ACADEMIA DA FORÇA AÉREA

A Segurança Computacional como fator de alinhamento entre Planos Organizacionais

Vasco Manuel Fernandes Lampreia

Aspirante a Oficial-Aluno Piloto-Aviador 138102-E

Dissertação para obtenção do Grau de Mestre em
Aeronáutica Militar

Especialidade de Piloto-Aviador

Júri

Presidente:	MGen/PilAv Manuel Fernando Rafael Martins/ Força Aérea
Orientador:	Prof. Doutor José Manuel Nunes Salvador Tribolet/ IST
Coorientador:	TCor/EngInf José Manuel António Gorgulho/ Força Aérea
Vogal:	Cor/PilAv Paulo Jorge Neves Ropio/ Força Aérea

Sintra, junho de 2016

ACADEMIA DA FORÇA AÉREA

A Segurança Computacional como fator de alinhamento entre Planos Organizacionais

Vasco Manuel Fernandes Lampreia

Aspirante a Oficial-Aluno Piloto-Aviador 138102-E

Dissertação para obtenção do Grau de Mestre em
Aeronáutica Militar, na Especialidade de Piloto-Aviador

Júri

Presidente:	Major-General Manuel Fernando Rafael Martins/ Força Aérea
Orientador:	Professor Doutor José Manuel Nunes Salvador Tribolet/ IST
Coorientador:	Tenente-Coronel José Manuel António Gorgulho/ Força Aérea
Vogal:	Coronel Paulo Jorge Neves Ropio/ Força Aérea

ISBN:

Sintra, junho de 2016

Este trabalho foi elaborado com finalidade essencialmente escolar, durante a frequência do Curso de Pilotagem Aeronáutica cumulativamente com a atividade escolar normal. As opiniões do autor, expressas com total liberdade académica, reportam-se ao período em que foram escritas, mas podem não representar doutrina sustentada pela Academia da Força Aérea

Agradecimentos

À Força Aérea,

Pela oportunidade que me deu de representar uma instituição de tamanho prestígio e da qual me orgulho como militar.

À Academia da Força Aérea

Pela formação, condições, conhecimento e vivências, pelos bons momentos mas também pelas dificuldades, que me deram a oportunidade de ser uma melhor pessoa.

Aos meus pais,

Por tudo, em particular pelo apoio e paciência, e pela educação e valores que fizeram de mim a pessoa que sou hoje.

À minha irmã,

Por ser a pioneira, pela ajuda e compreensão.

Aos Mustangs

Pela camaradagem e pelos momentos vividos pois são essas memórias que levo comigo para a vida.

Ao Dias,

Meu companheiro nesta viagem académica e pelas inúmeras incertezas que passámos.

Ao Sr. Tenente-Coronel José Gorgulho

Pela disponibilidade para a orientação e pelas dúvidas que me colocou e fizeram pensar.

Ao Sr. Coronel Carlos Páscoa

Pelo rigor e exigência, pela orientação fornecida que permitiu encaminhar esta dissertação para um bom porto.

A todos vós,

Obrigado!

Resumo

Com esta dissertação de mestrado pretende-se chegar a um modelo que permita alinhar os diferentes planos organizacionais de uma organização ou de um domínio pertencente a esta.

A metodologia utilizada na condução desta dissertação foi proposta por Raymond Quivy e LucVan Campenhoudt. Esta ajuda o autor e o leitor, a acompanhar gradualmente o desenvolvimento através das várias fases que a metodologia prevê.

Para garantir a coerência de um modelo é necessário um estudo prévio do tema em questão, por este motivo foi necessária uma revisão bibliográfica que abrangesse: os conceitos mais generalistas da área de engenharia organizacional, a linguagem e termos técnicos da segurança computacional, o estado atual da problemática da segurança de informação na Força Aérea e possíveis modelos que poderiam revelar-se úteis no desenvolvimento do objetivo desta dissertação como o *Bussiness Motivation Model.*

Durante o desenvolvimento do modelo surgiu a necessidade de definir o conceito de «Plano Organizacional» pois este estava pouco explorado na comunidade científica e fazia parte integrante do tema desta dissertação, definindo-o como tendo um conjunto de atributos que o identifica e universais a qualquer plano da organização. Identificados os atributos dos planos organizacionais foi possível concluir quais os fatores de alinhamento entre eles, a partir deste ponto surgiu a proposta de modelo capaz satisfazer o objetivo desta dissertação.

A validação é atingida através de uma instanciação do modelo no domínio da segurança computacional na Força Aérea, com algumas propostas de alinhamento.

No último capítulo é feita uma revisão de todo o trabalho, destacando alguns pontos mais importantes e possibilitando assim ao leitor terminar com uma visão global de toda a dissertação.

Palavras-chave: Alinhamento; Planos Organizacionais; Segurança Computacional; Business Motivation Model.

Abstract

The aim of this dissertation is to build a model that allows to align the different organizational plans of an organization or a domain belonging to one.

The methodology used in conducting this dissertation was proposed by Raymond Quivy and LucVan Campenhoudt. This helps the author and the reader, to gradually follow the development through the various stages of the dissertation.

To ensure the consistency of a model, it was required a prior study of the subject in question, for this reason a literature review was mandatory covering themes as: the more general concepts of organizational engineering, language and technical terms of computer security, the current state the information security in the Air Force and models that could prove useful in the development of the objective of this dissertation as Business Motivation Model.

During the model development it became necessary to define the concept of «Organizational Plan» because this was little explored in the scientific community and was an integral part of the theme of this work, defining it as having a set of attributes that identifies it and makes it universal to any organizational level. Having identified the attributes of the organizational plans it was possible to deduct the factors of alignment among them. From this point on a model able to meet the objective of this dissertation was proposed.

The validation was achieved through an instantiation of the model in the field of computer security in the Air Force, with the proposal of some alignment factors that were missing.

In the last chapter a review of the dissertation is made, highlighting some main points making it possible for the reader to have a general overview of all the dissertation.

Key-words: Alignment; Organizational Plans; Computational Security; Business Motivation Model.

Índice

Índice de Figuras

Índice de Tabelas

Lista de Acrónimos

AE	Arquitetura Empresarial
BMM	*Business Motivation Model*
CA	Comando Aéreo
CLAFA	Comando da Logística da Força Aérea
CPESFA	Comando de Pessoal da Força Aérea
EMFA	Estado-Maior da Força Aérea
EMGFA	Estado Maior General das Forças Armadas
EO	Engenharia Organizacional
FA	Força Aérea
OSA	Organizational Self-Awareness
PDSI	Plano Diretor dos Sistemas de Informação
PEMGFA	Publicação do Estado Maior General das Forças Armadas
PI	Plano Inferior
PS	Plano Superior
RFA	Regulamento da Força Aérea
SI	Sistemas de Informação
SIC	Sistemas de Informação e Comunicação

Glossário

Alinhamento	Nível de coerência entre dois conceitos *(PEREIRA;* et al.*, 2005)*
Ameaça	Potencial causa de um incidente no qual pode resultar danos a um sistema ou organização *(Iso.org, 2015)*.
Ataque Computacional	Tentativa de destruir, expor, alterar, roubar ou aceder sem autorização aos recursos da empresa *(Iso.org, 2015)*.
BMM	Ferramenta que disponibiliza um esquema para ajudar ao desenvolvimento, comunicação e gestão dos planos de negócio de uma forma organizada *(Business Rules Group, 2015)*.
OSA	Compreende duas dimensões principais, uma individual e outra organizacional. Refere-se à capacidade dos colaboradores conhecerem o seu papel na organização e a perceção da organização sobre os seus membros, recursos e procedimentos *(VICENTE; TRIBOLET, 2007)*.
Ontologias	Conjunto de termos e conceitos que definem o modelo de negócio da organização *(PÁSCOA,* et al., *2011)*.
Segurança Computacional	Define-se como a proteção conferida a um sistema de informação, a fim de atingir os objetivos aplicáveis à preservação da integridade, disponibilidade e confidencialidade dos recursos do sistema de informação *(NIST, 1995)*.
Vulnerabilidade	Uma fraqueza em qualquer recurso ou sistema de controlo da empresa que pode ser explorada por uma ou mais ameaças *(Iso.org, 2015)*.

1 Introdução

O *Boom* a que assistimos nas últimas décadas na área da informação e dos meios de comunicação, sobretudo devido à Internet, veio modificar completamente o desenrolar dos processos nas organizações, tornando-os muito mais rápidos e eficientes. Consequentemente as organizações tornaram-se altamente dependentes da disponibilidade, fiabilidade e integridade dos sistemas de informação, o que aumentou a sua vulnerabilidade e exposição ao risco (BERNARDINO, 2012).

Esta transformação revela a necessidade de alinhamento das empresas atuais em todo o seu domínio, a falta de alinhamento conduz a fragilidades que as organizações atuais, devido à enorme concorrência, não se podem dar ao luxo de ter e esta falta de alinhamento é salientada quando se percorre os diversos planos organizacionais.

Uma das áreas onde este aspeto é mais crítico é na segurança computacional pois, enquanto que para proteger documentos em papel bastavam quatro paredes bem guardadas, atualmente a segurança computacional tornou-se exponencialmente mais complexa, o número de perigos aumentou para níveis tais que por vezes nem é possível conhecer a própria ameaça (BERNARDINO, 2012).

