, apesar da liberalização do pensamento referente ao uso de equipamentos particulares no acesso à informação da empresa, questões relativas à segurança da informação e consequências organizacionais são uma preocupação constante nos cargos de chefia. Uma pesquisa global revelou o aumento desmesurado de funcionários que violam as políticas de uso e implementação das organizações que regem o uso de equipamentos informáticos particulares, de contas pessoais de armazenamento em *Cloud* e de novas tecnologias. Os funcionários declararam que violariam qualquer política em vigor que proibisse o uso de equipamentos informáticos particulares no local de trabalho ou para fins profissionais (Convergência Digital, 2013). Apesar desta liberalização e aceitação do uso de equipamentos informáticos particulares no seio das organizações, poucas adotam medidas e *software* de gestão para minimizar os riscos existentes (IT Web, 2014).

Em menos de dez anos, o consumismo de novas tecnologias levou, a que os elementos de direção das organizações se deparassem com novos desafios no âmbito da segurança da informação, controlo de produtividade e liberdade de ação (WatchGuard, 2013).

[6] O conceito *Cloud Computing Technology* baseia-se em tecnologias comprovadas, incluindo virtualização, arquiteturas orientadas para serviços, redes informáticas de banda larga, software como serviço, navegador como uma plataforma livre e software de código aberto (*freeware)*, sistemas autónomos, *frameworks* de aplicação na internet (Kizza, 2013, p. 465)

As particularidades de uma rede corporativa[7] informática conferem a esta vantagens na difusão de redes locais. As redes corporativas facultam melhores ambientes de trabalho, auxiliam e rentabilizam a repartição de recursos. No entanto, a difusão das redes locais têm desvantagens que deverão ser mitigadas de forma a garantir a integridade da informação, da organização e do indivíduo. Estas desvantagens passam pelo facto de toda a rede ficar vulnerável se algum dos seus componentes não conseguir garantir a segurança de todo o processo, exponenciando desta maneira possíveis ataques informáticos (MCS, 2006, p. 5).

A doutrina militar sobre Instruções de Segurança Militar do Exército Português, de 2013, neste caso específica de um ramo mas abrangente no seu conteúdo de forma transversal às FA, analisa os equipamentos informáticos particulares e define que "pela sua especificidade e a sua maior vulnerabilidade a comprometimentos deliberados ou acidentais, considera-se que estes requerem cuidados acrescidos, relativamente aos terminais fixos quanto às regras de segurança a observar". Aborda também as ameaças a que estes equipamentos estão sujeitos, as suas vulnerabilidades e o tipo de informação que deverá ser contida neles, definindo por sua vez que estes dispositivos estão sujeitos a uma maior gama de ameaças, do que os instalados de forma permanente numa determinada área de segurança, (…) e que, pela sua natureza, colocam constrangimentos tanto a nível do plano da segurança física como da segurança do pessoal e de procedimentos. Em particular, o seu tamanho reduzido e a sua portabilidade torna-os mais suscetíveis à perda acidental ou roubo, se comparados com os computadores não-portáteis" (Exército Português, 2013, p. 85).

Corremos o risco de expor o acesso de informação sensível a pessoas sem autorização para tal. As nossas informações percorrem as redes informáticas onde estamos inseridos, usando todo o tipo de dispositivos com acesso à internet. Materializa-se assim num problema ainda mais desafiante, quando os funcionários se deslocam de um local para outro a trabalhar, independentemente de onde organizacionalmente pertencem, através dos seus equipamentos informáticos particulares.

A crescente mobilidade dos trabalhadores e do crescimento do uso de equipamentos informáticos particulares correspondente a um crescimento de aplicações de armazenamento de informação retrata-se numa possível lacuna na segurança do sistema (Nunoo, 2013, p. 1).

[7] Definida em Cap.2 – O Conceito *Bring Your Own Device* e o seu impacto global.

Assim, o conceito *BYOD* é também abordado como *"bring your own danger, disaster, detonator!"* (Silva, 2013). A informação pessoal é armazenada no mesmo local que a informação da organização, existindo a possibilidade de ameaças à segurança da informação (Anon., 2012).

Atualmente, as restrições orçamentais condicionam a organização militar a um equilíbrio entre a responsabilidade fiscal e o cumprimento da missão. De forma a alinhar com as estratégias e iniciativas do Departamento de Defesa dos EUA e de acordo com a Estratégia do Corpo de Fuzileiros Navais, começou a existir uma consolidação de informação e acertada uma estratégia informacional na doutrina militar (Marine Corps, 2013, p. 3). Com o aumento da capacidade de dispositivos móveis, o Corpo de Fuzileiros Navais reconheceu a tendência de evolução das necessidades de informação dentro da organização e ambiente operacional e da necessidade de responder atempadamente a essas necessidades.

A exigência do utilizador para aceder e partilhar informação a partir de qualquer local permitirá o cumprimento mais eficiente da missão. A capacidade de aceder, partilhar e manipular dados e informação desses locais irá permitir liberdade adicional de movimento através de um ambiente de informação em expansão. Através desta estratégia, o Corpo de Fuzileiros Navais identificou requisitos de capacidade do dispositivo móvel, otimizou os recursos existentes para certificar equipamentos informáticos particulares e capacidades de equipamentos informáticos com informação classificada (Marine Corps, 2013, p. 3).

Também desta forma aberta às novas tecnologias, a *Defense Logistics Agency* (DLA)[8] em conjunto com o Departamento de Defesa dos EUA adotou um programa de implementação de uso de equipamentos particulares de forma a reduzir custos e a contribuir significativamente para o processo de liderança nas organizações (Citrix, 2013, p. 2).

A implementação do conceito *BYOD*, virtualizando a funcionalidade crítica, e padronizando as infraestruturas da tecnologia de informação residente, permitiu à DLA a portabilidade e flexibilidade de trabalho, exigida a uma organização moderna. Como resultado, foram evitadas despesas com novos equipamentos, reduzidos os custos de licenciamento de novas aplicações, consequentemente foi notório um aumento na

[8] A *Defense Logistics Agency* providencia um largo espectro logístico e serviços técnicos para Exército dos EUA, Marinha, Força Aérea e outros órgãos militares.

segurança, refletindo-se na motivação do utilizador, capital humano essencial para a prossecução dos objetivos organizacionais. Em 23 de maio de 2012, Steven VanRoekel, chefiando o *Digital Services Advisory Group and Federal Chief Information Officers Council*, ao analisar estudos de caso de implementação do conceito *BYOD*, de forma a desenvolver uma estratégia governamental, define o *BYOD* como "um conceito que permite os funcionários utilizarem os seus dispositivos particulares tecnológicos, por forma a ficarem ligados a algo, a acederem a informação ou completar tarefas para as suas organizações. No limiar, o programa *BYOD* permite aos utilizadores acederem a servidores e serviços exclusivos dos funcionários e/ou informação nos seus equipamentos informáticos particulares (*tablets/eReaders*, *smartphones* e outros dispositivos).Estes equipamentos podem incluir computadores *laptop/desktop*" (Digital Services Advisory Group and Federal Chief Information Officers Council, 2012).

O conceito *BYOD* é de emprego universal, com crescente aplicação, especialmente no setor empresarial. Relatórios[9] indicam que as empresas estão progressivamente a consentir que os seus funcionários tragam para os locais de trabalho os seus equipamentos informáticos particulares (Vmware, 2013, p. 3).

Esta aplicação do conceito *BYOD* é de simples perceção, visto que os equipamentos informáticos particulares oferecem uma enorme flexibilidade, associados a redução de custos para a organização que aprova a sua implementação. Hoje em dia, todos os equipamentos informáticos são particulares, sejam eles do próprio funcionário ou da organização, visto que a sua portabilidade confere-lhe uma plenitude de utilização, que se materializa no seu uso na organização, no deslocamento para casa e no interior de qualquer instalação (LetMobile, 2012, p. 7).

O conceito *BYOD* implica que os funcionários utilizam os seus *tablets* e *smartphones* diariamente nos seus locais de trabalho (Taurion, s.d.). Esta aplicabilidade de equipamentos pessoais comporta alguns fatores suscetíveis de análise pela organização: perda de produtividade por parte dos funcionários, iludindo-os pelo simples facto que o uso de equipamentos pessoais lhes confere autonomia para liberdade de tarefas, fora do interesse empresarial; falta de controlo na informação empresarial, compatibilidades de *software* e *hardware* dos dispositivos particulares com os equipamentos da organização e essencialmente questões de segurança (Walczak, 2013), cuja temática será abordada no capítulo cinco deste trabalho, a segurança na adoção do conceito *BYOD*.

[9] Cisco, Computerworld, CompTIA e Mobilisafe.

A implementação deste conceito agrega alguns equívocos nas organizações e nos utilizadores. Alguns destes mitos[10] não correspondem à realidade e tendem a negativar a ideia do conceito. No entanto, a aplicação do *BYOD* congrega em si vantagens que não podem ser ignoradas: a gestão do moral dos funcionários e consequente implementação da cultura organizacional pretendida; a especialização tecnológica que é requerida aos funcionários e o inerente aumento de produtividade da organização, através dos seus funcionários (Walczak, 2013). Assim, e para o propósito do estudo deste trabalho, torna-se imperativo caraterizar concetualmente o *BYOD*, quais os equipamentos aplicados a este conceito e quais as suas características.

Foi no meio académico em simultâneo com o empresarial, que foram identificadas caraterísticas para um equipamento ser contemplado numa política de implementação do conceito *BYOD*. Em várias instituições académicas[11], foram definidos requisitos específicos que os equipamentos deveriam ter para serem considerados na aplicação do conceito *BYOD*. Estes requisitos eram divididos em seis caraterísticas: o visor, a conetividade, o processamento, portabilidade, segurança e autonomia.

Para um equipamento ter autorização para ser aplicado como *BYOD*, com base nas caraterísticas identificadas anteriormente, ele tem que ter um visor com um mínimo de dez polegadas de diagonal, equipado com interface IEEE 802.11[12] e antivírus, equipado com um processador Celeron[13]1.5Ghz ou superior, ser de fácil transporte e possuir no mínimo uma autonomia de cinco horas (Booker T. Washington High School, 2011, p. 3).

Num estudo realizado em 2012 pelo Governo do Estado de Alberta, no Canadá, intitulado *"Bring Your Own Device: A Guide for Schools"*, foi analisado o uso de equipamentos informáticos particulares nas escolas. Este estudo incidiu sobre potenciais

[10] A maioria das grandes empresas não estão a implementar o conceito *BYOD*. A marca *Apple* é a principal referência na implementação do conceito *BYOD*. Os equipamentos informáticos particulares adotados no conceito *BYOD* têm salvaguardas que eliminam as preocupações de segurança da organização e o *BYOD* pode ser evitado (Smith, 2012).

[11] Kellyville High School, Hillfield Strathallan College, St Bedes College (Os *smartphones* não se incluíam no conceito *BYOD* (St Bede´s College, 2014, p. 2) e Booker T. Washington High School.

[12] "IEEE 802.11 refere-se ao conjunto de regras que definem a comunicação por *wireless* LANs (*wireless local area networks, or WLANs*)" (Techopedia, 2014).

[13] "O processador Celeron é o processador de nível básico para tarefas de computação simples, como e-mail, Internet e criação de documentos" (Intel, s.d.).

vantagens e inconvenientes, bem como os riscos associados, e implicações que poderiam surgir no uso destes equipamentos (School Technology Branch, 2012).

Os equipamentos informáticos particulares, neste estudo, foram divididos em seis categorias: *Laptop*, podendo estes serem usados com ou sem internet; Notebook, equipamentos que maximizam o seu desempenho com uma ligação à internet; *Smartphones* (ex.Blackberry, Android, iPhone, iPod Touch); Tablets (ex., iPad, Android Tablet, etc.); leitores E-book (ex., Kindle, Kobo) e leitores de mp3 (ex. iPod, etc.) (School Technology Branch, 2012, p. 3). Estas categorias por sua vez, assentavam em quatro modelos de seleção que iriam definir quais os equipamentos a poderem ser utilizados pelos alunos, indo esta seleção do padrão (*standard)*, identificação de um único tipo de dispositivos que todos os estudantes deveriam adquirir, ao flexível, modelo aberto que incentivava os alunos a poderem levar consigo qualquer dispositivo para a escola (figura nº 1.- Modelos *BYOD* de seleção).

Padrão Flexibilidade

1	2	3	4
Limita um equipamento informático particular a um determinado modelo ou marca específica	Limita um equipamento informático particular a determinadas especificações técnicas	Limita um equipamento informático particular a determinadas capacidades específicas (ex. *software*, ferramentas, aplicações)	Não existem limitações na seleção dos equipamentos informáticos particulares

Figura nº 1 – Modelos *BYOD* de seleção
Fonte: (Autor, 2014) adaptado de (School Technology Branch, 2012, p. 11).

Em abril de 2013, o Corpo de *Marines* no seu manual "*Commercial Mobile Device Strategy"* define o que entende por dispositivo móvel, na implementação do conceito *Personally Owned Mobile Devices*, normalmente conhecido como *Bring Your Own Device*. Este conceito de dispositivo móvel é definido como "um equipamento informático portátil equipado com um monitor que permite a entrada de dados (ex. écran tátil, teclado), quando ligado a uma rede informática, permite a partilha de informação em formatos especialmente concebidos para maximizar o uso desta face às limitações existentes nos dispositivos (ex.: tamanho do écran, bateria do computador). Equipamentos informáticos particulares têm as mesmas caraterísticas de computadores convencionais, portáteis ou não, num conjunto com maior portabilidade. Exemplos de equipamentos informáticos

particulares incluem *smartphones* e *tablets"* (Marine Corps, 2013, p. 4). Estes equipamentos permitem aos utilizadores obter acesso a uma rede corporativa percorrendo no caso do Corpo de *Marines*, dois sistemas operacionais ao mesmo tempo, dando aos utilizadores o melhor dos serviços comerciais e empresariais.

Numa variação da abordagem do conceito tradicional do *BYOD*, no seio do Corpo de *Marines*, a implementação do conceito tem como objetivo permitir que os utilizadores tragam os seus próprios dispositivos aprovados, adquiridos pelo utilizador e aproveitando as plataformas de outras agências como a Agência de Sistemas de Informação da Defesa, com a finalidade última de redução de custos (Grim, 2013).

Os equipamentos informáticos particulares portáteis poderão ser definidos como dispositivos pequenos e leves o suficiente para serem transportados à mão por um indivíduo. Os computadores portáteis, PDAs[14], telemóveis e Tablet PCs são exemplos comuns de dispositivos portáteis (Nunoo, 2013, p. 1).

Neste trabalho, entendem-se como equipamentos informáticos particulares para serem aplicados no conceito *BYOD* em redes corporativas[15] (figura nº 2 – Modelo de uma rede corporativa), equipamentos que sejam pessoais (no seu transporte e utilização), de pequenas dimensões, seguros[16], com capacidade *Wi-fi*[17] (equipado com interface IEEE

[14] Assistente Pessoal Digital *(Personal Digital Assistant)*.