Deve ser destacado que apesar do título desta dissertação se referir à segurança computacional, este domínio será apenas utilizado para fazer a validação do modelo, ou seja, o principal contributo deste trabalho é a proposta de um modelo de alinhamento universal, capaz de ser aplicado a qualquer domínio.

1.1 Motivação e Problemática

"Conhece-te a ti e ao inimigo e, em cem batalhas que sejam, nunca correrás perigo"

(SunTzu)

O panorama atual é caraterizado por uma grande incerteza económica que conduz a uma maior exigência de gestão. Dada a forte contenção orçamental, um planeamento criterioso e a alocação dos recursos reveste-se de especial importância para atingir levados níveis de eficiência (Força Aérea Portuguesa, 2015).

A «Defesa 2020» provem de uma Resolução do Conselho de Ministros e é um documento estruturante com vista à transformação das Forças Armadas para operarem com sustentabilidade, com recursos otimizados e para o aumento de eficiência (Ministério da Defesa Nacional, 2013).

Este documento expressa preocupações como: “Realinhar mecanismos de articulação e coordenação entre o EMGFA, os Ramos das Forças Armadas e os serviços centrais do Ministério da Defesa Nacional” e “Eliminar as duplicações de tarefas exercidas no contexto funcional dos serviços centrais do Ministério da Defesa Nacional” (Ministério da Defesa Nacional, 2013).

Através destes exemplos que comprovam a necessidade que melhorar o alinhamento das Forças Armadas compreende-se a importância desta dissertação que faz assim todo o sentido no panorama económico atual.

Genericamente falando, em qualquer organização, a ambição pela eficiência é uma meta a atingir. A par da eficiência, na teoria de engenharia organizacional, o alinhamento entre os diferentes planos organizacionais têm também uma elevada importância e é frequentemente objeto de estudo.

Concluindo, torna-se evidente a necessidade da escolha de um modelo holístico capaz de satisfazer as necessidades das organizações atuais, garantindo que não fica esquecida nenhuma componente, e que seja universal a todos os planos organizacionais para garantir o alinhamento e a eficiência da organização.

A problemática para esta dissertação fica assim evidente: inexistência de um modelo que garanta o alinhamento entre os vários planos organizacionais de um domínio.

1.2 Objetivo

Com esta dissertação de mestrado pretende-se chegar a um modelo que permita alinhar os diferentes planos organizacionais de uma empresa ou domínio desta, utilizando para isso o domínio da segurança computacional como domínio de instanciação, e assim analisar se na FA existe doutrina suficiente sobre este tema, identificar as falhas na aplicação do modelo e possivelmente propor algumas alterações.

1.3 Âmbito

O âmbito deste trabalho situa-se na Força Aérea e é transversal a todos os planos organizacionais. A abordagem à segurança computacional, no momento da validação, será efetuada utilizando os conhecimentos de Engenharia Organizacional.

1.4 Metodologia

A metodologia adotada para a realização desta dissertação foi proposta por Raymond Quivy e LucVan Campenhoudt no seu “Manual de Investigação em Ciências Sociais” e, tal como demonstrado na figura seguinte, está dividido em três atos e sete etapas:

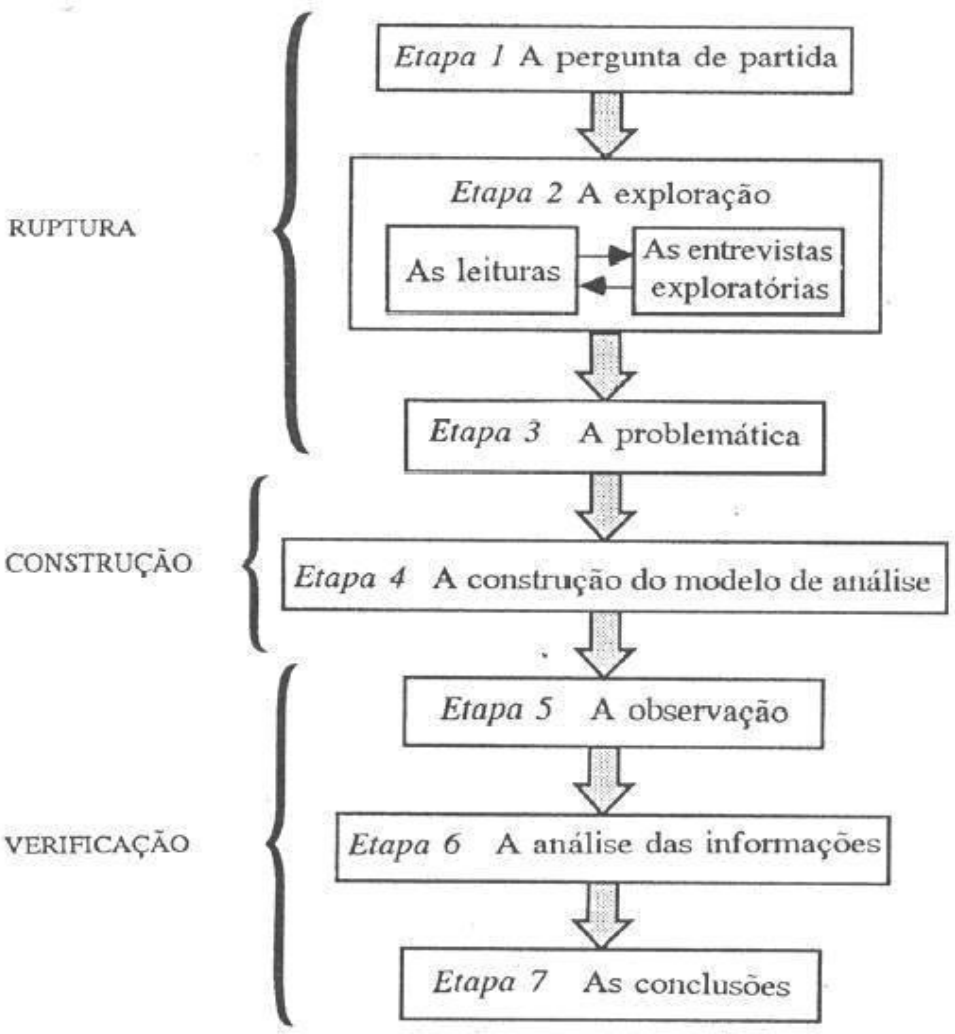


Figura 1 – Método de investigação (QUIVY; CAMPENHOUDT, 1998)

Na rutura pretende-se despir qualquer preconceito ou ideias pré concebidas sobre o tema para iniciar a abordagem a este de mente aberta, sendo por esse mesmo motivo o primeiro ato do procedimento científico (QUIVY; CAMPENHOUDT, 1998).

Na construção é suposto erguer as proposições explicativas do fenómeno a estudar, prever o plano de pesquisa a seguir e construir um modelo aplicável à investigação (QUIVY; CAMPENHOUDT, 1998).

Por fim, na verificação, para uma proposição adquirir o estatuto de científica, deve ser verificada por testes e factos, esse processo corresponde ao último ato do procedimento (QUIVY; CAMPENHOUDT, 1998).

As sete etapas elaboradas pelos autores, que estão representadas na figura acima, são:

- A **pergunta de partida** que deve resumir o projeto de investigação em forma de pergunta.
- A **exploração** que consiste, por exemplo, nas leituras e entrevistas exploratórias. Tem como objetivo proporcionar o primeiro contacto com o problema.
- A **problemática** que consiste na forma como se aborda o problema representado na pergunta de partida.
- A **construção do modelo de análise** que é caracterizada pela tradução dos dados adquiridos na fase exploratória para um modelo que permita ser trabalhado e analisado.
- A **observação** que é o momento de validar o modelo de análise confrontando-o com os dados observados no mundo.
- A **análise das informações** é a fase em que se verifica se as hipóteses colocadas através das perguntas derivadas são verdadeiras ou falsas.
- As **conclusões,** por fim, permitem obter uma linha de pensamento ampla e generalista, especificando concretamente o conhecimento adquirido com a elaboração do trabalho de investigação.

1.5 Questões e Hipóteses

1.5.1 Questão de Partida

A pergunta de partida pretende resumir a investigação e explicá-la de forma sucinta, sendo que dela poderão derivar algumas questões e hipóteses. A pergunta de partida identificada para esta dissertação foi a seguinte:

Q0 - Até que ponto é possível identificar um modelo na FA que permita o alinhamento de processos nos diferentes planos organizacionais?

1.5.2 Questões Derivadas

Para ajudar na investigação, a pergunta de partida foi decomposta noutras questões derivadas e respetivas hipóteses.

Q1 – Existe na Força Aérea um modelo holístico sobre a segurança computacional?

H1 – Não existe um modelo holístico, apenas alguma doutrina, em determinadas áreas de maior interesse, que pode ser utilizada para construir um modelo mais abrangente.

Q2 – O *Business Motivation Model* pode ser um modelo que permite modelar qualquer organização ou parte dela, promovendo o alinhamento entre os vários planos organizacionais?

H2.1 – É possível utilizar o BMM para modelar corretamente qualquer organização, limitando assim a existência de falhas não previstas.

H2.2 – Devido à especificidade de determinados modelos de negócio, o BMM não pode ser aplicado universalmente.

1.6 Panorâmica

Esta dissertação pretende que o leitor acompanhe gradualmente o pensamento do investigador no momento da investigação e para isso está construída sequencialmente em quatro capítulos.

O primeiro capítulo consiste na “Introdução”, onde o leitor terá a abordagem inicial ao tema com o objetivo, o âmbito e a metodologia utilizada na elaboração do

trabalho é também neste capítulo que o leitor terá conhecimento da pergunta de partida e respetivas questões derivadas e hipóteses.

O segundo capítulo, “Revisão da Literatura”, levará o leitor a interiorizar os conceitos teóricos fundamentais do tema para mais facilmente compreender o resto da dissertação. Estes fundamentos, que são o suporte da investigação, foram realizados através de pesquisa e das aulas lecionadas na cadeira de Engenharia Organizacional.

No terceiro capítulo, o leitor poderá encontrar o trabalho desenvolvido durante a investigação em busca das respostas às perguntas e problemas apresentados inicialmente.

Finalmente, o último capítulo, “Conclusões e Recomendações”, apresenta ilações retiradas da investigação bem como as recomendações propostas para a Força Aérea e para o desenvolvimento de futuros trabalhos.

2 Revisão da Literatura

2.1 Empresa/Organização

Uma empresa/organização consiste em qualquer coleção de organizações com um conjunto de objetivos e/ou uma linha estratégica comuns. Pode ser uma agência governamental, uma empresa, um departamento ou ainda uma cadeia de várias organizações separadas geograficamente mas interligadas por uma gerência comum. O termo «Empresa» no contexto da arquitetura empresarial pode ser utilizado para definir tanto a empresa toda como um domínio específico dentro desta. Em ambos os casos a arquitetura expressa as conexões entre os diferentes grupos e níveis organizacionais dentro da empresa (The Open Group, 2015).

Entenda-se «coleção de organizações» como a soma das partes que resulta numa empresa. Apesar de cada parte cumprir a sua função individualmente, esta ação singular deve ter sempre em vista o rumo da empresa e os seus objetivos estratégicos (The Open Group, 2015).

No âmbito desta dissertação os termos «empresa» e «organização» vão ser usados com o mesmo significado.

2.1.1 Caraterísticas da organização da Força Aérea

Segundo Páscoa et al (2011), a organização é constituída por duas grandes áreas, entidade organizacional e posição organizacional, cada uma destas áreas é caracterizada por atributos tal como demonstra o esquema seguinte:

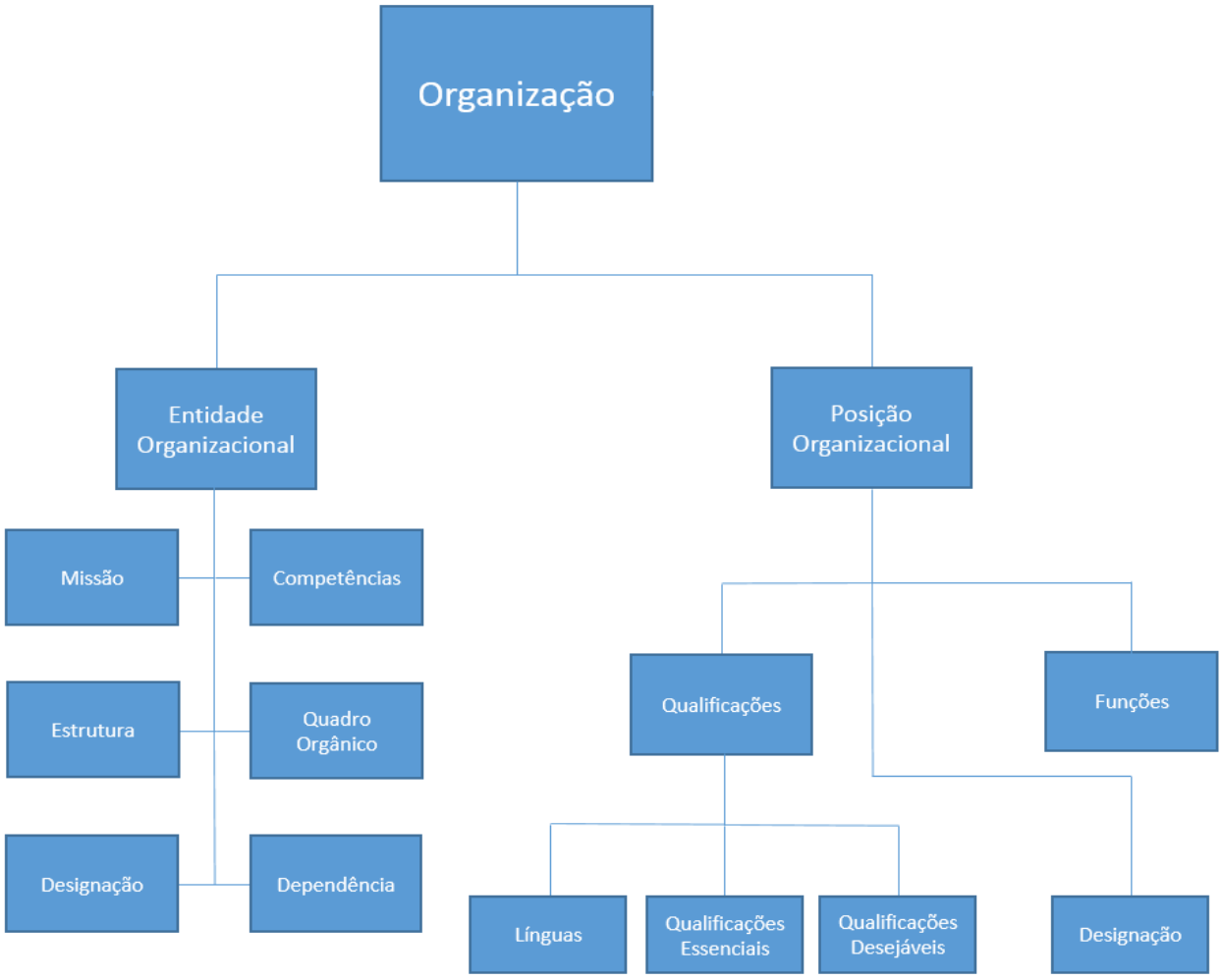


Figura 2 - Características da organização FA (MONTEIRO, et al., 2014)

A Entidade Organizacional tem os seguintes atributos (PÁSCOA, et al., 2011):

- **Designação**. Nome da Entidade Organizacional;
- **Missão**. Refere a missão da Entidade Organizacional;
- **Competências**. Conjunto de responsabilidades da Entidade Organizacional dentro da Organização;
- **Estrutura**. Composição da Entidade Organizacional**;**
- **Quadro Orgânico**. Identificação do total de pessoal militar e civil, pertencente à Entidade Organizacional;
- **Dependência**. Dependência hierárquica;
- **Posição Organizacional**. Entidades com um conjunto de atributos que preenchem uma certa posição da Organização.

Referente à Posição Organizacional, os pontos que a identificam, são os seguintes (PÁSCOA, et al., 2011):

- **Qualificações**. Dividem-se em **Línguas**, que são as línguas que é requerido ao trabalhador ter proficiência; **Qualificações Essenciais**, que mostram as qualificações que são exigidas para cumprirem com a posição organizacional; **Qualificações Desejáveis**, que mostram as qualificações que são desejáveis de ter para cumprirem com a posição organizacional;
- **Funções**. Referem todas as responsabilidades que são atribuídas, para cumprir com a posição organizacional;
- **Designação**. Representa a descrição da posição organizacional.

2.2 *Ontology*

O termo ontologia é utilizado para descrever um conjunto de conhecimentos sobre um determinando domínio de interesse, de forma a resolver qualquer problema de descrição deste. Uma ontologia contém necessariamente uma lista de conceitos, definições e das relações entre estes, esta contribuição para a semântica é um fator de alinhamento universal que deve estar presente em qualquer organização. A explicitação de uma ontologia pode adquirir várias formas mas garantidamente uma lista de vocabulário com a descrição do seu significado ou definição estará sempre presente (USCHOLD; GRUNINGER, 1996).

2.3 *Organizational Self-Awareness*

O ser humano é *self-aware* por natureza. É essa capacidade que permite o ser humano estar alerta para o que se passa à sua volta. Nas organizações, o *self-aware* é um requisito fundamental para a tomada de decisões, para completar tarefas e no processo de aprendizagem (ZACARIAS, et al., 2008).

Organizational self-awareness tem duas dimensões principais, uma individual e outra organizacional. A componente individual refere-se à capacidade que cada membro da organização tem para responder a perguntas como «W*ho am I in this organization?», «How are things done here?», «What is the organization -as a whole- doing now?».* Já a dimensão organizacional refere-se à combinação dos humanos ou agentes automatizados, recursos e procedimentos permite responder a perguntas

como “*who are my members?”, “how do they do things?”, “what are they doing now?”* (VICENTE; TRIBOLET, 2007). O elemento essencial para que exista *organizational self-awareness* é o alinhamento entre estas duas dimensões (VICENTE; TRIBOLET, 2007).

Uma das ferramentas para atingir uma *organizational self-awareness* eficiente é promover uma boa comunicação interna e esta assenta numa política de informação que tem de ser coerente com todos os elementos da cultura organizacional (artefactos, valores e presunções básicas). Esta coerência que oferece credibilidade à comunicação interna não assenta na riqueza ou na diversidade dos meios utilizados, mas apenas na existência, na organização, de uma cultura que privilegia a confiança, a solidariedade, a honestidade e a transparência (BILHIM, 1988).