[15] Uma rede corporativa carateriza-se por ter segmentos de rede local com um *backbone*, tem mais que um protocolo de rede, ligações dial-up para utilizadores que se ligam de casa ou em viagem, ligações dedicadas ao trabalho e disponibiliza ligações à Internet (Technet Library, 2005). A implementação do conceito *BYOD* nas redes corporativas é analisada na vertente de uma rede de computadores (Rede de nós de processamento de dados interligados com vista à comunicação de dados (ADatP-2/ISO-18).

[16] Equipado com *software* (todo ou parte dos programas, procedimentos, regras e documentação associada a um sistema de processamento de informação [ISO/IEC 2382-01: 1993]) antivírus, *firewall* e Anti Spam (temática abordada neste trabalho no capítulo cinco- A segurança na adoção do conceito *BYOD*.

[17] Wi-Fi significa *Wireless Fidelity*. Equipamentos informáticos particulares podem ser equipados com adaptadores Wi-Fi. A maioria de equipamentos informáticos particulares atualmente é equipada com estes adaptadores. Os adaptadores captam os sinais emitidos por dispositivos denominados de pontos de acesso (PA), que por sua vez são normalmente ligados às redes corporativas coaxiais existentes, empregando várias normas técnicas diferentes e referenciadas como a especificação IEEE 802.11, a fim de se comunicar com um ponto de acesso padrão 802.11a/b/g/n. Desta forma, os dispositivos com capacidade Wi-Fi têm acesso aos mesmos recursos que os dispositivos ligados à rede por fios têm (*Ethernet)*. Embora seja menos usual, os dispositivos Wi-Fi também podem comunicar diretamente com outros (St Bede´s College, 2014, p. 47).

802.11), portáteis[18], que incluem computadores portáteis, *netbooks*, *tablets*, *iPad*, e-*Readers* e *smartphones*.

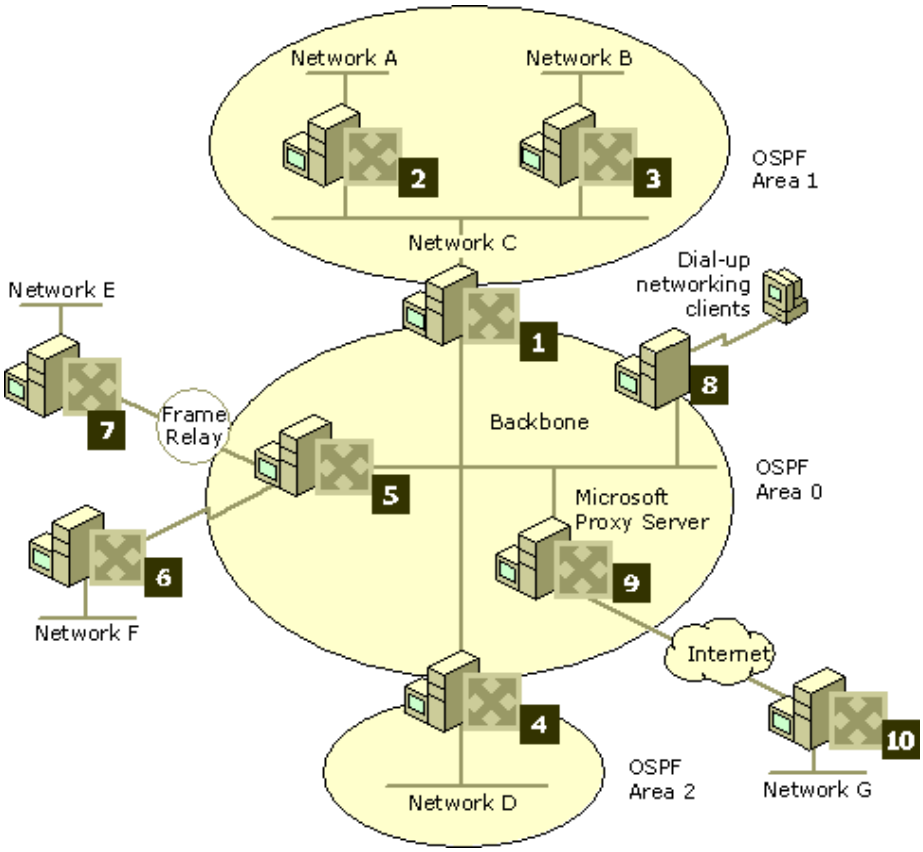


Figura nº 2 – Modelo de uma rede corporativa
Fonte: (Technet Library, 2005)

Face ao apresentado, identificadas as caraterísticas que o conceito de *BYOD* acarreta, no que diz respeito à portabilidade e no que diz respeito à segurança, referente à inclusão nos dispositivos particulares com aplicações, procedimentos e regras, considera-se validada a Hip 1 – Os equipamentos informáticos particulares que integram o conceito *Bring Your Own Device*, na ligação às redes corporativas das Forças Armadas, são portáteis e seguros.

Aquando a definição da base concetual em que o conceito *BYOD* assenta, vemos respondida a Pergunta Derivada 1 – Quais os equipamentos informáticos particulares que se integram no conceito *Bring Your Own Device*, na ligação às redes corporativas das Forças Armadas?

[18] 1. Que se pode transportar com facilidade. = portável, transportável; 2. Que se pode trazer no bolso; 3. Que se pode armar e desarmar; 4. Computador leve e de pequenas dimensões, dotado de bateria recarregável, que é de fácil transporte e que pode ser usado na posse de um utilizador (Priberam, 2013)

2. Os Domínios Operacionais das Redes Corporativas das Forças Armadas Portuguesas

"Com a internet, ser competitivo num mercado resume-se à comunicação de informação no ambiente informacional global. Não consiste simplesmente na proibição para aceder à informação de uma organização; consiste na gestão da troca dessa informação".

Jean-Philippe Jouas (Presidente da LUSIF), setembro 1998

Após a caraterização e definição de quais os equipamentos informáticos particulares a serem incluídos no conceito *BYOD*, torna-se pertinente identificar a possibilidade do conceito nas redes corporativas das Forças Armadas Portuguesas. Estas redes materializam, em cada um dos ramos, um sistema integrador de tecnologias de informação, em dois domínios que serão caraterizados: o domínio classificado e não classificado[19]. Esta caraterização da bipolaridade dos domínios nos diferentes ramos das FA identificará quais as limitações atuais que as redes corporativas classificadas das FA têm na adoção e implementação do conceito *BYOD*.

a. Estado-Maior-General das Forças Armadas

O Estado-Maior-General das Força Armadas (EMGFA), para cumprir as suas respetivas missões, auxilia-se através de variadas componentes. Estas, dividem-se em redes de dados com informação classificada, onde se incluem serviços de correio eletrónico, *chat*, serviço registado de mensagens, serviço de voz, videoconferência e portal de partilha de informação.

A rede de dados com informação não classificada engloba, à semelhança da rede de dados anteriormente escalpelizada, serviço de correio eletrónico, *chat*, intranet, internet, serviço de voz e videoconferência. O sistema de comunicações, no qual vai assentar na rede de dados classificada, alberga a rede fixa de comunicações militares (RFCM), apoiada por cabos de fibra ótica, feixes hertzianos e comunicações satélite, módulos de comunicações destacáveis, dispositivos móveis e sistemas cripto. Os restantes sistemas de informação, respetivamente para o comando e controlo das FA e de apoio à gestão destas,

[19] A diferença significativa entre estes domínios é a circulação de informação classificada ou não classificada nas redes informáticas.

suportam o Sistema Integrado de Comando e Controlo do Exército (SICCE), o *Military Message Handling System* (MMHS) e portal *Wise*.

O domínio do utilizador, englobado na rede de dados não classificados, reveste-se de caraterísticas que irão ser comuns e transversais aos diferentes ramos das FA e que se constituirá como objeto de estudo na rede corporativa do EMGFA, onde a análise de toda a exequibilidade de implementação do conceito *BYOD*, incidirá.

b. Marinha

As funções essenciais de comando e controlo "devem ser suportadas por Sistemas de Informação (SI) e Sistemas de Comunicação (SC) com adequada velocidade de transferência e processamento de informação, interoperáveis e de grande fiabilidade e sobrevivência" (Marinha, 2005, p. 17). Na Marinha, estes sistemas denominados de Sistemas de Informação e Comunicação Automatizados da Marinha (SICAM) são entendidos como "Sistema de Informação e Comunicação, constituído por um Sistema de Informação e Comunicação Automatizado (SICA) ou conjunto de SICA, que apoia, de forma direta ou indireta, o cumprimento da missão de uma das áreas funcionais da Marinha, ou de todas estas, de forma simultânea e equitativa (…) " (Marinha, 2005, p. 19).

Para a sustentabilidade da capacidade de comando e controlo, foram designados três pilares, no qual assenta a superioridade na utilização da informação. Esta superioridade assenta nos pilares: Infraestrutura tecnológica, Gestão da informação e Aptidões nas áreas da Gestão de Informação (GI) e das Tecnologias de Informação e de Comunicação (TIC).

Assim, englobando o primeiro pilar, temos a componente de comunicações constituída pelos Domínios de Rede[20] e Domínio do Utilizador[21]. A abordagem da aplicabilidade do *BYOD* focar-se-á nestes domínios, sabendo que incluirão, neste último domínio, todos "os meios existentes nas unidades e órgãos da Marinha que, diretamente explorados pelos utilizadores, sirvam para transferir, processar, armazenar e disponibilizar informação com os níveis de segurança adequados, designadamente: serviços que abrangem as funcionalidades associadas à transmissão em claro ou em modo seguro de voz

[20] "O Domínio de Rede compreende todos os suportes e recursos de comunicações de âmbito alargado mas controlados e geridos de um modo centralizado, que viabilizam a transferência da informação ou dados entre domínios do utilizador, assegurando funções de comutação, transmissão, armazenamento, processamento e segurança" (Marinha, 2012, p. 14).

[21] "Conjunto dos recursos de sistemas de comunicação e sistemas de informação que, sob controlo de cada utilizador, disponibilizam serviços como os de gestão e administração de cada utilizador, para além dos fornecidos a nível do domínio da rede" (Marinha, 2012, p. 14).

(e.g. telefonia, conferência de voz, correio de voz), dados (e.g. correio eletrónico, transferência de ficheiros, processamento de transações, transferência de dados interativa ou em bloco) e imagem (e.g. gráficos, fac-símile, vídeo e vídeo teleconferência) (Marinha, 2005, p. 31).

c. Exército

O Exército, como organização militar, conduz operações militares, através de forças operacionais e desenvolve diariamente atividades militares nas unidades territoriais. Quando estas forças operacionais são projetadas, são apoiadas em comunicações e sistemas de informação pelo Sistema de Informação e Comunicações Tático (SIC-T) que, paralelamente, garante a sua interligação com a sua estrutura territorial. Quando desenvolvem as suas atividades nas unidades, apoiam-se num conjunto diverso de tecnologias que constituem o Sistema de Informação e Comunicações Operacional (SIC-Op) (Exército Português, 2012, p. 4).

O estudo da aplicabilidade do conceito *BYOD* neste ramo das Forças Armadas apoia-se neste último sistema, permitindo assegurar solidez da capacidade de Comando e Controlo (C2) e a segurança da informação que circula nas suas redes de comunicações. Este sistema tem como estado final desejado a atingir: melhorar o processo de decisão; melhorar os processos de sincronização (trabalho em rede) dos utilizadores do sistema; otimização dos recursos; melhorar a interoperabilidade com a componente tática (SIC-T); maior precisão e qualidade da informação para apoio à gestão do conhecimento; melhorar a perceção da situação; melhorar a segurança da Informação; incrementar a confiança na informação; apoiar a gestão do conhecimento; disponibilizar os serviços necessários à atividade de comando e controlo do Exército; contribuir para o objetivo estratégico da Superioridade da Informação no Exército (Exército Português, 2012, p. 6).

De acordo com o plano de implementação do Sistema de Informação e Comunicações Operacional, do Exército, deverá materializar um sistema integrador de tecnologias de comunicações, nos domínios "NÃO CLASSIFICADO"[22] e "CLASSIFICADO"[23], que possibilite de uma forma simples, eficaz e segura, utilizar as facilidades e os serviços oferecidos pelas modernas Tecnologias de Informação (TI) (…) ".

[22] Domínio "NÃO CLASSIFICADO" – Infraestrutura do SIC-Op não classificada com acesso à internet, para o fluxo de informação não classificada.

[23] Domínio "CLASSIFICADO" – Infraestrutura do SIC-Op classificada para o fluxo de informação com classificação de segurança até Nacional SECRETO

O conceito *BYOD* irá ser abordado neste dois domínios, relativamente à segurança, no que concerne ao Exército. Este sistema subdivide-se em cinco subsistemas: Subsistema de Comunicações (SCom); Subsistema de Informação (SSI); Subsistema de Gestão (SG); Subsistema de Segurança da Informação (SSegI) e o Subsistema de Gestão da Informação e do Conhecimento. O estudo do conceito nestes domínios, irá ser focado no SCom/ Rede de Dados do Exército (RDE) / Redes locais das U/E/O, ao nível do acesso que constitui o ponto de entrada, em cada domínio da rede, para equipamentos terminais como computadores, telefones IP, impressoras de rede, terminais de videoconferência e sistemas de videovigilância. No SSI, e de acordo com os domínios de segurança, os serviços contemplados e alvo de análise são os seguintes, apresentados em forma de tabela:

Tabela nº 1 – Serviços de Apoio ao Comando e Controlo
Fonte: (Exército Português, 2012, p. 12)

Serviços	Domínio " NÃO CLASSIFICADO"	Domínio "CLASSIFICADO"
Voz	X	X
Voz Segura		X
VTC	X	X
Mensagens formais (MMHS)		X
E-mail funcional		X
E-mail informal	X	
Fax	X	
Fax seguro		X
Serviço de Portais	X	X
Armazenamento de Dados	X	X
Gestão Documental	X	X
Gestão de Tarefas	X	X
Gestão de Base de Dados	X	X
Informação geográfica		X
Informação meteorológica		X
Serviços Informações (ISR)		X
Serviços CIMIC		X
Informação Gestão (SIG)	X	(X)
Mensagens TDL		X
SICCE		X
Mensagens instantâneas	X	X
Serviço de internet	X	

No capítulo quatro, relativo à segurança e adoção do conceito *BYOD*, o SSegI será analisado, de forma a contemplar medidas para mitigar ameaças e vulnerabilidades deste. No entanto e de acordo com a doutrina do Exército Português, importa salientar que

”desejavelmente, como princípio, aos dispositivos de computação portátil não deverá ser atribuída uma classificação de segurança elevada. Em casos em que os requisitos operacionais o exijam, estes dispositivos poderão ser classificados para processar informação classificada, devendo ostentar uma etiqueta com a indicação da classificação de segurança e operar somente no modo de operação dedicado (…) e nenhum dispositivo de computação privado ou de outra organização deve ser ligado aos meios CSI do Exército” (Exército Português, 2013, p. 85).

d. Força Aérea

A evolução aferida nas últimas décadas ao nível da informatização nas organizações levou ao aperfeiçoamento de sistemas de comunicação e informação específicos (Força Aérea Portuguesa, 2009, p. 10). A Força Aérea Portuguesa (FAP) classifica os seus sistemas de informação[24] segundo a função para a qual foram gerados, os níveis de gestão da organização, o seu enquadramento temporal e tecnológico. Esta classificação resulta numa tipologia penta vetorial dos sistemas de informação, e segundo o Plano Diretor de Sistemas de Informação da Força Aérea (PDSIFA), 2009:

- Sistemas Operacionais ou Transaccionais – Sistemas que suportam as operações diárias da organização. Permitem a execução de tarefas específicas, com base em regras e procedimentos bem definidos, suportando grandes volumes de transacções. Apresentam como requisitos desempenho e disponibilidade elevadas. São sistemas vitais ao funcionamento da organização.
- Sistemas de Informação de Gestão – Permitem efectuar a análise dos dados disponíveis, convertendo-os em informação para apoio ao nível de decisão intermédio.
- Sistemas de Apoio à Decisão (SAD) – Auxiliam os utilizadores a tomar decisões fornecendo-lhes informação, modelos e ferramentas para a processar.
- Sistemas Estratégicos – Sistemas que fornecem informação estratégica para apoio à tomada de decisão, através de indicadores obtidos pela conjugação de diversas variáveis de informação. Privilegiam o processamento de elevadas quantidades de informação, em detrimento de tempos de resposta ou elevada disponibilidade. Destinam-se ao nível de topo da organização.