2.4 Security Awareness

Por vezes, um dos maiores riscos à segurança da informação nas organizações não são as fragilidades tecnológicas mas as ações - ou a falta delas - tomadas pelos colaboradores internos ou externos da empresa e estas podem traduzir-se num risco capaz de causar incidentes na segurança da informação (Security Awareness Program Special Interest Group PCI Security Standards Council, 2014).

A *Security Awareness* é o conhecimento e a consciência que os colaboradores de uma organização devem possuir sobre a importância de proteger a informação, os cuidados a ter com o seu manuseamento e as implicações que podem resultar para a organização se existirem incidentes com a sua informação (Security Awareness Program Special Interest Group PCI Security Standards Council, 2014).

2.5 Alinhamento

O alinhamento pode ser entendido como uma forma de quantificar o nível de coerência entre conceitos, existem várias formas de garantir o alinhamento numa organização através de um conjunto de heurísticas, como exemplo, não devem existir processos redundantes pois traduz-se num desperdício de recursos (PEREIRA, et al., 2005).

Segundo Monteiro, na FA ainda não existe o alinhamento desejado entre a organização e os seus processos de negócio, *"não existe coerência; não existe uma ponte entre os conceitos dos processos e da organização".*

2.6 Domínio

Retirando a definição de domínio do dicionário da língua Portuguesa obtemos o seguinte: "Império; poder; propriedade; conhecimento; influência; esfera de ação". Na matemática é "a parte aberta e convexa, num espaço topológico, o domínio de uma função representa o conjunto inicial ou de partida, totalidade dos pontos onde a função é definida" (COSTA; MELO, 1999).

No âmbito desta dissertação importa frisar que o domínio é uma esfera de ação, dentro de uma empresa, podendo até ser a própria na globalidade, incluí todos os elementos dentro da mesma sem exceção, pretende-se que exista um conhecimento vasto sobre este domínio para conseguir a influência necessária ao alinhamento que é proposto.

2.7 Arquitetura

É a organização fundamental de um sistema, corporizada pelos seus componentes, as suas relações (entre si e o ambiente), e pelos princípios que guiam o seu desenho e evolução. Uma arquitetura pode também ser definida segundo o seu contexto, como uma descrição formal de um sistema ou como a estrutura de componentes, as suas relações, princípios e linhas orientadoras para controlar o seu *design* e evolução no tempo (The Open Group, 2015).

2.8 Arquitetura Empresarial

Um processo vital na criação de valor nas empresas envolve a arquitetura empresarial e o alinhamento que esta proporciona. Tem-se tornado cada vez mais evidente que a maturidade de uma arquitetura empresarial tem impactos positivos em varias áreas do negócio, como a redução de custos, melhorias nas velocidades dos processos, redução da complexidade e risco e um progresso geral na eficiência da tecnologia (BURNS, et al., 2009).

Numa definição rápida, a arquitetura empresarial pode ser considerada um conjunto coerente de princípios, métodos, e modelos que são usados no desenho e realização dos seguintes aspetos de uma empresa: Estrutura Organizacional; Processos de Negócio; Sistemas de Informação; Infraestrutura (The Open Group, 2015).

A empresa *Booz & Company* considera a arquitetura empresarial como um quadro lógico que estabelece a relação entre a estratégia e as estruturas organizacionais, processos de negócio, informação e tecnologia necessária para satisfazer a estratégia. Ao proporcionar uma visão holística da empresa, a arquitetura empresarial proporciona o suporte à tomada de decisões e assim permite a melhoria contínua da eficácia e eficiência do negócio (BURNS, et al., 2009).

Este modelo metodológico proporciona o alinhamento entre o negócio ou missão da empresa e todos os meios tecnológicos que a suportam. A sua representação deve incluir a Arquitetura Organizacional, Arquitetura de Processos, Arquitetura de Informação, Arquitetura de Aplicações e Arquitetura Tecnológica.

A grande mais-valia deste método é a capacidade de analisar o correto equilíbrio entre os diferentes tipos de recursos, humanos e tecnológicos, bem como os procedimentos utilizados pela empresa.

2.9 Arquitetura de Informação

A Arquitetura de Informação congrega aquilo que é mais perene na organização – a Informação – descrevendo a estrutura do que a organização necessita de saber para desenvolver os processos de negócio. Para isso, define-se de forma abstrata a informação necessária para o negócio, independentemente dos sistemas, tecnologias e processos de negócio, estruturada em forma de Entidades Informacionais. Pode mudar a estratégia de negócio bem como os processos ou as aplicações, contudo, a informação mantém-se praticamente perene e inalterável ao longo do tempo. Já o entendimento que se tem e a forma como se trata a informação pode mudar (GAMA, et al., 2006)**.**

2.10 Arquitetura de Sistema de Informação

À semelhança das outras arquiteturas, esta identifica as entidades e as suas relações, no caso de um sistema de informação de uma organização este cumpre a sua tarefa no contexto da própria organização. O mesmo pensamento se coloca para as aplicações, que se traduz na identificação e relacionamento das próprias aplicações entre si.

Qualquer sistema de informação deve ter algumas características, um nome que o identifica univocamente, a sua missão e os seus benefícios, as funcionalidades do sistema bem como as informações que gere e as suas dependências com outros sistemas (GAMA, et al., 2006).

Um sistema destes traz valor acrescentado na medida em que permite justificar as melhores aplicações em detrimento de outras e torna a arquitetura de sistemas de informação mais determinístico e consequentemente menos sujeito a fatores subjetivos.

Podemos assim perceber que o principal objetivo da arquitetura de sistemas de informação é determinar o caminho a seguir pela organização na aquisição ou atualização das tecnologias de informação, bem como reduzir os custos daí provenientes e melhorar o suporte ao negócio. Concretiza a implementação das Arquiteturas numa infraestrutura e escolhe quais as tecnologias que deverão ser utilizadas como suporte aos sistemas e aplicações definidos (GAMA, et al., 2006).

2.11 Sistema de Informação

Um sistema de informação é um tipo de sistema e pode ser definido de várias formas. Nomeadamente como um conjunto de elementos ou componentes inter-relacionados com entradas, processos e saídas de dados e informação, fornece também um mecanismo de realimentação utilizando as saídas. Tem o objetivo de auxiliar uma empresa a responder a todas as solicitações e apoiar as decisões necessárias dos processos de negócio. (STAIR; REYNOLDS, 2006)

É de salientar que um sistema de informação pode ser manual ou automatizado, com recurso a computadores e neste caso pode ser chamado de «aplicação» (TELHA; GORGULHO, 2014). Um sistema de informação que tenha por base computadores (CBIS – *computer-based information system)* é composto por: *hardware, software,* bases de dados, telecomunicações, pessoas e procedimentos,

alinhados com o objetivo de tratar, armazenar e processar dados ou informação (STAIR; REYNOLDS, 2006).

Conclui-se assim que um sistema de informação serve para gerir, armazenar e processar informação e/ou dados. Tanto os seus *inputs* como *outputs* são dados ou informação e a sua principal função é apoiar as decisões necessárias aos processos de negócio e como já foi referido acima caso esse sistema de informação seja totalmente automatizado pode designar-se por «aplicação».

Estando explicitas as diferenças entre uma aplicação e um sistema de informação, importa realçar que estes conceitos, no âmbito deste trabalho, serão utilizados para se referir ao mesmo conceito: um sistema de informação digital ou aplicação. Esta aproximação de conceitos faz todo o sentido pois se os novos sistemas de informação trazem grandes vantagens ao nível da rapidez, eficiência e eficácia no tratamento dos dados, também escondem perigos bastante diferentes dos antigos sistemas de informação analógicos.

2.12 Informação

«Informação» é um dos recursos mais valiosos e importantes nas organizações (STAIR; REYNOLDS, 2006).

Atualmente um dos maiores problemas das empresas é exatamente o excesso de dados, no entanto a informação é crucial para delinear as linhas de ação. A principal diferença entre dados e informação é simplesmente a forma como esta está organizada e selecionada. Os dados avulsos são inúteis a qualquer gestor, no entanto, atualmente o fluxo de dados a entrar numa empresa é enorme. Para que seja dada igual relevância a todos, os dados têm, necessariamente, que passar por um processo de seleção, organização, sintetização para finalmente serem considerados informação. Esta, por oposição aos dados, é útil e prática para ser analisada. A diferença entre dados e informação resume-se basicamente ao processo que estes sofrem para serem facilmente compreendidos e interpretados (STAIR; REYNOLDS, 2006).

O conhecimento por fim é o entendimento de um conjunto de informações e formas de torná-las úteis para apoiar uma tarefa específica ou tomar uma decisão (STAIR; REYNOLDS, 2006).

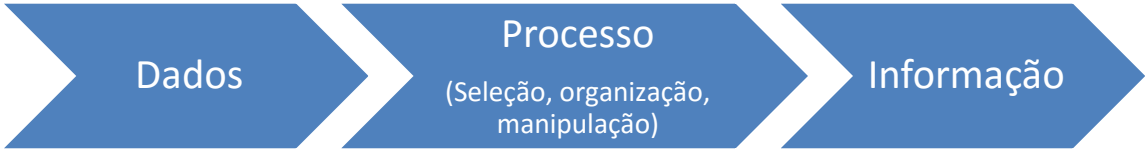


Figura 3 - (STAIR; REYNOLDS, 2006)

2.13 Segurança da informação

Abraham Maslow, na sua teoria das necessidades humanas - ou pirâmide de Maslow como é vulgarmente conhecida - coloca a segurança na base, isto significa que é uma necessidade humana básica que deve estar satisfeita em todo o momento. Desde do início da humanidade que o Homem precisa de segurança e esta prática é intemporal (MASLOW, 1943).

A segurança da informação e dos sistemas de informação é também uma necessidade básica essencial a qualquer organização. Contudo, com a massificação da tecnologia, cada vez mais pessoas e negócios estão vulneráveis a sofrer falhas na sua segurança e, como retrata esta dissertação, falhas na sua segurança computacional. Estes riscos podem estar associados a vírus ou outros *softwares* maliciosos, falhas dos sistemas de informação ou podem ainda ter uma origem social e serem causados por *hackers* ou pelos próprios colaboradores da empresa (BERNARDINO, 2012).

Importa deixar bem definido o conceito de segurança de informação. Segundo a ISO/IEC 27000:2014, um documento produzido pela *International Organization for Standardization*, e que tem como objetivo deixar explícitos alguns termos e definições sobre a gestão de sistemas de segurança de informação, a segurança da informação consiste na preservação de três caraterísticas fundamentais: a confidencialidade, a integridade e a disponibilidade. Numa análise mais detalhada é ainda possível identificar outras propriedades com menor relevância, tais como a autenticidade, responsabilidade, a não rejeição e a confiança (Iso.org, 2015).

2.13.1 Confidencialidade

A confidencialidade garante que a informação não é disponibilizada ou divulgada a indivíduos não autorizados, entidades ou processos (Iso.org, 2015), consistindo portanto na manutenção do segredo das informações.

A vantagem competitiva das empresas assenta muitas vezes na informação que detêm e por isso, deverão encontrar mecanismos que garantam a confidencialidade da informação mas que não impeçam o acesso atempado de pessoas à mesma (SILVA, et al., 2003).

É possível distinguir-se dois conceitos relacionados, a «confidencialidade dos dados», que procura assegurar que a informação não está na posse de indivíduos não autorizados e a «privacidade», que garante que qualquer individuo autorizado a ser detentor dessa informação possa ter acesso à mesma e que pode inclusive guarda-la, desde que tenha a necessidade de a conhecer para a utilizar nas tarefas que desempenha na empresa (STALLINGS; BROWN, 2012).

2.13.2 Integridade

A integridade refere-se a uma propriedade de exatidão e perfeição (Iso.org, 2015). Por outras palavras, a integridade é uma qualidade daquilo que é íntegro, que não sofreu qualquer alteração ou modificação e, neste contexto, garantir que a informação não é alterada impropriamente ou mesmo destruída. Pretende-se a exatidão, autenticidade, retidão e honestidade da informação.

À semelhança da confidencialidade, também a integridade se pode subdividir. A integridade dos dados assegura que a informação e os programas são apenas alterados de uma forma específica e autorizada e a integridade dos sistemas procura que todos os sistemas da organização funcionem inequivocamente, de forma a prevenir erros deliberados ou inadvertidamente autorizados pelo sistema (STALLINGS; BROWN, 2012).

2.13.3 Disponibilidade

A disponibilidade caracteriza-se pela informação estar acessível e pronta a ser utilizada assim que solicitado por uma entidade autorizada (Iso.org, 2015). Assegura

que os sistemas disponibilizam prontamente a informação solicitada e o serviço não é negado a indivíduos autorizados (STALLINGS; BROWN, 2012).

O acesso atempado à informação é vital e dele depende a execução dos processos da empresa. Possuir informação mas não a ter disponível no momento adequado, equivale a não possuir qualquer informação (SILVA, et al., 2003).

A **autenticidade** traduz-se na veracidade, na prova que uma informação é realmente aquilo que afirma ser. A responsabilidade torna-se muito generalista, portanto é mais fácil definir recorrendo a alguns exemplos. É da responsabilidade do criador da informação garantir que esta segue todas as outras propriedades, que é convenientemente introduzida no sistema de informação e é também sua responsabilidade dar as credenciais aos seus possíveis utilizadores. Por outro lado, é da responsabilidade dos utilizadores da informação utiliza-la de forma legítima, não violar princípios como o da integridade e não disponibilizar informação a ninguém que não seja autorizado a tê-la (STALLINGS; BROWN, 2012).

A **não rejeição** ou o **não-repúdio**, uma tradução pouco feliz do inglês *non-repudiation*, refere-se à associação de um ato ou ação a um individuo inequivocamente, de modo a que sejam imputadas responsabilidades. Por fim, a **confiança** traduz-se na convicção que os resultados estarão de acordo com o esperado pois existe segurança na informação (STALLINGS; BROWN, 2012).

Na doutrina da FA, a segurança da informação (INFOSEC) resulta da junção da *Communications Security* (COMSEC) e da *Computer Security* (COMPUSEC). Esta é resultante da aplicação de medidas de segurança destinadas a proteger a informação processada, armazenada ou transmitida (RFA 390-3, 2008).

Atualmente, a tarefa de desenvolver um sistema de segurança informacional nas empresas tornou-se uma tarefa bastante desafiante e complexa, pois tem de abordar duas dimensões diferentes: uma tecnológica e outra não tecnológica. Para além disto, a variedade de soluções que se podem encontrar torna difícil a tarefa de escolher aquela que mais se adequa aos procedimentos e este ponto é vital para garantir o alinhamento da empresa (BERNARDINO, 2012).

2.14 Fator social

O fator humano é o elo mais fraco numa cadeia complexa constituída por equipamentos, aplicações e procedimentos de operação e manutenção (Força Aérea RFA 390-6, 2011).

A segurança de informação tende a dedicar-se, principalmente, à faceta tecnológica dos problemas, focando-se nas soluções técnicas para as fragilidades inerentes à tecnologia. E é, por vezes, nesta área que se investe mais e como consequência constata-se frequentemente que é conferida muito pouca importância a um dos elos mais importantes da cadeia: a componente humana. São as pessoas que interagem diariamente com os próprios sistemas, que utilizarão a informação neles contida e que a gerem, por este motivo as pessoas são também a principal ameaça a esses sistemas (SILVA, et al., 2003).

Aliada a esta vulnerabilidade, o aumento do número de ataques informáticos conduziu à sofisticação tecnológica nas medidas defensivas e esta maior dificuldade em obter êxito numa ação maliciosa poderá tornar apetecível a exploração do fator humano. Uma formação de segurança adequada e contínua poderá ser o caminho para preparar os utilizadores para lidar com as quebras de protocolo e procedimentos (Força Aérea RFA 390-6, 2011).

As entidades com papel de destaque na estrutura de informação da FA devem receber formação, preferencialmente, em escolas NATO para acompanhar a sua doutrina. As restantes entidades com responsabilidade no manuseamento de informação, em qualquer fase do seu ciclo, devem receber formação nos principais conceitos relacionados com esta matéria (Força Aérea RFA 391-1 , 2011).

2.15 Gestão da informação

Contrariamente à ideia amplamente disseminada de que a Gestão da Informação se refere apenas a uma componente tecnológica, devido ao elevado grau de automatização de atividades através de Sistemas de Informação (SI), esta é uma matéria complexa que envolve os colaboradores da organização, a informação processada, sob qualquer formato e o modo como a mesma é produzida ou manuseada através dos processos da organização e os sistemas de informação que a processam (Força Aérea RFA 391-1 , 2011).

Figura 4 - Elementos intervenientes na gestão de informação (Força Aérea RFA 391-1 , 2011)

Importa salientar que a informação é o recurso mais perene nas organizações. Por oposição aos processos que as manuseiam e produzem, às aplicações e sistemas de informação e até às pessoas que intervêm nos processos (Força Aérea RFA 391-1 , 2011).

A gestão de risco é um conceito inseparável da gestão da informação e pode revelar-se um tema complexo. Traduz-se no processo de identificação de um conjunto de medidas que permitam proporcionar à empresa o nível de segurança pretendido. O *risk assessment* representa todo o processo de identificação (encontrar, reconhecer e descrever o risco), análise (compreender a natureza e determinar o nível de risco) e avaliação (a determinar a aceitação ou tolerância ao risco). (SILVA, et al., 2003)

2.16 *Business Motivation Model (BMM)*

O *Business Motivation Model* disponibiliza um esquema para ajudar ao desenvolvimento, comunicação e gestão dos planos de negócio de uma forma organizada. Mais especificamente, o BMM é capaz de identificar os fatores que motivam o estabelecimento de planos de negócio: identifica e define bem quais os elementos dos planos de negócios e, por fim, relaciona estes fatores e elementos entre si (Business Rules Group, 2015). Assim sendo, o BMM torna-se uma poderosa ferramenta de Engenharia Organizacional capaz de ser aplicada a toda a empresa ou organização, ou apenas a uma área ou departamento.

2.16.1 Vantagens do Business Motivation Model

O Business Motivation Model é composto por um conjunto de conceitos que define os elementos dos planos de negócio que estão associados a uma estrutura que dará suporte às várias aproximações possíveis para criar e manter o BMM de uma empresa. É de realçar que este modelo é particularmente forte no suporte de processos que estejam em constante mudança. O BMM não é especialmente construído para desenvolver processos de gestão de negócio, para definir um projeto ou gerir um processo, isto é, pode ser utilizado desse modo mas é capaz de ir muito além disso (Business Rules Group, 2015).