[24] “Um conjunto de equipamentos, métodos e processamentos e, se necessário, pessoal, organizados com vista ao desempenho de funções de processamento de informação” (NATO, 2008, p. 81).

– Sistemas Cooperativos ou de "*Workgroup*" – Permitem a execução de tarefas típicas de ambiente de escritório. Neste segmento enquadram-se as ferramentas de correio electrónico, gestão documental, folhas de cálculo, processamento de texto, entre outras.

A nossa análise para a implementação do conceito *BYOD* incidirá sobre as redes corporativas, sendo estas nas suas caraterísticas diametrais aos ramos, podendo ser abordadas de uma forma singular. Este sistema *Workgroup* materializa as diversas interligações que existem entre este ramo e os restantes.

A caraterização dos domínios operacionais nos diferentes ramos apresenta particularidades significativas em cada um deles. Os domínios de rede são em alguns casos distintos, tendo a análise de se focar, de forma a contemplar aspetos similares, no domínio do utilizador.

Em 2005, convindo a uma carência reconhecida no âmbito das FA, procedeu-se à interligação[25] das redes internas da Marinha, do EMGFA, do Exército e da FAP. Esta interligação tinha como principal objetivo promover o acesso, a troca e a partilha de informação profícua e proeminente entre as FA. Esta interligação possibilitava o acesso a dados, por exemplo o correio eletrónico, através da internet (Marinha, 2008, p. 18).

Desde 2012 que, apesar da adoção do *BYOD* ser uma realidade, a comunidade de informações militares dos EUA não encara com leviandade a implementação deste conceito em redes informáticas com informação classificada (Corbin, 2012).

A restrição do estudo dos Marine Corps ao uso de equipamentos particulares informáticos em redes não classificadas é similar à estratégia usada pelo Departamento da Defesa dos Estados Unidos da América, que serviu de orientação para a implementação do conceito *BYOD* nas redes não classificadas dos *Marines*[26] (Marine Corps, 2013, p. 3).

Este estudo incide em tempo de paz, não abordando a análise ao domínio do utilizador em tempo de campanha, em ambiente tático ou qualquer interação em teatros de operações.

[25] "Os serviços que atualmente estão disponibilizados através desta interligação são NÃO CLASSIFICADOS" (Marinha, 2008, p. 31).

[26] À semelhança dos casos de estudo analisados em Digital Services Advisory Group and Federal Chief Information Officers Council, 2012, onde nenhum dos programas *BYOD* envolvia a transmissão de informação classificada.

Para analisar a implementação do conceito *BYOD* nas redes corporativas das FA, o nosso estudo incidiu nos aspetos comuns nos diferentes domínios operacionais. Focou-se no domínio do utilizador, nas redes internas dos ramos, onde a informação limita-se a conteúdos envolvendo matéria não classificada.

Identificadas as caraterísticas das redes corporativas das FA e a inviabilidade da aplicação do conceito *BYOD* nas redes com a informação classificada, pela doutrina analisada e limitando a análise aos domínios existentes nas redes, no nosso caso o domínio do utilizador, face ao apresentado considera-se validada a Hip 2 – As atuais redes corporativas classificadas das Forças Armadas não permitem a aplicação do conceito *BYOD.*

Ao serem analisadas as interligações nas redes, com informação classificada e informação não classificada, foram identificadas limitações, essencialmente na vertente de segurança existente nas redes corporativas classificadas, tendo desta maneira respondido à Pergunta Derivada 2 – Quais as limitações atuais que as redes corporativas classificadas das Forças Armadas têm na adoção e implementação do conceito *BYOD*?

3. Os Requisitos Operacionais das Redes Corporativas das Forças Armadas Portuguesas

"Existem inúmeras aplicações e cada aplicação tem diferentes requisitos…"

Matthew Lesko

O conceito *BYOD*, quando foi abordado pela primeira vez, por Ballagas, et al., 2005, identificou requisitos essenciais para a interação entre os utilizadores, os equipamentos informáticos particulares e projetores para locais grandes[27]. Esses requisitos incluíam: a portabilidade, a sanitização, a habilidade, a multiutilização, a segurança física, a segurança da informação e privacidade, a aceitabilidade social, a interruptibilidade, a intencionalidade interacional e a manutenção.

A portabilidade é entendida como a capacidade dos equipamentos informáticos serem transportados pelos utilizadores, permitindo a sua ligação aos servidores de uma organização, neste caso materializado por um equipamento de projeção audiovisual. É feita também a distinção entre alta e baixa portabilidade, se esta comporta a utilização de outro material além do equipamento informático particular ou se simplesmente é requerida para uma ligação entre dois equipamentos a presença física do utilizador e o seu equipamento, seja ele um *smartphone*, *tablet* ou *laptop* (Ballagas, et al., 2005, p. 12).

Neste documento de Ballagas, et al., (2005), o requisito da sanitização corresponde às condições técnicas e de limpeza exigidas de um equipamento de forma a permitir a interação entre equipamentos e servidores. A habilidade, por sua vez, limita-se à identificação, no que concerne ao utilizador, da sua capacidade para lidar e trabalhar com os seus equipamentos informáticos e a multiutilização caracteriza-se pela capacidade de um sistema[28], permitir o acesso a mais do que um utilizador.

No que diz respeito à temática da segurança como requisito, a segurança física, aquando a sua abordagem por Ballagas (2005), correspondia à proteção que o sistema tem que ter contra o roubo e vandalismo. Esta segurança física, é contemplada na doutrina

[27] Quando o conceito aparece, o objetivo é a ligação com um determinado tipo de projetores, os projetores para locais grandes. No entanto, os projetores podem-se assumir diferentes tipologias: projetores de negócios, projetores de cinema digital, projetores de pós-produção, projetores de simulação e projetores estereoscópicos (Barco, 2014).

[28] Ligação existente entre equipamento informático particular e rede corporativa da organização onde está inserido.

nacional[29] como uma medida de proteção, sendo no entanto a definição de segurança[30] ambrangente, contemplando a segurança física e a segurança da informação, que é definida de seguida como segurança da informação e privacidade.

A segurança da informação[31] e privacidade referem-se ao grau de classificação da informação com que o utilizador é "atingido" quando interage, através dos seus equipamentos, com as redes corporativas. As técnicas de interação entre utilizadores e redes têm que permitir que informação sensível[32] não é disponibilizada a quem não tem permissão para ter acesso a ela. A segurança da informação baseia-se em quatro pilares: a disponibilidade, a integridade, a confidencialidade e a autenticidade.

Estes princípios são garantidos quando a informação está acessível, através de pessoas ou entidades autorizadas, de confiança, certificadas como tal, e completa, ausente de quaisquer alterações (Anon., 2007, pp. 1,2).

A aceitabilidade social refere-se à aceitação de uma técnica de interação, na presença de outros utilizadores, que presenciam passivamente a ligação entre equipamentos. Esta interação pode ser destabilizadora para quem observa e embaraçadora para os utilizadores. As ligações entre equipamentos e servidores, ao serem frequentemente de pouca duração e descontinuadas por eventos externos ao sistema carateriza o requisito da interruptibilidade. Por sua vez, a intencionalidade interacional depende da vontade do utilizador efetuar a ligação entre o seu equipamento e o servidor, não sendo necessária a ação de nenhuma iniciativa de virtualização, por parte do utilizador, aquando a presença do utilizador.

Finalmente, a manutenção contempla a periocidade que um sistema necessita de apoio técnico para ficar ou permanecer operacional e manter uma aparência que atraia o utilizador (Ballagas, et al., 2005, p. 13).

A Marinha quando analisa os requisitos nos SIC, releva a importância de dotar estes sistemas com especificidades imprescindíveis para o normal funcionamento dos mesmos.

---

[29] Publicação Doutrinária do Exército (PDE 2.00) – Informações, Contra informação e Segurança (2009)

[30] " A Segurança é definida como a condição obtida quando a informação, o material, o pessoal, as atividades e as instalações estão protegidos contra a espionagem, a sabotagem, a subversão e o terrorismo, assim como contra perdas ou divulgações não autorizadas." (Exército Português, 2009, pp. 1-2).

[31] "Os utilizadores dos sistemas de informação e comunicação (SIC) devem estar credenciados e autorizados a ter acesso, com base na necessidade de conhecer e de acordo com o grau de classificação de segurança da informação neles armazenada, processada ou transmitida" (Exército Português, 2003, p. 10).

[32] Nomes e números de telefone (Ballagas, et al., 2005).

Estes requisitos são especificados em diferentes características: a sobrevivência, a segurança, a flexibilidade, a prontidão, disponibilidade e importância operacional, a interoperabilidade[33]. São especificadas como outras caraterísticas, a integração e a racionalização (Marinha, 2005, pp. 38-46).

O requisito da sobrevivência compreende que os sistemas, abrangendo os domínios de rede e do utilizador, devem suportar medidas que garantam o perfeito funcionamento dos mesmos.

No caso específico da Marinha, o requisito da segurança apresenta-se como a área definida de uma forma uniforme e transversal nos diferentes ramos, abrangendo a classificação de segurança da informação, as credenciações de pessoal e acessos a instalações. Contempla que todas as medidas deverão ser postas em prática de forma a mitigar todos os riscos existentes e comprometedores da organização.

O requisito da flexibilidade está diretamente relacionado com a existência de planos de contigência, podendo estes ser utilizados em conformidade.

A prontidão, disponibilidade e importância operacional traduz-se no grau de disponibilidade, a fiabilidade, o nível de redundância e a demora requerida para acções de manutenção (Marinha, 2005, p. 41).

A interoperabilidade, apesar de ser caraterizada de diferentes maneiras quanto ao seu âmbito[34], quando esta é analisada entre uma organização e outra(s) externa(s), foca-se na interação dos sistemas, a capacidade de partilha de dados e procedimentos entre diferentes equipamentos e aplicações, englobando diversos níveis.

A integração e a racionalização, dizem respeito à maximização do *software* que é utilizado e diretamente relacionado com a permanente avaliação da relação custo-eficácia.

Tomando a base de observação do Exército Português e no que diz respeito aos requisitos levantados e identificados, face à sua atualidade, pertinência e adequabilidade para a temática em análise, os requisitos elencados e necessários para a interação de equipamentos particulares com uma rede corporativa, materializam-se na adoção de normas, de forma a garantir a interoperabilidade entre equipamentos.

[33] "Capacidade de comunicar, executar programas ou transferir dados entre várias unidades funcionais de um modo que requer ao utilizador pouco ou nenhum conhecimento acerca das características específicas dessas unidades" [ISO/IEC 2382-01: 1993].

[34] Tipo vertical, horizontal, interna ou externa (Marinha, 2005, p. 43).

Esta interoperabilidade é atingida através do uso de equipamentos e sistemas comuns, através da compatibilidade[35].

Outro requisito a ser respeitado é o da segurança, podendo esta se subdividir na segurança da informação, segurança do pessoal, segurança física e segurança de sistemas de informação e comunicação (INFOSEC)[36] (Exército Português, 2003, p. 6), permitindo operar em dois domínios de segurança de rede. Um para a informação "NÃO CLASSIFICADA" com ligação à internet e outro para a informação "CLASSIFICADA".

É necessário garantir flexibilidade de forma a permitir a utilização dos diferentes tipos e gerações de equipamentos e a incorporação de novas tecnologias. Deve ainda ser assegurada qualidade de serviço, disponibilidade e sobrevivência do sistema.

Na FAP, os requisitos identificados como essenciais ao sistema de informação analisado são: a reutilização, a flexibilidade e a segurança.

A reutilização incide sobre a utilização e implementação de funcionalidades em vários sistemas e sua disponibilização num único serviço, devendo estes estarem interligados entre si.

A flexibilidade permite a integração de sistemas com diferentes graus de maturidade, através do nível de abstração providenciado pelo serviço, (…) permitindo acrescentar serviços dinamicamente e possibilitando a implementação de segurança incluindo esta mecanismos de autenticação (Força Aérea Portuguesa, 2009, p. 32).

Após a identificação dos requisitos operacionais nos diversos ramos das FA, conclui-se que os requisitos comuns aos três ramos, devendo serem estes analisados, de forma a proporcionar uma análise linear e transversal são a flexibilidade/portabilidade, a segurança e a interoperabilidade (tabela nº 2 – Requisitos Operacionais na implementação do conceito *BYOD*).

---

[35] A compatibilidade é uma condição necessária para a obtenção da interoperabilidade. Define-se como a capacidade de dois ou mais componentes de equipamentos ou sistemas funcionarem na mesma estrutura ou ambiente sem que exista interferência mútua (Marinha, 2012, p. 23).

[36] "A INFOSEC, que inclui as vertentes de COMPUSEC (segurança dos computadores/informática, incluindo hardware e o software/sistemas de informação) e COMSEC (segurança das comunicações, entendidas como a infraestrutura de transporte da informação), consiste na aplicação de medidas de segurança e procedimentos com vista à proteção de informação processada, guardada ou transmitida em meios de comunicações e sistemas de informação (CSI), contra a perda da confidencialidade, integridade e disponibilidade da informação por causas acidentais ou deliberadas, assim como da integridade e disponibilidade dos próprios sistemas" (Exército Português, 2013, pp. 78,79).

É necessário analisar face aos requisitos operacionais identificados, a temática da segurança e formas de proteção. Este assunto é abordado no capítulo seguinte, pretendendo dar resposta às ameaças existentes por forma a materializar as contra medidas de segurança para preservar, o "controle de acessos, autenticação do utilizador, a confidencialidade, a reputação e a integridade" (Kizza, 2013, p. 46).