Idealmente o desenvolvimento do modelo seria feito em perspetiva, ou seja, os elementos dos planos de negócio deveriam ser pensados antes de desenhar o sistema ou de este estar desenvolvido. Deste modo, os planos de negócio surgiriam antes da implementação da atividade da empresa e não haveria tanta margem para erros, as soluções aos problemas estavam pensadas previamente e estariam muito mais firmemente implementadas e seriam também menos dispendiosas (Business Rules Group, 2015).

O Business Motivation Model não pode ser considerado um modelo de negócio completo sendo que não detalha aspetos essenciais a um modelo de negócio, como os processos de negócio, as atividades, sequências, dependências e interações que os descrevem. O BMM também não inclui o fluxo de trabalho, a atribuição de papéis a cada individuo e as responsabilidades, mas inclui as estratégias e táticas que

podem configurar a organização nesse sentido. Para além disso, é necessária uma definição do vocabulário da empresa com termos e factos necessários aos negócios, no entanto, as regras de negócio sugerem a sua elaboração (Business Rules Group, 2015).

O BMM trará benefícios a três tipos de pessoas em particular: responsáveis pelo desenvolvimento de planos de negócio, modeladores de empresas e responsáveis pela implementação de ferramentas de Software (Business Rules Group, 2015).

Esta ferramenta conceptual é particularmente útil aos desenvolvedores de planos de negócio pois funciona com uma *checklist* que inclui todos os fatores a ter em conta, disponibiliza um vocabulário Standard e flexível o suficiente para se adaptar ao processo de desenvolvimento de cada organização. No Futuro, para os modeladores de negócios, serão usados *standards* como o BPMN (*Business Process Model and Notation)* e a utilização do BMM garantirá o alinhamento (à *priori)* das arquiteturas e da linguagem utilizada (Business Rules Group, 2015).

2.16.2 Descrição do modelo

Existem duas grandes áreas do BMM, a primeira inclui os fins e os meios dos planos de negócio e a segunda, os influenciadores, *assessment* e o *potential impact* como ficará explicito de seguida*,* de acordo com a doutrina do *Business Rules Group.*

Os **Fins** são aquilo que a empresa pretende alcançar sem especificar a forma de os atingir. Aqui está incluída a visão e os resultados desejados dos quais fazem parte as metas e os objetivos.

- A **visão** descreve o estado futuro da empresa, suporta e torna operacional a missão e é amplificada pelas metas.
- Os **resultados desejados** são um fim que a empresa quer manter, são suportados pelas linhas de ação e incluem as metas e os objetivos.
- As **metas** amplificam a visão e descrevem genericamente o estado que a empresa pretende atingir. Devem ser quantificadas pelos objetivos e suportadas pelas estratégias.

- Os **objetivos** devem ser atingíveis, delimitados no tempo, mensuráveis, adequados e relevantes para quantificar as metas. São atingidos através das táticas e, comparativamente às metas, tendem a ser mais específicos.

Figura 5 - Hierarquia dos fins (Business Rules Group, 2015)

Os **meios** traduzem-se em qualquer capacidade, técnica, instrumento, método entre outros. Estes podem ser utilizados para alcançar os fins mas não indica os passos necessários para alcançá-los, nem a responsabilidade por essa tarefa, indicando apenas as capacidades que podem ser exploradas para os atingir.

- A **missão** indica o negócio da empresa, isto é, aquilo que é a sua atividade quotidiana. Operacionaliza a visão, ou seja, revela a forma de a alcançar e é planeada através de estratégias.
- As **linhas da ação** resumem-se aos esforços feitos para alcançar os resultados desejados e são governadas por diretivas. Ou seja, é o plano ou aproximação da empresa em determinado aspeto que envolve, por exemplo, os processos e as pessoas com vista a alcançar os resultados desejados. As linhas de ação incluem as estratégias e táticas e são operacionalizadas por processos de negócio.
- A **estratégia** representa as linhas de ação gerais para alcançar os fins, mais particularmente as metas, por isso, tendencialmente, as estratégias trabalham no sentido de concretizar as metas.

- Uma **tática** é uma linha de ação que representa detalhadamente as estratégias e por isso, pode afirmar-se que as implementa. Paralelamente às estratégias, as táticas canalizam os seus esforços para realizar os objetivos.
- As **diretivas** indicam o modo como as linhas de ação devem ou não ser conduzidas, ou seja, governam as linhas de ação e englobam as políticas de negócio e as regras de negócio.
- As **políticas de negócio** são diretivas generalistas cujo propósito é governar a empresa. Estas fornecem as linhas orientadoras básicas para as regras de negócio e existem para controlar as estratégias, táticas e processos sendo que em comparação com as regras de negócio são menos precisas e objetivas.
- Uma **regra de negócio** deriva normalmente das políticas de negócio e tem como objetivo suportá-las, dando resposta às oportunidades, ameaças, pontos fortes e fracos. São bastante específicas e estruturantes e fornecem, por exemplo, restrições, autorizações e linhas orientadores em áreas específicas da empresa ou organização.

Figura 6 - Hierarquia dos meios (Business Rules Group, 2015)

Um **influenciador** pode ser qualquer coisa capaz de causar um efeito sem exercer uma ação diretamente ou sem intenção. Os influenciadores relevantes são todos aqueles que podem causar impacto nos meios, levando a que estes alcancem diferentes fins, as influências que estes causam devem ser julgadas no *assessement*. Os influenciadores podem ser externos ou internos.

- Os **influenciadores externos** são todos aqueles que estão para além das fronteiras da empresa. Podem ser rivais, clientes, parceiros, legislação, o ambiente, os fornecedores ou a tecnologia.
- Os **influenciadores internos** situam-se dentro da empresa e podem ser as infraestruturas, o habitat, os recursos, pressupostos, problemas, as chefias e os valores da instituição que tanto podem ser explícitos, se estiverem declarados ou implícitos se forem naturalmente assumidos por todos.

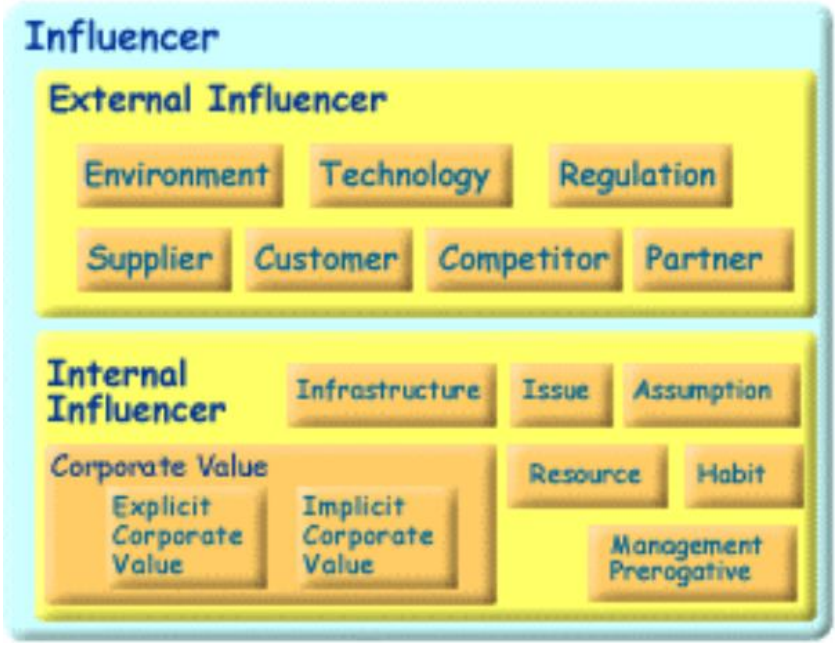


Figura 7 - Possíveis influenciadores (Business Rules Group, 2015)

O ***assessment*** é um julgamento sobre os influenciadores que podem afetar a utilização dos meios ou o alcance dos fins, ou seja, o *assessment* expressa uma conexão lógica entre os influenciadores e os meios e fins, indicando quais são relevantes. É feito através de uma análise SWOT a cada influenciador, e conclui quais são os pontos fortes e fracos, as oportunidades e ameaças da empresa.

Esta análise contrui para chegar a um ***potencial impact*** que mede o risco e os ganhos potencias. Concorrendo assim para motivar novas políticas de negócio.

Figura 8 - Categorias de *assessment* (Business Rules Group, 2015)

O ***Potential Impact*** contem o risco e os ganhos potenciais. A sua origem provem do *assessment* e pode motivar alterações na doutrina da organização (Business Rules Group, 2015).

O BMM representa um modelo bastante completo para ajudar nos planos de negócio de qualquer empresa. É graças à sua versatilidade e abrangência que é garantido que nenhum ponto é esquecido durante a implementação do modelo, apesar de estar separado em quatro áreas principais, estas encontram-se alinhadas entre si através de conexões lógicas.

Na figura seguinte é possível ver a representação completa do modelo, com todas as suas entidades e relações esquematizadas.

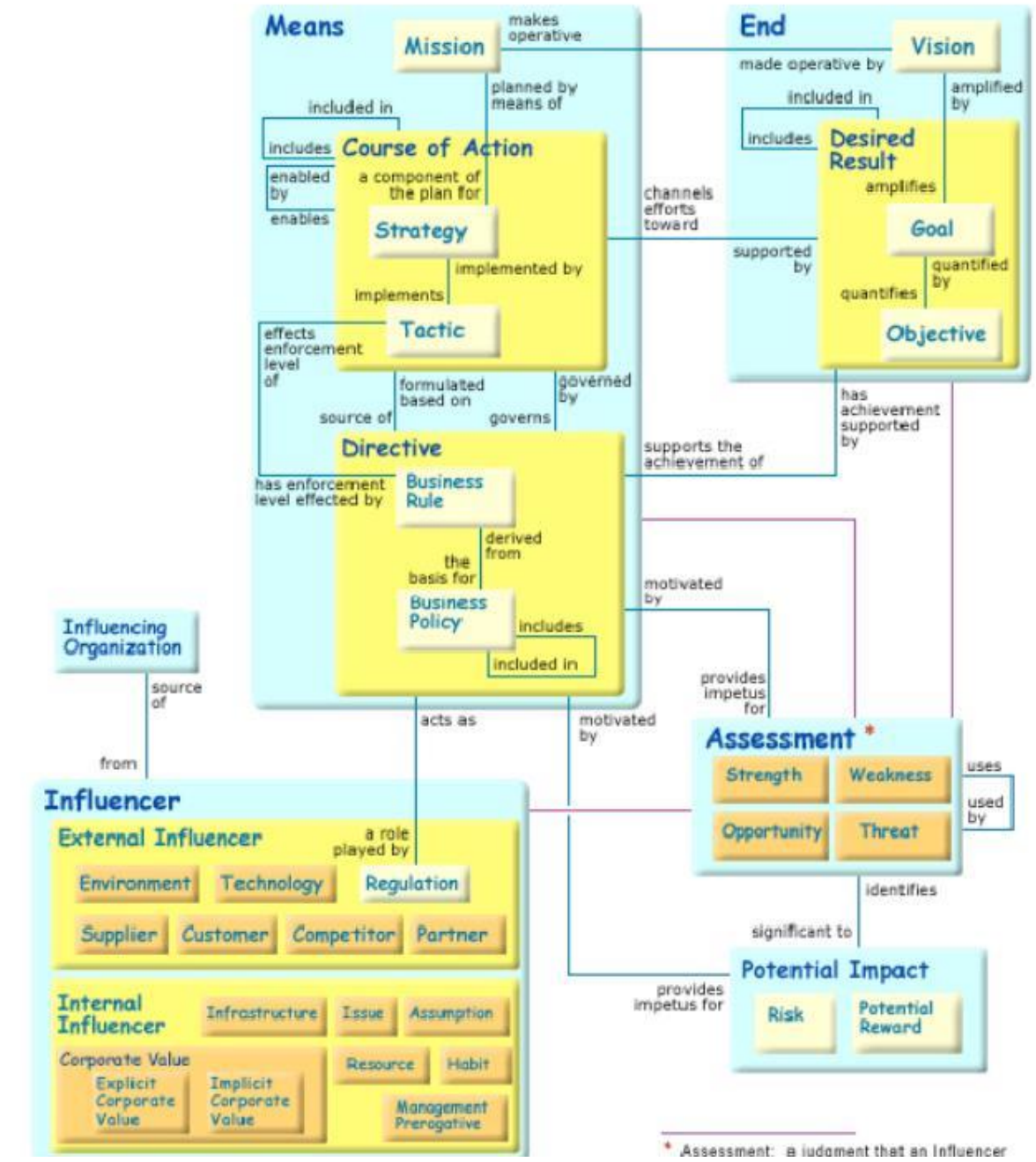


Figura 9 – Business Motivation Model (Business Rules Group, 2015)

2.17 Plano

A definição existente no dicionário da língua Portuguesa apresenta diferentes significados. Sendo um adjetivo, significa que não existem desigualdades nem

ondulações, raso ou liso. Previsão, geralmente para mais de um ano, destinada a servir de guia para determinadas atividades; planta; traçado; desenho; disposição geral de uma obra; projeto; desígnio; planície. Na economia é o principal instrumento coordenador de toda a política económica, na geometria representa uma superfície plana, que pode considerar-se gerada por uma reta que se move em torno de um eixo a ela perpendicular (COSTA; MELO, 1999).

Matematicamente, um plano representa um objeto bidimensional que se estende infinitamente e pode ser definido das seguintes formas:

- Três pontos não colineares;
- Uma linha e um ponto fora dessa linha;
- Duas retas distintas que se intersetem;
- Duas retas paralelas.

Se o plano estiver delimitado no espaço é chamado de semiplano (FONTE, 2016).

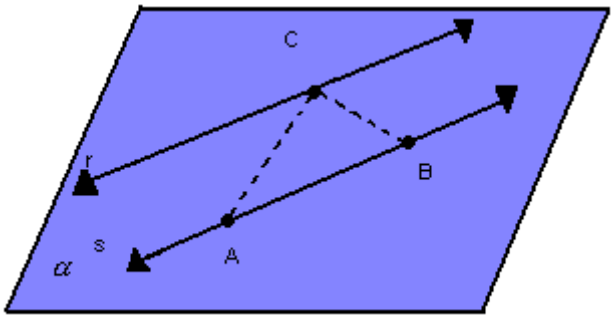


Figura 10 - Plano (Só Matemática, 2016)

2.18 Estrutura organizacional

Qualquer organização estrutura-se segundo vários níveis hierárquico que se relacionam entre si, segundo as funções específicas de cada plano. Também a cada plano está associado um nível de decisão e todos eles são vitais para o seu desempenho (GUEDES, 2013).

A cada nível organizacional está associado um nível de decisão e um conjunto de funções, bem como as competências desejáveis para quem ocupa esses níveis organizacionais. Ao nível estratégico compete fazer o planeamento a longo prazo da estratégia da organização. O plano tático é menos abrangente e preocupa-se em elaborar planos de ação a médio prazo. Na base da pirâmide encontra-se o plano operacional responsável por efetuar processos e atividades de curto prazo e bastante técnicas (CHIAVENATO, 2004).

Figura 11 - Modelo dos planos organizacionais (CHIAVENATO, 2004)

Outro modelo conceituado na comunidade científica foi apresentado por Thompson (2003), semelhante ao anterior, dividido em três níveis: Institucional, Direcional e Tático.

Figura 12 – Níveis organizacionais de Thompson (FERNANDES, 2011)

Mintzberg (1995), outro autor, demonstra um modelo que representa a estrutura organizacional, em que considera que, de toda a atividade humana de uma

organização, impõem-se duas exigências fulcrais: divisão do trabalho em várias tarefas e coordenação dessas tarefas. A partir deste pressuposto, Mintzberg classifica e divide uma organização em seis partes básicas: vértice estratégico, linha hierárquica, tecnoestrutura, pessoal de apoio, centro operacional e ideologia. Será feita uma análise detalhada aos conceitos referidos:

No **vértice estratégico** estão inseridas as pessoas com responsabilidade global pela organização, chefes de alto nível com cargos globais. É no vértice estratégico que se encontram as pessoas encarregues de assegurar o cumprimento da missão da organização de forma eficaz, e que analisam as necessidades dos *stakeholder* (MINTZBERG, 1995).

Na **linha hierárquica** encontram-se os gestores intermediários, que fazem o ponto de ligação entre o vértice estratégico e o centro operacional. Estes são responsáveis pela execução de tarefas na corrente de supervisão direta acima e abaixo deles: adquirem informações de *feedback* e transferem as mais importantes aos gestores acima; intervêm no fluxo de decisões; identificam os problemas da unidade, as propostas de mudança e decisões que requerem autorização para níveis acima. Uma vez que existe uma interdependência entre as unidades há, então, um fluxo horizontal, sendo que os gestores intermédios estabelecem contacto entre eles. Estes formulam as estratégias da sua unidade, que devem estar alinhadas com os objetivos e com as regras de negócio da organização. À medida que se vai descendo no nível da hierarquia, as atividades administrativas vão se tornando mais detalhadas e operacionais (MINTZBERG, 1995).

O **centro operacional** é responsável por garantir as entradas para a produção, transforma essas entradas em saídas, criando valor para a organização. As pessoas que se encontram inseridas neste centro estão diretamente ligadas à entrada da matéria-prima, à sua transformação no produto e à sua distribuição (MINTZBERG, 1995).

A **tecnoestrutura** é responsável pela definição dos processos, as especificações do produto e a formalização do comportamento. Esta tem como objetivo a diminuição da necessidade de supervisão direta, tornando as tarefas mais eficazes (MINTZBERG, 1995).

A área do **pessoal de apoio** é responsável por apoiar a organização fora da corrente de produção do seu produto principal, dando suporte às operações da organização. Estas áreas especializadas, normalmente são autossuficientes, e são

estruturadas como pequenas organizações, recebendo os recursos da organização principal (MINTZBERG, 1995).

A ideologia traduz a parte da organização responsável pela elaboração, manutenção, disseminação e interiorização das ideologias e doutrinas. Mintzberg afirma que a ideologia é «a parte viva» de qualquer organização. A ideologia é vista como um regime de crenças sobre a própria organização, e não as crenças da sociedade que a envolve (MINTZBERG, 1995).