Tabela nº 2 – Requisitos Operacionais na implementação do conceito BYOD
Fonte: Do autor (2014)

	(Ballagas, et al., 2005)	Marinha	Exército	FAP
Portabilidade/Flexibilidade	X	X	X	X
Sanitização	X			
Habilidade	X			
Multiutilização	X			
Segurança	X	X	X	X
Aceitabilidade	X			
Interruptibilidade	X			
Intencionalidade	X			
Manutenção	X			
Sobrevivência		X	X	
Prontidão		X		
Disponibilidade		X	X	
Interoperabilidade		X	X	X
Qualidade			X	

Os requisitos operacionais comuns, transversais aos diferentes ramos das FA, foram identificados como sendo: a portabilidade/flexibilidade, a segurança e a interoperabilidade. As redes corporativas detentoras de informação não classificada das FA, ao serem alvo da implementação de um programa *BYOD*, são possuidoras destas caraterísticas. Assim, face ao apresentado considera-se validada a Hip 3 – As redes corporativas não classificadas das Forças Armadas, na adoção do conceito *BYOD*, são interoperáveis, seguras e flexíveis e respondida à Pergunta Derivada 3 – Quais as características que as redes corporativas não classificadas das Forças Armadas têm, na implementação do conceito *BYOD*?

4. A segurança na adoção do conceito *BYOD*

"Infelizmente não é um assunto simples. O volume de *malware* pode ser visto como uma causa de preocupação, mas o que deverá ser de extrema preocupação é a cada vez mais sofisticação da natureza das ameaças que as empresas encaram nos tempos que correm"

David Emm, Senior Researcher na *Kaspersky Lab*

O crescimento da utilização e a propagação de equipamentos informáticos particulares em organizações criou desafios de segurança às organizações onde o conceito *BYOD* é aplicado. Os equipamentos trazem associados a eles novas aplicações, novos aplicativos, novos sistemas, novos ambientes, novos riscos de segurança (Antonopoulos, 2011).

Estes riscos de segurança estão percetíveis numa sondagem realizada em 2013 pelos laboratórios *Kaspersky*. Nesta sondagem constatou-se que a perceção acerca de ataques cibernéticos, tentativas de intromissão ou recolha de dados de forma ilícita têm vindo a diminuir. No entanto, a realidade mostra diferenças significativas. A sondagem revela que o volume de *malware*[37] tem vindo a aumentar, existindo diariamente 200,000 novos casos de *malware*. O número de ameaças a dispositivos informáticos móveis referenciado em 2011 foi igual ao número de casos referenciados entre 2004-2010, e o número em 2012 foi seis vezes superior ao de 2011. Em março de 2013 mais de 9,000 novas ameaças de *malware* foram referenciadas (Kaspersky Lab's, 2013, p. 5).

A gravidade e a frequência de incidentes referentes à segurança sejam estes intencionais ou não, estão a aumentar, representando uma ameaça crítica, uma preocupação a não ser descurada, ao perfeito funcionamento dos sistemas de tecnologia e informação (European Commission, 2013, p. 11).

O conceito *BYOD* agrega com ele novos riscos de segurança, não contemplando quaisquer medidas de controlo. Ao contrário dos computadores portáteis, onde a segurança visa essencialmente aplicações para evitar a intrusão dos equipamentos por parte de ações exteriores não autorizadas, os *smartphones* e os *tablets* estão vocacionados para conterem aplicações essencialmente contra o roubo dos próprios equipamentos, localização dos mesmos e proteção da informação contida nestes (Antonopoulos, 2011). Esta divergência

[37] "Entende-se por *malware* qualquer *software* que tem como finalidade infiltrar ou criar dano num computador individual, servidor ou rede" (Avira, 2008).

ocorre, em certa medida, por os computadores portáteis serem da organização ao invés dos equipamentos informáticos, *smartphones* e *tablets*, pertencerem aos utilizadores.

O fator desfavorável na adoção e aprovação da implementação do conceito *BYOD* numa organização é o fator da segurança. Os equipamentos informáticos particulares revestem-se de tamanha vulnerabilidade, materializando a "porta de entrada" para qualquer tipo de ataque com o intuito de aceder a material interno, que de outra forma não teria acesso. Através destes ataques, podendo estes serem divididos em cinco categorias[38] (figura nº 3.- Classificação de diferentes tipos de ataque), as organizações são colocadas em risco, vendo elas conteúdos de informação privada comprometidas (Vmware, 2013).

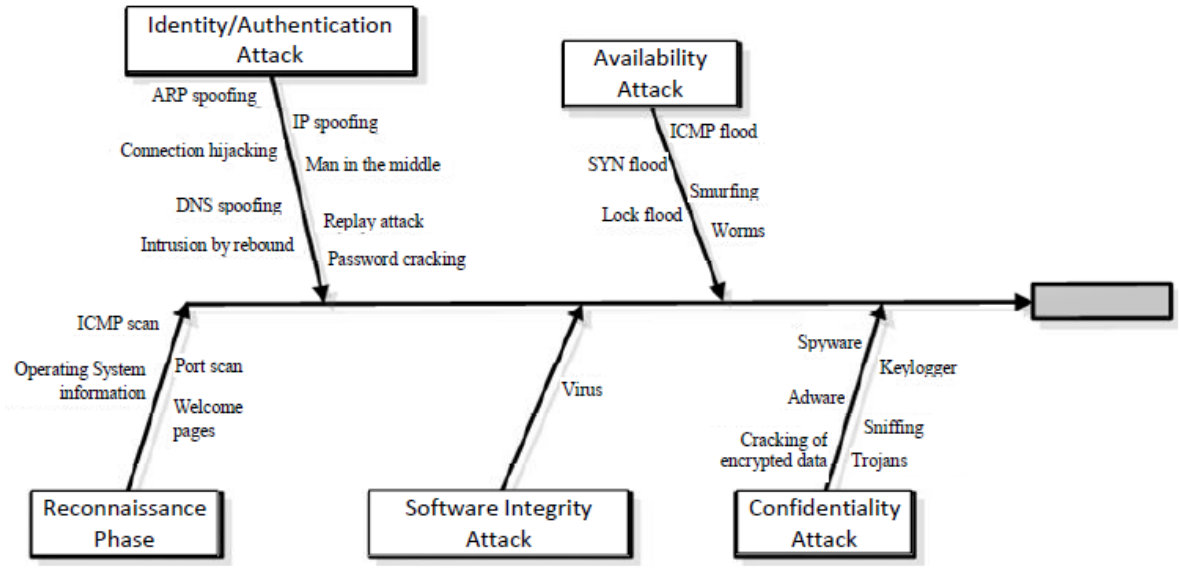


Figura nº 3 – Classificação de diferentes tipos de ataque
Fonte: (Assing & Calé, 2013, p. 16)

Na conceção de um programa de implementação *BYOD* existem riscos a serem mitigados. São eles: perda de controlo no âmbito da segurança[39], quebras de segurança, gerir e manter obrigações contratuais legais com os funcionários da organização e a exposição da informação da organização, podendo esta ter uma classificação de segurança que não permite a sua divulgação a qualquer pessoa, pelo facto dos equipamentos informáticos particulares poderem ser usados para fins que não organizacionais (Hayes & Kotwica, 2013, p. 4).

[38] *"Reconnaissance phase, identity/authentication attack, confidentiality attack, availability attack* e *software integrity attack"* (Assing & Calé, 2013, pp. 15,16).

[39] Intrusão, deteção e uso de *malware* (Hayes & Kotwica, 2013, p. 3).

Existem várias categorias onde se englobam as diversas ferramentas informáticas que se poderão constituir como um risco a mitigar. Estas ferramentas irão ser identificadas, tendo em vista as perspetivas de ataques (ameaças), as defesas (contra medidas) e as falhas no sistema (vulnerabilidades). Para o efeito, identificámos doze ferramentas, tendo sido divididas da seguinte maneira (Amado, 2006, pp. 3-6):

Tabela nº 3 – Ferramentas e Categorias de mobile security
Fonte: Do autor (2014)

	Ameaças	Vulnerabilidades	Contra Medidas
Anonimity	X	X	
Antitrojans			X
Antivírus			X
Exploits		X	
Firewalls			X
Messengers	X	X	
Nukers	X		
Password Crackers	X		
Scanners	X	X	
Trojans	X		
Vírus	X		
Assinaturas Digitais			X

a. As ameaças atuais existentes nas redes corporativas

As ameaças aos equipamentos informáticos particulares são reais, atuais e diversas. À medida que o preço destes equipamentos vai reduzindo, o acesso ao consumidor fica facilitado, aumentando consequentemente o número de funcionários de uma organização com equipamentos aplicáveis ao conceito *BYOD*. Esta facilidade de acesso, posse e uso generalizado de equipamentos informáticos torna-se um alvo para *hackers*[40] e *malware*, com vista à obtenção de dados pessoais e organizacionais (Nunoo, 2013, p. 81).

Os equipamentos informáticos particulares são alvo de diversas ameaças, sendo as mais comuns (LetMobile, 2012, p. 4): a perda ou roubo de um equipamento, o comprometimento do canal de comunicação em uso por um equipamento e a partilha sem restrições de segurança de um equipamento.

[40] "Pessoas com grandes conhecimentos de informática e programação, que se dedicam a encontrar falhas em sistemas e redes computacionais" (Priberam, 2013).

Os ataques a equipamentos informáticos móveis podem assumir a forma de: *Denial of Service* (DOS), *Hacking phone*, Vírus, *Spyware* e ataques de exploração, *phishing*, *SMiShing* e *Vishing.* (Kizza, 2013, p. 440). No entanto, alguns equipamentos têm particularidades, que lhes permite retirar informação de qualquer local, gravar qualquer tipo de informação, sem ser necessário ausentar-se do local de trabalho[41].

As tipologias de ameaças existentes foram identificadas na tabela anterior, totalizando sete tipologias. Estas definições foram adaptadas, devido à sua ambrangência e atualidade, da obra de João Amado (2006), *Hackers - Técnicas de Defesa e de Ataque*. A ameaça tipificada como *anonimity* tem como finalidade: conservar o anonimato do utilizador, enquanto este utiliza uma rede ou equipamento informático, podendo esta utilização ser através de servidores, de mensagens de *e-mail* ou através de outros programas e aplicações existentes na internet. Converte-se também em vulnerabilidade, visto que os equipamentos particulares, ao poderem ser ligados a uma rede corporativa poderão ser realizados sem identificação do utilizador.

Outra tipologia de ameaça são os *messengers*, programas cuja utilização concentra-se essencialmente em trocas de mensagens entre utilizadores que estejam ligados na internet. Esta troca de mensagens poderá incluir troca de ficheiros de dados, imagens, vídeos e sons. Estas ameaças refletem-se, à semelhança da anterior, também numa vulnerabilidade, visto que existem peculiaridades nos programas que os servidores estão sujeitos e que lhes poderão provocar danos ou mesmo quebras de confidencialidade.

Os *nukers*, por sua vez, destinam-se essencialmente a degradar o desempenho de um equipamento informático, estando este ligado a uma rede corporativa ou não.

As ferramentas destinadas a quebrar e identificar quaisquer senhas e contrassenhas de segurança que os utilizadores utilizem para aceder aos diversos sistemas, programas e aplicações, conhecidas como *password crackers* são outra tipologia comum da ameaça que está presente nos sistemas de informação e comunicação.

Os *scanners* são ferramentas destinadas à procura de portas de comunicação abertas, num específico equipamento, podendo ser utilizada esta quebra de segurança no acesso a informação sem consentimento ou autorização.

[41] Caso dos leitores de mp3, ou qualquer outro dispositivo eletrónico portátil que tenha um disco-rígido (WatchGuard, 2013).

Os *trojans*, por sua vez, são programas que ao serem executados por quem os recebe em forma de ficheiro, mensagem ou outro qualquer tipo de documento, permitem o acesso ao computador e a toda a informação residente nele (figura nº 4.- Exemplo de aplicações maliciosas).

Figura nº 4 – Exemplo de aplicações maliciosas
Fonte: (Ballano, 2011)

Finalmente, os *vírus* são programas que ao serem enviados para outro computador e a não serem detetados, infetam ficheiros, podendo atingir no limite a total inutilização do computador infetado.

b. As vulnerabilidades existentes na adoção do *BYOD*

Uma vulnerabilidade do ponto de vista da segurança da informação pode ser definida como "uma fraqueza identificada de um sistema controlado, em que os controles necessários não estão presentes ou já não são eficazes" (Whitman & Mattord, 2011, p. 11).

A segurança da informação organizacional, primariamente foi uma preocupação consignada exclusivamente a dispositivos que estivessem fisicamente ligados a uma rede de uma organização, ou dentro das instalações desta (Allam & Flowerday, 2010, p. 2). Atualmente existe a necessidade de proteger os equipamentos informáticos particulares que têm ligações sem fios a estas organizações.

Uma vulnerabilidade numa rede corporativa provém de lacunas que um *software* pode ter devido à sua complexidade e interação. Estas lacunas poderão, em muitas das

vezes, serem produto de um fraco controlo de qualidade, insuficiência na revisão do produto e testes incompletos. Exemplo destas falhas de *software* foi o caso detetado no sistema "*Distributed Common Ground System-Army* (DCGS-A) ", utilizado no Afeganistão pelas forças norte americanas, onde a escolha de equipamentos com falhas ao nível de requisitos adequados e problemas técnicos constitui-se como obstáculo a todo o processo de decisão (Smith, et al., 2013).

Algumas organizações empresariais refugiam-se em técnicos com desajustada preparação, expondo assim os seus produtos, afetando *à posteriori*, sistemas operativos, aplicações de sistema e aplicações de utilizadores (MCS, 2006, p. 6). Aproximadamente quatro em dez organizações empresariais têm um historial de quebras de segurança (Hayes & Kotwica, 2013, p. 1).

A utilização de equipamentos informáticos particulares pressupõe a utilização do *email* e outras aplicações, com autorização para incorporarem os equipamentos autorizados na ligação às redes corporativas. O *email* é a aplicação mais popular para usuários profissionais, sendo esta um ponto de partida para implementação de boas práticas de segurança (LetMobile, 2012, p. 3).

As tipologias de vulnerabilidades identificadas totalizam quatro tipos. Além do *anonimity*, *messengers* e *scanners*, cujos conceitos foram definidos anteriormente, existe também a ferramenta *exploit*[42]. Esta ferramenta identifica falhas ao nível da segurança, normalmente em sistemas operativos, existindo mecanismos cuja finalidade é eliminar estas vulnerabilidades, incluindo-se nas contra medidas que se poderão utilizar de forma a amenizar as falhas de segurança.

c. Contra Medidas a adotar na implementação do *BYOD*

Existem variadas contra medidas que podem ser utilizadas por forma a mitigar as vulnerabilidades expostas às ameaças anteriormente definidas. A escolha de uma contra medida depende de fatores como o tipo de informação que a organização tem na sua posse, bem como as rotinas e padrões que os funcionários têm aquando da interação com os sistemas informáticos. Não existem contra medidas padrão, como que de um referencial se tratasse que abranja todas as organizações da mesma forma. As organizações devem ter esta consciência e procurar as melhores e mais adequadas soluções para as suas realidades. As organizações na procura da otimização das contra medidas que deverão vigorar no seu

[42] Também conhecida por *holes, backdoors* (Amado, 2006, p. 4).

interior, deverão fazer as suas próprias avaliações de risco e pesar as vantagens e desvantagens nos seus casos específicos (Nunoo, 2013, p. 82).

A virtualização do *desktop* permite a utilização por parte dos funcionários, através de identidades, da rede corporativa, concedendo acesso por estes, à sua informação na rede através de qualquer equipamento informático particular autorizado para o efeito, estando no interior da organização (Vmware, 2013).

Torna-se inevitável a monitorização dos equipamentos informáticos particulares, pois as novas tecnologias ao surgirem constantemente e os novos hábitos de utilização por parte dos utilizadores, proporciona a que as ameaças estejam permanentemente a surgirem e a reajustarem-se (Taurion, s.d.). No entanto, essa monitorização levanta um problema de legitimidade legal, pois uma possível confiscação e uma potencial destruição de qualquer equipamento não é suscetível de ser pacífico.

A segurança pode ser analisada em diferentes componentes num caso de aplicabilidade de *BYOD*. A segurança pode ser abordada no âmbito da segurança do conteúdo da informação, no âmbito da segurança do sistema da rede e no âmbito da acreditação de infraestruturas e equipamentos. Nestas abordagens, importa salientar que transversalmente devem-se adotar medidas de forma a mitigar e eliminar quaisquer ameaças que comprometam a organização militar. Assim, as contra medidas deverão ser: (Exército Português, 2012, p. 17): Proteger, controlar, monitorizar e auditar, de modo centralizado, o acesso à informação; gerir dinamicamente os acessos, em função da validade da credenciação e autorização de acesso; responder a desafios como a prevenção do roubo de propriedade intelectual ou de dados confidenciais, por parte de utilizadores não autorizados; prevenir fugas de informação involuntárias, que resultam do envio de conteúdos por correio eletrónico para um destinatário errado, do roubo ou perda de uma *pendrive*, de um disco externo ou de um computador portátil; colocar ficheiros, sobre os quais recaiam suspeitas, de "quarentena", isto é, bloqueá-los de forma centralizada até se efetuar uma investigação e eventualmente voltarem a ficar disponíveis e o registo centralizado das ações que os utilizadores executem ao nível de classificação de informação, dotando os administradores de capacidade para detetar possíveis tentativas de violação de políticas de segurança, através de uma ferramenta de auditoria.

As tipologias de contra medidas identificadas totalizam quatro formas[43]: os Antitrojans, programas destinados a proteger o computador contra a presença da ameaça *trojan*; os Antivirus, ferramentas destinadas a proteger o computador de qualquer tentativa de "infeção" por parte de vírus; as firewall, programas ou sistemas " que permitem controlar o acesso a computadores, interligados numa rede" (Amado, 2006, p. 4) e finalmente as assinaturas digitais, que através de tecnologia de criptação torna-se possível a proteção da autenticidade de documentos e da sua informação.

No entanto, uma variável na equação da segurança nunca deverá ser ignorada. Esta variável denominada "*Invisible Security Threat*", materializa a ameaça mais perigosa à segurança de uma organização, a ameaça interna. Existe uma disparidade entre a comodidade de acesso e de utilização de equipamentos informáticos particulares e a formação necessária para a apropriada proteção da segurança de informação neles contidos (Santos, 2011, p. 114). Esta ameaça é materializada pelos próprios membros, dignos de confiança, normalmente uma pessoa, com possível acesso privilegiado a informação sensível, que usa esta oportunidade para recolher e disseminar informações da organização para entidades externas a esta, sem autorização para tal (Kizza, 2013, p. 79).

O futuro irá ser caraterizado pelas organizações a prestarem cada vez maior atenção às ameaças internas e a adotarem medidas para se protegerem contra os perigos que daí advenham e que poderão colocar em risco a sobrevivência da própria organização (Coviello, 2014).

Ao serem identificadas quais as ameaças que poderão surgir na adoção do conceito *BYOD* nas redes corporativas das FA, foram elencadas as vulnerabilidades dos sistemas informáticos e como estas poderão ser exploradas. Torna-se necessário de forma a amenizar estas vulnerabilidades, a inclusão de procedimentos de segurança denominados de contra medidas, minimizando efeitos indesejados, mitigando desta maneira qualquer ameaça anteriormente analisada.

[43] Quando as ameaças são originadas por *hacker* profissionais (distinguem-se dos amadores pelos objetivos, recursos, acesso e tempo) as contra medidas dividem-se em: *"Source Code Inspection, Security Test and Evaluation, Software Engineering, Object-Oriented Programming (OOP), and Developmental Assurance Approaches, Gratuitous Formal Methods, Verifiable Systems* e *Verifiable Protection"* (Anderson, et al., 2004, pp. 6-9).

Face ao apresentado considera-se validada a Hip 4 – As contra medidas, face à exploração das vulnerabilidades pelas ameaças existentes, conseguem ser mitigadas, na adoção do conceito *BYOD* nas redes corporativas das Forças Armadas e respondida à Pergunta Derivada 4 – Quais as ameaças à segurança militar, na ligação de dispositivos *BYOD* às redes corporativas das Forças Armadas?

5. Mobile Device Management – Caso de estudo (*Huawei Technologies co., LTD*)

O conceito *BYOD* alarga os limites "fronteiriços" de uma qualquer organização. A sua implementação permite aos utilizadores empregarem os seus equipamentos, quer no trabalho ou no simples *download* de aplicações lúdicas.

À medida que as pessoas vão variando entre aplicações pessoais e aplicações empresariais da organização a que pertencem, os limites entre o que é pessoal e o organizacional começa a tornar-se ambíguo. Para muitas organizações empresariais torna-se impraticável negar a utilização de equipamentos informáticos particulares no seio desta.

Perante estes casos, a empresa *Huawey Technologies* desenvolveu uma série de procedimentos que servem de base de estudo, tanto estrutural como modelar, para poder ser aplicado numa qualquer organização. Estes procedimentos, que irão ser analisados de seguida, constituem-se como uma resposta a novas vulnerabilidades de segurança, já caraterizadas no capítulo anterior. Esta variedade de problemas sejam eles tentativas de intrusão nas aplicações pessoais, ou através destas, tentarem atingir as aplicações organizacionais, surgem como desafios para os quais as organizações do futuro terão que estar preparadas. Esta preparação surge como uma solução de segurança, que a *Huawey* desenvolveu, exposta na figura nº 5 com o nome de *"Huawey BYOD Security Solution"* (Deng, et al., 2014).

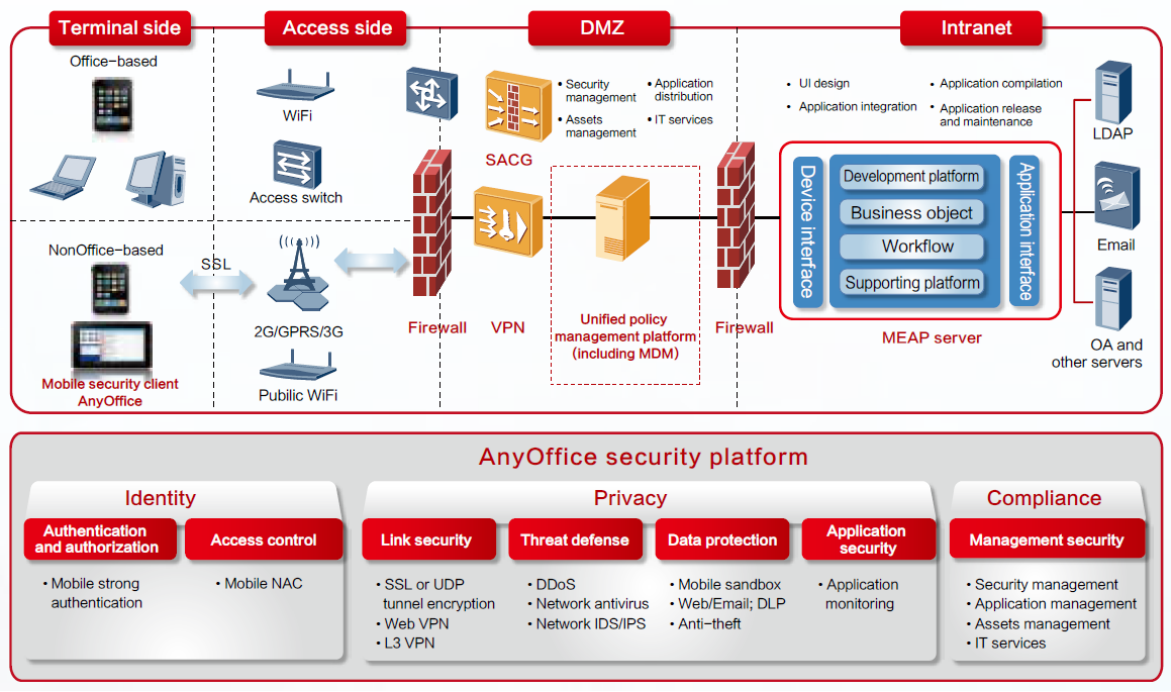


Figura nº 5 – Arquitetura e componentes chave na solução de segurança
Fonte – (Deng, et al., 2014, p. 3)

Para a resolução de conflitos que possam existir entre os requisitos dos utilizadores pertencentes a uma organização e as políticas de implementação da mesma entidade, a *Huawei Technologies co., LTD* desenvolveu uma solução que permite aos utilizadores maior liberdade no uso de equipamentos informáticos particulares.

Esta solução é composta em componentes essenciais: *Smart Mobile Access Client*[44], *Consistent Network Acess Control*, *Secure Remote VPN Acess*, *Carrier-Class Mobile Threat Defense*, *Unified Security Police Management* e *Simple Plataform for Releasing Mobile Enterprise Applications* (Deng, et al., 2014, pp. 3,4), assentando em três pilares: a identidade, a privacidade e a conformidade.

Estas componentes caraterizam-se pela criação de uma solução de segurança que proporciona interação entre os utilizadores, redes e aplicações. Providencia uma gestão de fácil aplicação, integrando um conjunto de aplicativos[45] cuja utilidade se materializa na capacidade de identificação de utilizadores internos e externos. Os três pilares anteriormente identificados, a identidade, a privacidade e a conformidade, são a simplificação da solução de segurança (figura nº 6.- Solução de Segurança- AnyOffice).

Figura nº 6 – Solução de Segurança (*Huawey Technologies*) - AnyOffice
Fonte: (Deng, et al., 2014, p. 6)

[44] Denominado como " cliente AnyOffice" (Deng, et al., 2014, p. 3)

[45] "*Secure sandbox, secure email client, secure browser, mobile device management (MDM) software, Layer 3 virtual private network (L3 VPN) client and virtual desktop"* (Deng, et al., 2014, p. 4).

A identidade materializa políticas de controlo de acesso baseadas em conhecimento de conteúdos. Esta caraterística corporaliza a possibilidade de configuração de variados modelos de política de gestão.

O cliente AnyOffice inicia um módulo de segurança de forma a controlar a rede de acesso. Assim, um utilizador pode remotamente aceder a uma rede corporativa de uma empresa a partir de um qualquer local (café, aeroporto,…). Este processo é completamente transparente, protegendo as ligações de uma rede. O modelo de gestão garante políticas de segurança consistentes e em conformidade com a rede e com as políticas de segurança da organização. Permite que qualquer indivíduo consiga aceder de forma livre aos recursos corporativos internos, usando qualquer dispositivo autorizado (*BYOD*) ou dispositivo virtual a partir de qualquer lugar e através de qualquer rede (com fios, sem fios ou rede remota).

A privacidade contempla, através do cliente AnyOffice, a criação de uma zona de segurança onde as aplicações pessoais estão isoladas das aplicações organizacionais ou corporativas, no mesmo dispositivo móvel (figura nº 7.- Segurança de Dados e Ameaças).

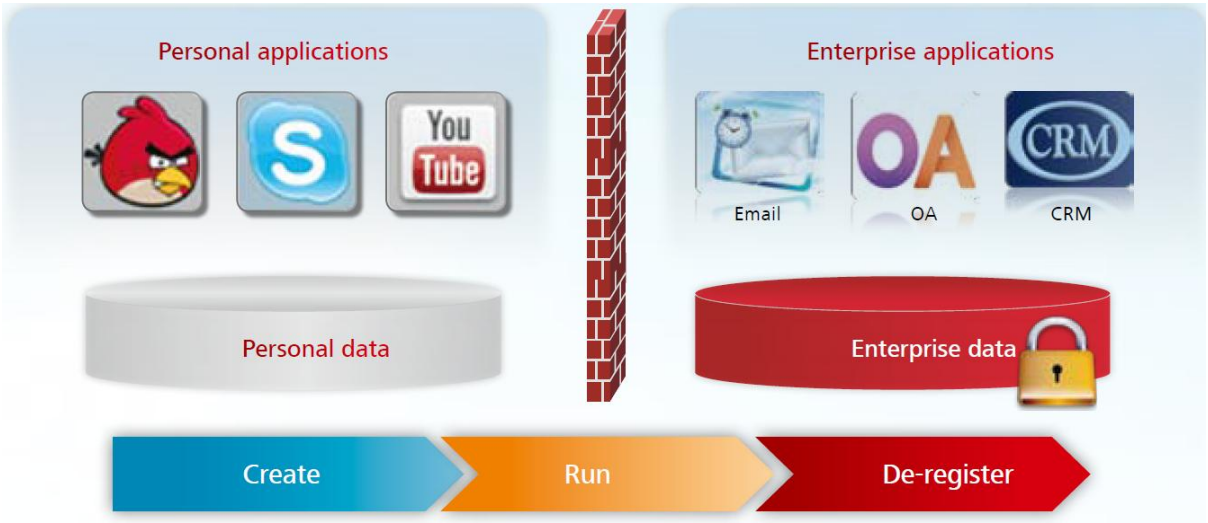


Figura nº 7 – Segurança de Dados e Ameaças
Fonte: (Deng, et al., 2014, p. 7)

Esta zona de segurança suprime infindos riscos, tais como a fuga de informação, infeção por vírus incorridos quando as aplicações pessoais ou privadas são misturadas com aplicações corporativas.

Quando um utilizador utiliza a aplicação *AnyOffice*, todas as ações internas da organização são processadas no interior de um ambiente seguro e estanque de quaisquer dados pessoais. Os dados são armazenados numa área isolada e segura e protegidos através de um sistema criptográfico. Este processo compreende um conjunto de ações que coloca em prática: Monitoriza o desempenho das aplicações, previne a possibilidade de acesso de aplicações pessoais a aplicações corporativas, ativa o *download* ou *upload* de aplicativos com base numa política pré-definida e limpa arquivos temporários e dados sem deixar qualquer vestígio durante a aplicação de registo, reduzindo ainda mais o risco de divulgação de dados, contribuindo para esta aplicação móvel de segurança dois fatores determinantes: o *secure push mail* e o *Huawei firewall*, mitigando essencialmente as ameaças provenientes da internet contra plataformas móveis pessoais e/ou organizacionais.

A conformidade por sua vez materializa-se num ciclo dividido em quatro fases: a aquisição, a projeção, a execução e a retirada.

A solução para a segurança que a empresa em estudo proporciona assenta em especificações técnicas muito concretas. Esta especificidade é essencial no processo de aquisição de novo material.

Antes de um qualquer equipamento ser projetado, uma organização tem que garantir a conformidade dos aparelhos. Na solução *Huawei BYOD* as *firewall* e módulos Wi-fi podem ser configurados de uma forma segura e políticas de implementação desenvolvidas quando os equipamentos são entregues ao destinatário. Assim, a execução e o seu foco centra-se na segurança das aplicações e na informação contida nelas.

Na retirada, esta fase engloba a saída de um qualquer funcionário da organização ou um equipamento perdido, a organização tem capacidade de desinstalar aplicações do equipamento e apagar informação retida nele.

Na inclusão do uso de equipamentos informáticos particulares na organização empresarial, a *Huawei* materializa assim uma eficiente solução de segurança *BYOD* para organizações semelhantes, materializando-se como um dos exemplos a contemplar como referência, permitindo desta maneira, criar uma zona segura entre um ambiente organizacional e pessoal, equilibrando uma balança entre segurança e eficiência para o *BYOD*.

6. Contributos para o *BYOD* nas Forças Armadas Portuguesas – do *BYOD* ao *BYOC*

"Se existe uma competência na vida que todas as pessoas necessitam, é a habilidade de pensar com objetividade criativa"

Josh Lanyon

A título de corolário da investigação, deixam-se algumas considerações finais, desafios futuros face a uma implementação do conceito *BYOD* nas redes corporativas das FA e propostas a considerar:

- De forma a minimizar os riscos associados a fugas de informação e consequente comprometimento do indivíduo e organização, torna-se fulcral evitar que informação da organização esteja armazenada nos equipamentos informáticos particulares;
- Torna-se pertinente que uma cultura organizacional de segurança[46] seja reforçada, cabendo ao utilizador e respetiva organização, sensibilidade referente à proteção física dos equipamentos de forma a evitar o seu roubo, encriptação e *backup* de informação, uso de aplicações para controlar e localizar remotamente os equipamentos informáticos pessoais e evitar o uso de *hot-spots Wi-fi*[47];
- Para tornar possível a implementação do conceito *BYOD* numa organização deverão ser identificadas e priorizadas políticas de segurança e medidas adicionais a implementar;
- Aumentar a consciencialização dos funcionários de uma organização sobre os riscos da engenharia social[48] e prevenir as ameaças com treino. Desta forma, a harmonização de procedimentos pode reduzir o risco de perda de informação ou outros quaisquer tipos de risco;

[46] A cultura organizacional de segurança destina-se a chamar a atenção generalizada e maciça para uma ameaça à segurança. Quando as pessoas têm consciência da ameaça, espera-se que se tornem mais cuidadosas, mais atentas e mais responsáveis nas suas ações. Tornam-se mais propensas a seguir as orientações de segurança.

[47] "*Hotspot Wi-fi* indica um lugar onde é possível ter acesso à internet, e é um termo que vem do inglês. *Hotspot* significa "lugar quente" (Anon., 2014).

[48] "Engenharia Social é a habilidade de conseguir acesso a informações confidenciais ou a áreas importantes de uma instituição através de habilidades de persuasão" (Cipoli, 2012)

- O acesso e a transmissão de dados têm que acontecer dentro dos sistemas da organização e fornecidos por estas. Os dados no conceito *BYOD* não são aplicados da mesma maneira que no conceito *Cloud Computing*;
- Todos os equipamentos informáticos particulares ligados a uma rede corporativa deverão estar protegidos e toda a informação residente nestes criptografada;
- A preservação de dados da organização deverá obedecer a padrões definidos, copiados e armazenados de uma forma centralizada;
- Criar uma política de implementação onde o contrato seja aceite entre as partes e as condições estabelecidas sejam respeitadas na implementação do conceito *BYOD* na organização;
- Providenciar que as medidas de prevenção de perda de dados têm a capacidade de apagar remotamente a informação que está no equipamento informático particular com acesso à organização, censurando as informações pessoais a menos que considerado (Singh, 2013);
- Analisar o conceito *Cloud Computing Technology* e ver a sua relação com o conceito *BYOD*, a sua pertinência face aos custos associados, flexibilidade e desenvolvimento tecnológico.

No planeamento de um projeto de implementação do conceito *BYOD* é necessário, para minimizar o risco, implantar uma solução de acesso remoto.

Torna-se fundamental estar ciente que não existe a mitigação total da ameaça, sendo imprescindível o recurso a várias formas de proteção. Estas poderão passar pela implementação de uma arquitetura de rede multinível (Assing & Calé, 2013, pp. 194,195).

Além disso, uma vez implementadas, as soluções de segurança poderão tornar-se muito rapidamente obsoletas, devido à constante evolução da ameaça. Terá que existir um equilíbrio entre as limitações impostas por ferramentas, aplicações e rotinas de segurança, e a flexibilidade fornecida por essas soluções de mobilidade.

Devem ser tomados todos os cuidados por forma a assegurar a integridade da informação da organização, através dos elementos técnicos (*firewall*, antivírus,etc), e envolvimento do utilizador, seja com treino ou procedimentos específicos adaptados, pois o utilizador é a chave do sucesso de qualquer política de segurança.

Face a um futuro onde a implementação do conceito *BYOD* se materialize no seio das FA, deverão existir três fases ondes questões relevantes se levantam tornando

imperativo responder de forma a viabilizar com sucesso essa implementação. Da análise dos fatores abordados neste trabalho em cada capítulo identificámos que a efetuação deste conceito divide-se em três fases: antes do *BYOD*, durante o *BYOD* e depois do *BYOD* (figura nº 8).

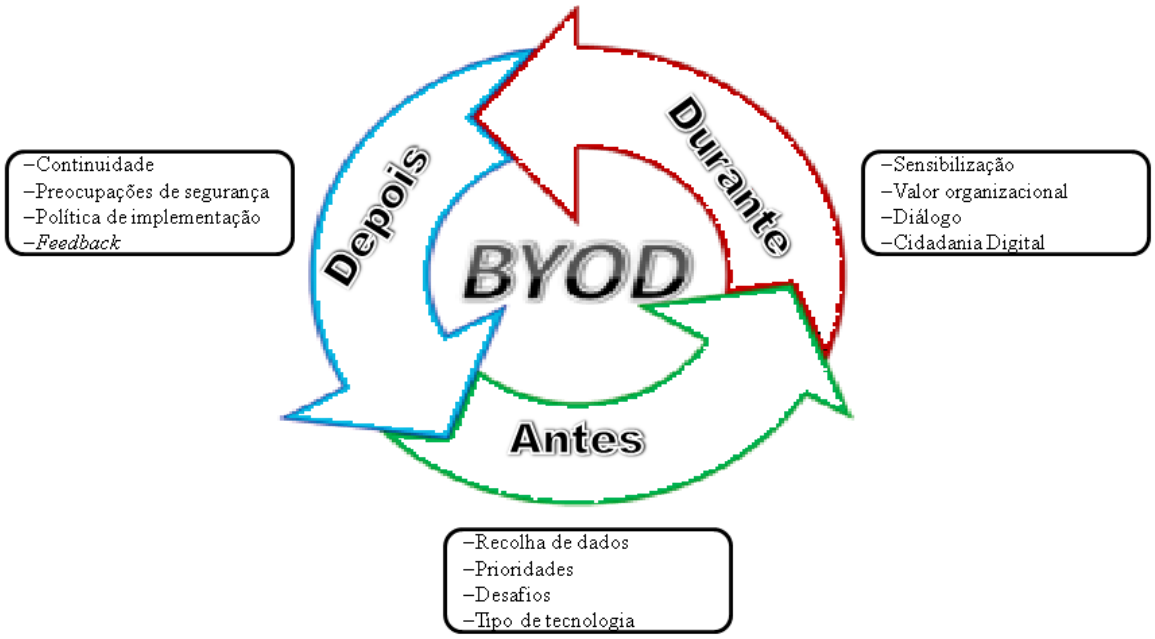


Figura nº 8 – Fases de implementação do *BYOD*
Fonte: Autor, 2014

Antes da implementação do conceito é necessário recolher dados de forma a rentabilizar todas as variáveis existentes na implementação de um programa deste tipo. Torna-se necessário responder a variadas questões: Quais são as prioridades das redes corporativas das FA? Que desafios se apresentam para os utilizadores face a um modelo *BYOD* organizacional? Que tipo de tecnologia têm os utilizadores para uso particular? Qual é o acesso à internet que os utilizadores têm externo à organização? Qual a razoabilidade dos custos para um projeto de implementação desta tipologia? Qual a formação, apoios e treino que será exigido ao utilizador face ao conceito *BYOD* no seu local de trabalho?

Durante a efetuação do programa, é essencial para a organização sensibilizar os utilizadores sobre os dispositivos, suas especificações e qual a evolução tecnológica que assiste. Deve ser realçada a importância para a organização, a sua inserção direta ou indiretamente na cultura organizacional, o valor que acrescentam a todo o processo de

apoio à decisão bem como o contributo para uma cultura de cidadania digital[49]. Além de sessões informativas, onde a segurança assume papel de relevo, sites e aplicações, a organização deverá promover o diálogo entre todos os intervenientes no processo para que seja possível proporcionar oportunidades para que se expressem preocupações e perguntas específicas sobre o modelo *BYOD* existente. Este diálogo deverá incluir temáticas diversas, sendo a cidadania digital pertinente face à sua atualidade, exigindo, tal como Seth Robinson, diretor de análise de tecnologia da CompTIA o afirmou, "o uso de novas tecnologias uma mudança na abordagem de segurança" (Convergência Digital, 2013).

Na última fase, a informação terá de ser continuamente providenciada aos utilizadores devido à dinâmica das tecnologias de informação. A organização terá que se preparar para poder responder à pergunta: Após um ano de implementação do conceito *BYOD* nas redes corporativas das FA, quais as ilações tomadas e quais as melhorias ou viabilidade de todo o processo? Esta questão está associada a uma recolha permanente de dados quantitativos e qualitativos, bem como a consequente análise desses resultados. Deverá existir oportunidade de *feedback* por parte dos utilizadores, quais as vantagens e inconvenientes que os próprios constataram e quais as inovações, dos seus pontos de vista a serem implementadas.

Todo este pós- processo deverá ser seguro, recaindo as preocupações na segurança *online*, na segurança quando os utilizadores trazem os equipamentos para casa, no acesso e sequente filtragem da Internet. Procedimentos e políticas de implementação que as organizações usam para assegurarem a integridade e segurança da informação devem ter em conta a cultura organizacional, para que as mudanças e melhorias aos procedimentos reinantes não sejam percecionados pelos funcionários como barreiras à mudança (Nunoo, 2013, p. 17).

No que se refere à implementação e acesso à informação e sistemas sem informação classificada, a organização militar deverá ponderar, no que se refere a soluções de segurança e opções tecnológicas, parcerias com organizações empresariais, especialistas locais e globais relacionados com conteúdos digitais, instituições de ensino, ligação com revendedores locais e prestadores de serviços de tecnologia.

Uma das soluções na recolha de dados em todo este processo de implementação, tomando como base a sondagem feita e formalizada no relatório "*The personalisation*

[49] Cidadania digital ou *Digital Citizenship*, é " a abordagem global no uso de tecnologias digitais..." (School Technology Branch, 2012, p. 24).

challenge - Business culture and mobile Security", pela *Intelligence Unit* do *"The Economist"*, poderá passar pela inclusão das seguintes questões num inquérito organizacional:

- Como é que o uso de equipamentos informáticos particulares no local de trabalho tem impacto em si, nos seus colegas e na sua *performance*?
- Quais as preocupações do utilizador no âmbito da segurança com os riscos, invasão de privacidade, gestão da sua informação pessoal contida no seu equipamento informático?
- Quais as preocupações inerentes para o utilizador, face ao acesso que a organização poderá ter no acesso a dados pessoais contidos nos equipamentos informáticos do utilizador?
- Qual a sua perceção na descrição da política de implementação e uso de *BYOD* da sua organização face à propriedade de dispositivos móveis do utilizador?
- A sua organização providencia aplicações móveis para uso na realização das suas funções de trabalho?
- Até que ponto o utilizador acha mais fácil ou mais difícil aceder às informações da organização através de um dispositivo móvel, comparado com o seu dispositivo de trabalho, providenciado pela organização?
- Como é que a organização comunica as suas políticas de segurança e restrições de uso ao utilizador?

Como contributo e tendo sido já sumariamente abordada a questão da *Cloud Computing Technology*, este princípio, que" assenta no facto de que qualquer computador, ligado a uma rede que permite a ligação a um computador central (servidor de *Cloud Computing*), pode utilizar todos os serviços por ele disponibilizado, podendo os utilizadores armazenar e aceder a ficheiros pessoais, como músicas, fotos, vídeos, *bookmarks*, processar texto e utilizar folhas de cálculo. Tudo isto num servidor remoto a partir do seu computador" (Exército Português, 2011, p. 79) poderá se constituir como a alternativa do futuro. Este conceito vem suprimir todas as dificuldades de compatibilidade entre aplicações e equipamentos, convergindo num só único processo.

O conceito *Cloud Computing* tem como vantagens o requisito da flexibilidade, pois não é necessário equipamento físico para armazenamento de qualquer tipo de dados (o espaço do servidor, após *login* é suficiente), retirando ao utilizador o encargo de transporte e posse de qualquer periférico externo, sendo possível a qualquer utilizador " aceder e

editar informação em qualquer parte do mundo utilizando apenas um computador, um *browser*[50] e uma ligação de dados" (Exército Português, 2011, p. 80).

Ao contrário do *BYOD*, o "*Bring Your Own Cloud*[51] *(BYOC)* " irá defrontar uma maior resistência por parte das organizações. Falhas na gestão de dispositivos portáteis e no controlo dos sistemas informacionais irão constituir-se como reais obstáculos à evolução do *BYOC*, mesmo que esta tendência se revista de inúmeras vantagens.

Com a adoção do conceito do *BYOC*, a informação residente na organização é descentralizada para fora das redes corporativas, criando inúmeros desafios de segurança, residindo esta informação em vários serviços de *Cloud*.

Do ponto de vista da providência de perda de informação o *BYOC* representa um maior desafio de segurança em relação ao *BYOD*, visto que a informação na *Cloud* poderá ser copiada, roubada, duplicada ou, em última análise poderá se perder na rede global que é a internet. (Froehlich, 2014).

No entanto, à semelhança da implementação do conceito *BYOD*, o conceito *BYOC* comporta preocupações atuais e essenciais para o sucesso e rentabilização do mesmo. O desafio da segurança da informação revela-se como primordial, comparativamente à adoção de qualquer conceito e ao amadurecimento da cultura de segurança, nas suas vertentes da segurança física e da segurança pessoal, no que diz respeito às redes corporativas das FA.

[50] "*Browser* é um programa desenvolvido para permitir a navegação pela internet, capaz de processar diversas linguagens" (Significados.com.br, 2012).

[51] *BYOC* – "expressão que define o uso de aplicações pessoais em nuvem pelos funcionários de uma organização, por forma a aumentar a sua competitividade no local de trabalho

Conclusões

"Se tu pensas que a tecnologia pode resolver os teus problemas de segurança, então não compreendes os problemas e não compreendes a tecnologia."

Bruce Schneier, Chief Security Technology Officer, BT

Como já aprofundado no nosso trabalho, em qualquer projeto de tecnologias de informação, a política de implementação deverá preceder a tecnologia. De forma a efetivar a gestão dos equipamentos móveis pessoais e a sua utilização numa determinada organização, existe a necessidade de traçar estas políticas de implementação (Information Technology Experts, 2011, p. 4) .

A implementação do conceito *BYOD* requer uma interatividade no seu processo, tendo implicações ao nível dos recursos humanos, da tecnologia, da legalidade e da segurança. As entidades, quer no setor privado, quer no setor público que adotaram o conceito no seio das suas organizações, relataram que a autorização do uso de equipamentos informáticos particulares resultou, na maioria dos casos num aumento de produtividade e satisfação (Digital Services Advisory Group and Federal Chief Information Officers Council, 2012).

Se a aplicação do conceito *BYOD* e a adoção de políticas de implementação por parte de empresas tem vindo a crescer, sendo uma inevitabilidade no mundo empresarial, a aplicação do conceito em instituições militares, mais concretamente em departamentos de informações está longe de ser uma realidade (Corbin, 2012).

Estejam as estruturas preparadas ou não, o *BYOD* é um conceito que tende a prosperar. Ele irá transformar organizações, aumentar eficiência e produtividade. Isto tudo a um preço, indissociado de risco a ser incluído na equação. No entanto, segundo Kaneshige (2014), até 2016, um em cada cinco programas de *BYOD* não irá ter sucesso devido à implementação de medidas de gestão de equipamentos informáticos demasiado restritivas.

Em consonância com a nossa análise, reforçada com afirmações do analista Van Baker, do Gartner Technology Industries, já é plausível a perceção da deterioração da experiência do utilizador em equipamentos informáticos particulares por conta do mau uso das ferramentas de gestão de dispositivos móveis. Questões relacionadas com má utilização de equipamentos e violações de segurança vão-se constituir como barreiras ao desenvolvimento do *BYOD* (Kaneshige, 2014).

Numa perspetiva de segurança da informação em consonância com o documento, Digital Services Advisory Group and Federal Chief Information Officers Council, 2012, os equipamentos de forma a garantir a integridade da informação que circula nas organizações, deverão ser configurados, implementados com *software* que permita o seu controlo remoto, de forma que em caso de roubo ou perda de informação, esta não seja comprometida[52].

Na implementação da utilização de equipamentos informáticos particulares em redes corporativas, apesar de esta prática reduzir custos, aumentar a eficiência, produtividade e experiência (Digital Services Advisory Group and Federal Chief Information Officers Council, 2012), a temática da segurança reveste-se de capital importância para o sucesso desta experiência. Fruto desta preocupação é o facto de comummente os dispositivos informáticos particulares não serem detentores de aplicações específicas de controlo de acessos e de segurança. Esta falta de especificidades resulta do mediano conhecimento dos utilizadores nesta área (MCS, 2006, p. 6).

O procedimento metodológico deste trabalho apoiou-se em três grandes fases: revisão de literatura (vertentes conceptual e legal); revisão empírica documental (diagnóstico dos principais problemas e disfunções e experiências de outros casos de estudo de implementação da mesma problemática) e avaliação das hipóteses e construção (edificação de um modelo renovado).

Da revisão empírica destacam-se os estudos e relatórios produzidos por entidades privadas e públicas, sendo estas últimas maioritariamente bipartidas em origem, governamental e académica.

Na investigação, de matriz longitudinal, foram utilizadas, sobretudo, metodologias hipotético-dedutivas (investigação no contexto da prova). Os dados recolhidos a partir da exploração documental, em certos casos de experiências de outras organizações foram objeto de uma análise de conteúdo (categorial), como descrito por Bardin (2000).

Os resultados alcançados com o presente estudo aproximam-se do previsto, confirmando as grandes orientações inscritas nas hipóteses de investigação, considerando-se atingido o Objetivo Geral e respondida a Pergunta de Partida previamente definida e que aqui recuperamos:

[52]Permitirá à organização gerir aspetos relacionados com segurança nos equipamentos informáticos, de forma a remotamente limpar qualquer informação sensível.

Que possibilidades as redes corporativas das Forças Armadas oferecem na implementação do conceito *Bring Your Own Device*?

As hipóteses foram avaliadas com base nos dados recolhidos dos vários estudos e relatórios, e posteriormente trabalhados. Da avaliação das hipóteses relevam-se as seguintes conclusões (perspetiva alargada):

A Hip 1 é confirmada:

Os equipamentos informáticos particulares que integram o conceito *Bring Your Own Device,* na ligação às redes corporativas das Forças Armadas, são portáteis e seguros.

Ao caraterizarmos o que entendemos pelos equipamentos a serem incluídos no conceito *BYOD* e quais as suas particularidades concluiu-se que a portabilidade era uma das suas caraterísticas. Estes equipamentos deveriam ter ferramentas que proporcionassem também, segurança física e da informação que poderia circular no seu interior.

A Hip 2 é confirmada:

As atuais redes corporativas classificadas das Forças Armadas não permitem a aplicação do conceito *BYOD*.

Os casos analisados da Digital Services Advisory Group and Federal Chief Information Officers Council (2012) e dos Marine Corps (2013), revelaram que a implementação do conceito *BYOD* não contemplava sistemas onde a informação classificada circulava. À semelhança das redes analisadas nos documentos anteriormente referidos, as redes corporativas das FA revelaram lacunas no domínio do utilizador, mostrando que a aplicação do conceito nas redes classificadas não seria viável.

A Hip 3 é confirmada:

As redes corporativas não classificadas das Forças Armadas na adoção do conceito *BYOD* são interoperáveis, seguras e flexíveis.

O enunciar e consequente identificação das caraterísticas dos requisitos operacionais nos ramos, levou à identificação de certos requisitos comuns e transversais. Assim, o nosso estudo, ao incidir nestes requisitos de flexibilidade, interoperabilidade e segurança, confirmou a hipótese por nós levantada, permitindo-nos identificar agora, nas redes não classificadas, as condições essenciais e indispensáveis para o sucesso da implementação do conceito *BYOD*.

A Hip 4 é confirmada:

As contra medidas, face à exploração das vulnerabilidades pelas ameaças existentes, conseguem ser mitigadas, na adoção do conceito *BYOD* nas redes corporativas das Forças Armadas.

Ao identificar-se quais as ameaças e as vulnerabilidades que poderão existir na implementação do conceito *BYOD*, foram também identificadas as contra medidas a adotar, de forma a mitigar essas ameaças. Foi reconhecido que o uso de *software* específico, *antitrojans*, antivírus, *firewall* e assinaturas digitais, minimizava a ameaça, garantidos os requisitos de segurança essenciais para o uso de equipamentos informáticos particulares nas redes corporativas das FA.

Ao confirmarem-se todas as hipóteses levantadas no início do trabalho de investigação, revelaram-se alguns contributos desta para o conhecimento, materializando-se em considerações de ordem prática, já identificadas no capítulo anterior.

As mais-valias deste estudo centram-se, especialmente, na revisão concetual, no diagnóstico apoiado metodologicamente e na construção do modelo renovado que, partindo dos principais problemas e disfunções, das possibilidades e caraterísticas, das ameaças e vulnerabilidades, integrando vários contributos nacionais e estrangeiros, sugere uma perspetiva integrada e holística de análise e resolução das questões mais relevantes equacionadas na investigação.

É nossa convicção que a implementação do conceito *BYOD* nas redes corporativas nas FA, no qual este trabalho é um pequeno contributo, tem ainda um longo caminho a percorrer, carecendo essencialmente de uma consciência de segurança, transversal aos diferentes ramos.

Bibliografia

Allam & Flowerday, 2010. *A Model to Measure the Maturity of Smartphone Security at Software Consultancies,* África do Sul: Faculty of Management and Commerce of the University of Fort Hare.

Amado, J., 2006. *Hackers - Técnicas de Defesa e de Ataque.* 3ª Edição ed. Lisboa: FCA_Editora de Informática.

Anderson, E., Irvine, C. & Schell, R., 2004. *Subversion as a Threat in Information Warfare,* Estados Unidos da América: Journal of Information Warfare.

Anon., 2007. *Segurança da Informação,* Brasil: s.n.

Anon., 2012. *Security Technologies for mobile and byod,* Moscovo: Kaspersky.

Anon., 2014. *Significados.com.br.* [Online]
Available at: http://www.significados.com.br/hotspot-wifi/
[Acedido em 11 03 2014].

Antonopoulos, A., 2011. *IT Security's Scariest Acronym: BYOD, Bring Your Own Device.* [Online]
Available at: http://www.pcworld.com/article/236727/it_securitys_scariest_acronym_byod_bring_your_own_device.html
[Acedido em 07 11 2013].

Assing, D. & Calé, S., 2013. *Mobile Access Safety- Beyond BYOD.* 1ª Edição ed. Great Britain e United States of America: ISTE Ltd and John Wiley & Sons, Inc..

Avira, 2008. *Definição de spyware e malware.* [Online]
Available at: http://www.computadorseguro.com/definicao-malware-spyware/
[Acedido em 23 04 2014].

Ballagas, R., Rohs, M., Sheridan, J. & Borchers, J., 2005. *BYOD: Bring your Own Device,* s.l.: UBICOMP.

Ballano, M., 2011. *Android Threats Getting Steamy.* [Online]
Available at: http://www.symantec.com/connect/blogs/android-threats-getting-steamy#
[Acedido em 14 04 2014].

Barco, 2014. *Barco Visibly yours.* [Online]
Available at: http://www.barco.com/pt/produtos-e-solu%C3%B5es/projetores
[Acedido em 09 01 2014].

Bardin, L., 2000. *Análise de Conteúdo. Tradução de Luís Antero Reto e Augusto Pinheiro.* Edições 70 ed. Lisboa: s.n.

Booker T. Washington High School, 2011. *BYOD Executive Report,* Washington: s.n.

Canal Tech Corporate, 2013. *BYOD: tendência consolidada mundialmente.* [Online] Available at: http://corporate.canaltech.com.br/noticia/byod/BYOD-tendencia-consolidada-mundialmente/ [Acedido em 14 04 2014].

Cipoli, P., 2012. *Canal Tech Corporate.* [Online] Available at: http://corporate.canaltech.com.br/o-que-e/seguranca/O-que-e-Engenharia-Social/ [Acedido em 14 04 2014].

Citrix, 2013. *U.S. Department of Defense: Defense Logistics Agency (DLA) achieves unmatched agility through telework and BYOD strategy,* Bethesda: citrix.com/USgovernment.

Convergência Digital, 2013. *BYOD: funcionários admitem violar regras de segurança para acesso à nuvem.* [Online] Available at: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=35439&sid=18#.U0xnM-leHIV [Acedido em 15 04 2014].

Convergência Digital, 2013. *Faltam profissionais para lidar com BYOD, nuvem e ferramentas sociais.* [Online] Available at: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=35641&sid=16#.U0xyg-leHIW [Acedido em 16 04 2014].

Corbin, K., 2012. *Cloud and BYOD Security Concerns Make Military and Intelligence Agencies Hesitate.* [Online] Available at: http://www.cio.com/article/719640/Cloud_and_BYOD_Security_Concerns_Make_Military_and_Intelligence_Agencies_Hesitate [Acedido em 04 março 2014].

Coviello, A., 2014. *Segurança da informação: 5 previsões para 2014, segundo a RSA.* [Online]
Available at: http://computerworld.com.br/seguranca/2014/03/03/seguranca-da-informacao-5-previsoes-para-2014-segundo-a-rsa/
[Acedido em 15 04 2014].

Deng, J., Su, X. & Wang, J., 2014. *Huawey BYOD Security Solution.* [Online]
Available at: http://enterprise.huawei.com/topic/byod_en/
[Acedido em 11 03 2014].

Digital Services Advisory Group and Federal Chief Information Officers Council, 2012. *The White House - Digital Government.* [Online]
Available at: http://www.whitehouse.gov/digitalgov/bring-your-own-device
[Acedido em 06 03 2014].

European Commission, 2013. *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union,* Bruxelas: European Commission.

Exército Português, 2003. *RAD 280-1- Segurança da Informação armazenada, processada ou transmitida nos sistemas de informação,* Lisboa: Ministério da Defesa Nacional.

Exército Português, 2009. *PDE 2.00- Informações, contra-informação e segurança.* Lisboa: MDN.

Exército Português, 2011. Cloud Computing. *Dragões d´Entre Douro e Minho,* julho, pp. 79-80.

Exército Português, 2012. *Plano de implementação do Sistema de Informação e Comunicações Operacional,* Lisboa: Ministério da Defesa Nacional.

Exército Português, 2013. *PDE 00-25-00 Instruções de Segurança Militar do Exército Português,* Lisboa: Ministério da Defesa Nacional.

Força Aérea Portuguesa, 2009. *PDSIFA - Plano Diretor de Sistemas de Informação da Força Aérea,* Lisboa: Ministério da Defesa Nacional.

Froehlich, A., 2014. *Prepare-se para barrar o BYOC.* [Online]
Available at: http://www.itforum365.com.br/noticias/detalhe/1/prepare-se-para-barrar-o-byoc
[Acedido em 15 04 2014].

Grim, N., 2013. *Defense Systems.* [Online]
Available at: http://defensesystems.com/Articles/2013/07/26/Marine-Corps-mobile-device-strategy.aspx?Page=2
[Acedido em 21 fevereiro 2014].

Hayes, B. & Kotwica, K., 2013. *Bring your own device (BYOD) to work - Trend Report,* Oxford: Security Executive Council.

Information Technology Experts, 2011. *Top 10 Things you should know about managing BYOD´s,* Boston: nskinc.

Intel, s.d. *Processador Intel Celeron.* [Online]
Available at: http://www.intel.com.br/content/www/br/pt/processors/celeron/celeron-processor.html
[Acedido em 23 04 2014].

IT Web, 2014. *BYOD representa ameaça à segurança para 60% das empresas na América Latina.* [Online]
Available at: http://itweb.com.br/111377/byod-representa-ameaca-a-seguranca-para-60-das-empresas-na-america-latina/
[Acedido em 15 04 2014].

Kaneshige, T., 2014. *Uso excessivo de recursos MDM pode matar o BYOD.* [Online]
Available at: http://cio.com.br/gestao/2014/03/25/uso-excessivo-de-recursos-mdm-pode-matar-o-byod/
[Acedido em 15 04 2014].

Kaspersky Lab's, 2013. *Exclusive 2013 Survey Results. IT Security.Fighting the silent threat.A global report into business attitudes and opinions on IT security.,* Boston: Kaspersky Lab's.

Kizza, J. M., 2013. *Guide to Computer Network Security.* 2ª Edição ed. Tennessee,USA: Springer.

LetMobile, 2012. *Securing Corporate Email on Personal Mobile Devices,* EUA: LetMobile.

Marine Corps, 2013. *Commercial Mobile Device Strategy,* Washington: Headquarters, U.S., Marine Corps.

Marinha, 2005. *PCA 2 - Doutrina para os sistemas de informação e comunicação automatizados (SICA) na Marinha,* Lisboa: Ministério da Defesa Nacional.

Marinha, 2008. *PCA 15- Doutrina para a Intranet e a Internet na Marinha,* Lisboa: Ministério da Defesa Nacional.

Marinha, 2012. *PCA 12 (A) - Conceito de Implementação dos Sistemas de Informação e Comunicação Automatizados (SICA) no domínio da rede,* Lisboa: Ministério da Defesa Nacional.

MCS, T., 2006. *Segurança Informática,* Brasil: s.n.

NATO, 2008. *AAP-6 NATO Glossary of terms and definitions,* s.l.: NATO.

Nunoo, E. M., 2013. *Master´s Thesis Smartphone Information Security Risks - Portable Devices and Workforce Mobility,* Suécia: Luleå University of Technology.

Priberam, 2013. *Priberam dicionário.* [Online]
Available at: http://www.priberam.pt/dlpo/port%C3%A1til
[Acedido em 17 04 2014].

Priberam, 2013. *Priberam dicionário.* [Online]
Available at: http://www.priberam.pt/dlpo/hacker
[Acedido em 23 04 2014].

Quivy, R. & Campenhoudt, L. V., 2008. *Manual de Investigação em Ciências Sociais.* 2ª ed. Lisboa: Gradiva.

Santos, J. L. A. d., 2011. *Contributos para uma melhor governação da cibersegurança em Portugal,* Lisboa: Universidade Nova de Lisboa.

School Technology Branch, 2012. *Bring Your Own Device:A Guide for Schools,* ALBERTA : Alberta Education Cataloguing.

Significados.com.br, 2012. *Significado de Browser.* [Online]
Available at: http://www.significados.com.br/browser/
[Acedido em 23 04 2014].

Silva, P., 2013. *White paper- BYOD 2.0: Moving Beyond MDM,* Seattle: F5 Networks, Inc..

Singh, J., 2013. *4 Keys to Creating a BYOD Program.* [Online]
Available at: http://www.securitymagazine.com/articles/84771-keys-to-creating-a-byod-program
[Acedido em 26 março 2014].

Smith, G., 2012. *TechRepublic.* [Online]
Available at: http://www.techrepublic.com/blog/10-things/10-myths-of-byod-in-the-enterprise/3049/
[Acedido em 26 março 2014].

Smith, L. C. N., Burke, M. C. & King, M. J., 2013. *Small Wars Journal.* [Online]
Available at: http://smallwarsjournal.com/jrnl/art/abort-retry-fail-fixing-army-software
[Acedido em 25 março 2014].

St Bede´s College, 2014. *Recommended Specification for the BYOD Programme,* Nova Zelândia: St Bede´s College.

Tailândia, P., 2012. *As Redes Sociais mais famosas de 2012, você conhece todas?.* [Online]
Available at: http://portaltailandia.com.br/tecnologia-tai/internet/as-redes-sociais-mais-famosas-de-2012-voce-conhece-todas/
[Acedido em 10 01 2014].

Taurion, C., s.d. *Pequenas e Médias Empresas - Soluções de Negócios: BYOD (Bring your Own Device) na prática.* [Online]
Available at:
http://www.ibm.com/midmarket/br/pt/articles_byod_como_comecar.html
[Acedido em 02 10 2013].

Technet Library, 2005. *Windows Server.* [Online]
Available at: http://technet.microsoft.com/pt-BR/library/cc782833(v=ws.10).aspx
[Acedido em 27 02 2014].

Techopedia, 2014. *Techopedia.* [Online]
Available at: http://www.techopedia.com/definition/24967/ieee-80211
[Acedido em 02 03 2014].

Unit, E. I., 2013. *The personalisation challenge - Business culture and mobile security,* s.l.: The Economist.

US Army, 2009. *FM 6-02.43 - Signal Soldiers Guide,* Washington: Department of the Army.

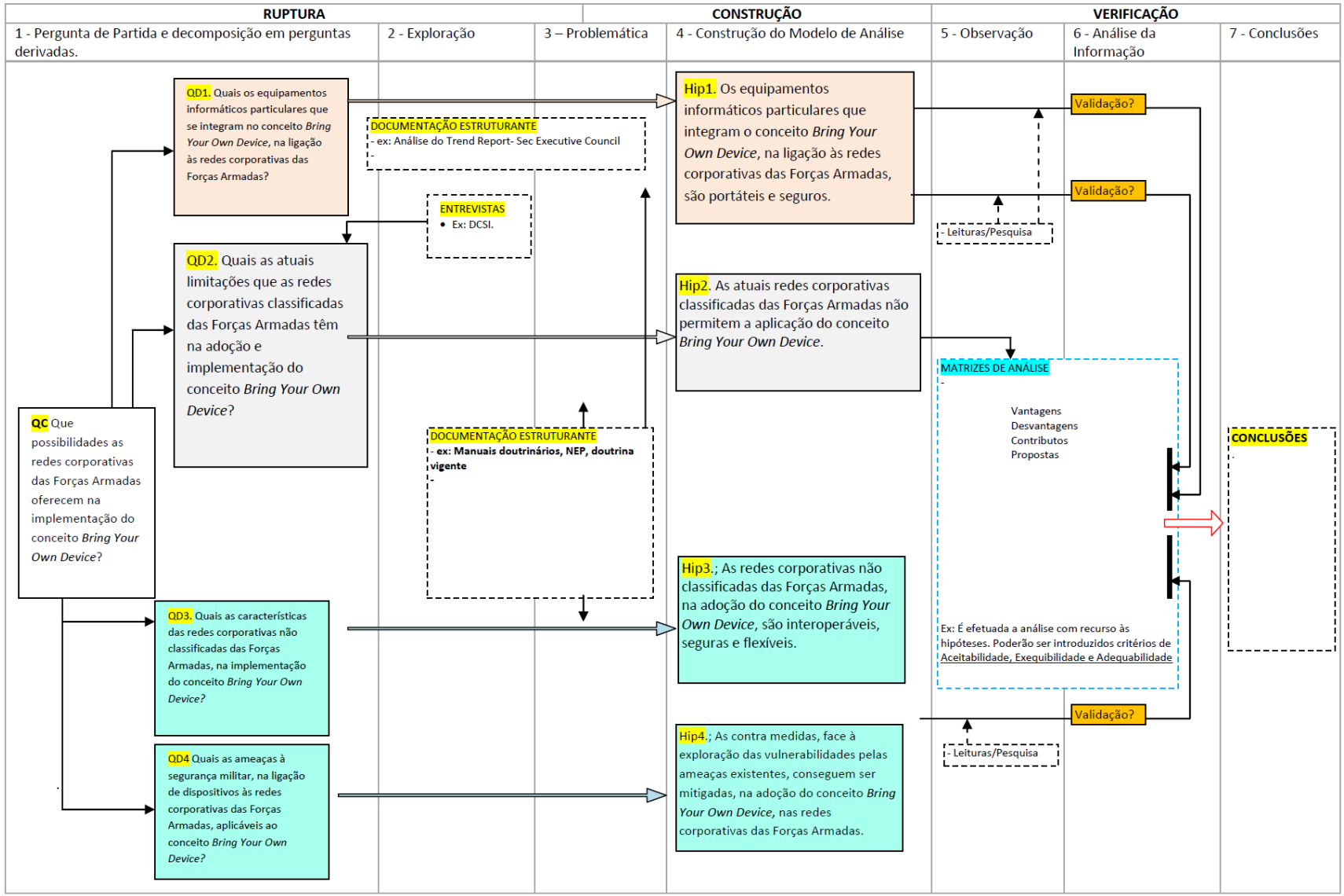
Vmware, 2013. *The BYOD Opportunity,* Califórnia: s.n.

Walczak, M., 2013. *The Bring Your Own Device (BYOD) movement is catching on..* [Online]
Available at: http://blog.getbase.com/bring-your-own-device-trend
[Acedido em 07 11 2013].

WatchGuard, 2013. *BYOD: Bring Your Own Device-or Bring Your Own Danger?,* Seattle: WatchGuard Technologies.

Whitman, M. & Mattord, H., 2011. *Principles of Information Security.* 4ª Edição ed. Boston: Cengage Learning.

Apêndice 1 – Percurso metodológico



Apêndice 2 – Modelo concetual da investigação

Pergunta Derivada 1 –Quais os equipamentos informáticos particulares que se integram no conceito *bring your own device,* na ligação às redes corporativas das Forças Armadas?

Hipótese 1- – Os equipamentos informáticos particulares que integram o conceito Bring Your Own Device, na ligação às redes corporativas das Forças Armadas, são portáteis e seguros.

CONCEITOS	DIMENSÕES	INDICADORES	INSTRUMENTOS DE OBSERVAÇÃO
C1 – *Bring your own device (BYOD)*	**D1.1**- Tecnológica **D1.2**- Humana	**ID1.1.1**- Visor, monitor **ID1.1.2**- Teclado **ID1.1.3**- Capacidade de conetividade **ID1.1.4**- Capacidade de processamento **ID1.2.1**- Utilização individual (intransmissível)	Documentação estruturante
C2- Portabilidade	**D2.1**- Tecnológica **D2.2**- Humana	**ID2.1.1**- Peso **ID2.2.1**- Transporte (1 pessoa) **ID2.2.2**- Utilização individual	
C3- Segurança	**D3.1**- Informação **D3.2**- Física **D3.3**-Pessoal **D3.4**-Informática	**ID3.1.1**- Classificação de Segurança da informação **ID3.2.1**- Acesso a instalações **ID3.2.2**- Tentativas de intrusão **ID3.2.3**- Número falhas de segurança **ID3.3.1**- Credenciação de Segurança **ID3.4.1**- *Hardware & Software* seguros	Documentação estruturante Relatórios de Segurança
C4- Redes Corporativas	**D4.1**- Tecnológica **D4.2**- Física	**ID4.1.1**- Número e tipo de equipamentos ligados entre si **ID4.1.2**- Programas instalados **ID4.1.3**- Programas partilhados **ID4.2.1**- Ligações a outros equipamentos de organizações diferentes	Documentação estruturante

Pergunta Derivada 2 – Quais as atuais limitações que as redes corporativas classificadas das Forças Armadas têm na adoção e implementação do conceito Bring Your Own Device?

Hipótese 2- As atuais redes corporativas classificadas das Forças Armadas não permitem a aplicação do conceito Bring Your Own Device.

CONCEITOS	DIMENSÕES	INDICADORES	INSTRUMENTOS DE OBSERVAÇÃO
C1 – Redes Corporativas classificadas	**D1.1**- Tecnológica **D1.2-** Física **D1.3-** Segurança	**ID1.1.1-** Número equipamentos ligados entre si **ID1.1.2-** *Software* instalado **ID1.2.1-** Ligação de equipamentos a outras organizações **ID1.3.1-**Classificação de Segurança da informação **ID1.3.2-** Acesso a instalações **ID1.3.3-** Tentativas de intrusão **ID1.3.4-** Número falhas de segurança (relatórios de segurança) **ID1.3.5-** Credenciação de Segurança **ID1.3.6-** *Hardware & Software* seguros	Documentação estruturante Relatórios técnicos
C2- Aplicabilidade (*byod*)	**D2.1**- *Software* **D2.2-** *Hardware*	**ID2.1.1**- Programas que permitem a ligação entre equipamentos **ID2.2.1**- Equipamentos que permitem ligação física às redes **ID2.2.2**- Equipamentos que permitem ligação às redes (sem fios)	
C3- Permissão (autorização)	**D3.1**- Humana **D3.2**- Material **D3.3**-Informação	**ID3.1.1**- Credenciação de Segurança (homem) **ID3.2.1-** Classificação das redes (classificada, não classificada) **ID3.3.1-** Classificação de segurança da informação	

Pergunta Derivada 3 – Quais as características das redes corporativas não classificadas das Forças Armadas, na implementação do conceito Bring Your Own Device?

Hipótese 3- As redes corporativas não classificadas das Forças Armadas, na adoção do conceito Bring Your Own Device, são interoperáveis, seguras e flexíveis.

CONCEITOS	DIMENSÕES	INDICADORES	INSTRUMENTOS DE OBSERVAÇÃO
C1 – Interoperabilidade	**D1.1**- Tecnológica **D1.2-** Física **D1.3-** Semântica	**ID1.1.1-** Ligações existentes entre equipamentos **ID1.2.1-** As organizações militares (FA) têm os seus equipamentos ligados entre si **ID1.3.1-** Os documentos são partilhados	Documentação estruturante
C2- Segurança	**D2.1**- Informação **D2.2**- Física **D2.3**-Pessoal **D2.4**-Informática	**ID2.1.1**- Classificação de Segurança da informação **ID2.2.1-** Acesso a instalações **ID2.2.2-** Tentativas de intrusão **ID2.2.3-** Número falhas de segurança (relatórios de segurança) **ID2.3.1-** Credenciação de Segurança **ID2.4.1-** *Hardware & Software* seguros	Documentação estruturante Relatórios de Segurança
C3- Flexibilidade	**D3.1**- Tecnológica **D3.2**- Utilização	**ID3.1.1**- Ligação entre equipamentos rápida e intuitiva, *software* 3G/4G **ID3.2.1-** "O saber" do utilizador, o dono do equipamento *byod* tem formação que lhe permite a ligação às redes	Entrevista exploratória (Direção Comunicação e Sistemas de Informação)
C3- Redes corporativas não classificadas	**D3.1**- Tecnológica **D3.2**- Física **D3.3**-Segurança	**ID3.1.1**-Número equipamentos ligados entre si **ID3.1.2-** *Software* instalado **ID3.2.1-** Ligação de equipamentos a outras organizações **ID3.3.1-**Classificação de Segurança da informação **ID3.3.2-** Acesso a instalações **ID3.3.3-** Tentativas de intrusão **ID3.3.4-** Número falhas de segurança (relatórios de segurança) **ID3.3.5-** Credenciação de Segurança	Documentação estruturante Relatórios de Segurança

Pergunta Derivada 4 – Quais as ameaças à segurança militar, na ligação de dispositivos às redes corporativas das Forças Armadas, aplicáveis ao conceito Bring Your Own Device?

Hipótese 4- As contra medidas, face à exploração das vulnerabilidades pelas ameaças existentes, conseguem ser mitigadas, na adoção do conceito Bring Your Own Device, nas redes corporativas das Forças Armadas.

CONCEITOS	DIMENSÕES	INDICADORES	INSTRUMENTOS DE OBSERVAÇÃO
C1 – Contra medidas	**D1.1**- *Software* **D1.2-** Humana **D1.3-** *Hardware*	**ID1.1.1-** Programas que previnam ataques informáticos **ID1.2.1-** Autorização para acesso à informação e equipamentos **ID1.3.1-** Classificação de Segurança ao material, aplicável ao conceito *byod*	Documentação estruturante
C2- Vulnerabilidades	**D2.1**- Informática **D2.2**- Organização **D2.3**-Pessoal	**ID2.1.1**- Falhas (*bugs)* no *software* **ID2.2.1-** Acesso a locais (autorização a áreas classificadas) **ID2.2.2-** Falta de credenciação(processos de credenciação por número de militares com acesso a redes informáticas)	Relatórios de Segurança internos
C3- Ameaças	**D3.1**- Informática – *on line* **D3.2**- Humana **D3.3-** Informação	**ID3.1.1**- Ataques informáticos internos a dispositivos **ID3.1.2-** Ataques informáticos externos a dispositivos **ID3.1.3**- Ataques informáticos internos às redes corporativas das Forças Armadas **ID3.1.4**- Ataques informáticos externos às redes corporativas das Forças Armadas **ID3.2.1**- Existência de autorização de acesso a dados com informação classificada **ID3.3.1**- Fugas de informação da organização (Ex. blogs, portais sociais,…)	

Apêndice 3 – Modelo de Análise