Na figura seguinte é possível observar o modelo organizacional proposto por Mintzberg, com as suas seis partes básicas:

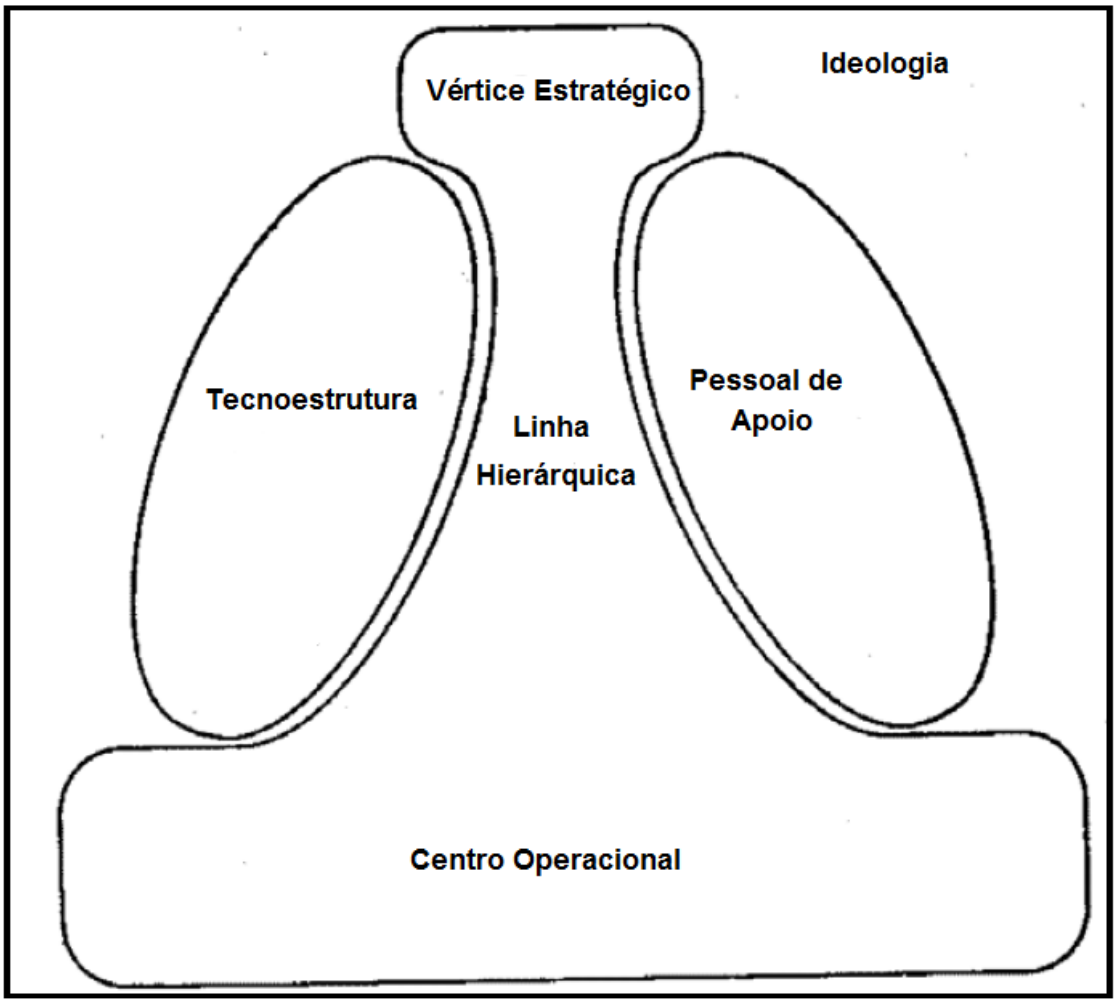


Figura 13 - Estrutura de uma organização (MINTZBERG, 1995)

2.18.1 Estrutura organizacional da Força Aérea

A organização da Força Aérea baseia-se numa estrutura vertical e hierarquizada onde os respetivos órgãos se relacionam através de quatro níveis de

autoridade: hierárquica, funcional, técnica e de coordenação (Decreto-Lei nº 187/2014, 2014).

A autoridade hierárquica corresponde ao comando completo e existe sem prejuízo de outras dependências, é a única que inclui competência disciplinar. A funcional é a autoridade conferida a um órgão para controlar processos, no âmbito das respetivas áreas ou atividades específicas. A autoridade técnica é a autoridade conferida a um órgão para fixar e difundir normas de natureza especializada, por fim, a autoridade de coordenação é conferida a órgãos subordinados, em qualquer nível, com o intuito de consultar ou coordenar diretamente uma ação com um comando, dentro ou fora da respetiva linha de comando (Decreto-Lei nº 187/2014, 2014).

O modelo em pirâmide da Força Aérea assemelha-se ao descrito por Chiavenato (2004) e Thompson (2003), apesar de, no meio militar, a nomenclatura atribuída ser diferente Estratégico-Operacional-Tático (FERNANDES, 2011).

Figura 14 – Estrutura Organizacional da Força Aérea (Fonte: Autor)

Ao mais alto nível de decisão da FA, o estratégico, encontra-se o Chefe do Estado-Maior da Força Aérea (CEMFA), tendo como suporte, o Gabinete do CEMFA (GCEMFA), que é o órgão de apoio direto e pessoal ao CEMFA. É também onde se situa o Estado-Maior da Força Aérea (EMFA), que constitui o órgão de estudo, conceção e planeamento da atividade da Força Aérea, para apoio à decisão do CEMFA, o Departamento Jurídico da Força Aérea (DJFA) tem como missão conduzir os assuntos de natureza jurídica, no âmbito das atribuições e competências da Força

Aérea. Encontra-se também a Academia da Força Aérea (AFA), que tem como missão, formar os oficiais do Quadro Permanente, a Direção de Finanças da Força Aérea (DFFA), que assegura a administração dos recursos financeiros, os Órgãos de Conselho (OC), que apoiam as decisões do CEMFA em diversos temas, a Inspeção-Geral da Força Aérea (IGFA), que conduz a missão de apoiar o CEMFA no exercício da função de controlo, avaliação e prevenção e investigação de acidentes e, por último, os Órgãos de Natureza Cultural (ONC), que têm a missão de assegurar as atividades de apoio geral da Força Aérea no âmbito cultural (MONTEIRO, 2014).

No nível abaixo, existe o Comando de Pessoal da Força Aérea (CPESFA), com a missão de administrar os recursos humanos para a execução dos planos e diretivas aprovados pelo CEMFA, o Comando da Logística da Força Aérea (CLAFA), com a missão de administrar os recursos materiais, de comunicações e sistemas de informação e infraestruturas da Força Aérea e garantir o cumprimento dos requisitos para a certificação da navegabilidade das aeronaves militares e o Comando Aéreo (CA), que suporta a missão de apoiar o comando por parte do Chefe de Estado-Maior da Força Aérea, tendo em vista a preparação, o aprontamento e a sustentação das forças e meios da componente operacional do sistema de forças, o cumprimento das missões particulares, de missões reguladas por legislação própria ou outras missões de natureza operacional que sejam atribuídas à Força Aérea (MONTEIRO, 2014).

Num nível ainda mais abaixo é possível identificar as restantes dependência da FA, obviamente ao descer a pirâmide a quantidade de órgão a enumerar será muito maior mas, como exemplo, temos as diferentes bases, repartições, as esquadras e esquadrilhas.

2.19 Segurança Computacional

O conceito de segurança computacional surge para fazer face aos avanços nas tecnologias da informação. Define-se como a proteção conferida a um sistema de informação, a fim de atingir os objetivos aplicáveis à preservação da integridade, disponibilidade e confidencialidade dos recursos do sistema de informação (Hardware, Software, informações/dados, e telecomunicações). Engloba todas as técnicas que assegurem que as informações guardadas não podem ser lidas, modificadas ou destruídas sem autorização, exemplos disso vão desde simples palavras passe até códigos encriptados (NIST, 1995).

No âmbito desta dissertação, o conceito surge para dar resposta à lacuna existente devido à falta de uma definição de segurança computacional na FA que englobe todas as preocupações com a segurança da informação.

Este conceito pretende ser abrangente o suficiente para cobrir toda a informação presente na FA, desde da classificada à mais simples processada por qualquer posto de trabalho, independentemente do suporte em que é tratada, ou seja em formato analógico, digital ou até mesmo informação empírica adquirida pela experiencia e prática.

Um exemplo da necessidade desta visão holística sobre a informação na FA são as publicações existentes e o edifício de publicações referentes à Gestão da Informação na Força Aérea. Atualmente existem quatro regulamentos da Força Aérea que doutrinam a temática da informação:

- RFA 391-1 Politica de gestão da informação da Força Aérea;
- RFA 390-3 Politica de segurança da informação e dos sistemas de informação e comunicações na Força Aérea;
- RFA 390-4 Organização e estrutura de segurança dos SIC da Força Aérea (Reservado);
- RFA 390-6 Política de ciberdefesa da Força Aérea.

Estão ainda previstas mais publicações que deverão estar em fase de elaboração, nomeadamente:

- RFA 391-2 Politica de utilização de recursos de informação da Força Aérea;
- RFA 391-3 Política de sistemas de informação da Força Aérea.

No entanto, no seguinte edifício de publicações presente no RFA 391-1 não vem representado o RFA 390-6 nem o RFA 390-4. Representando, portanto, uma falha de alinhamento ao nível da doutrina existente.

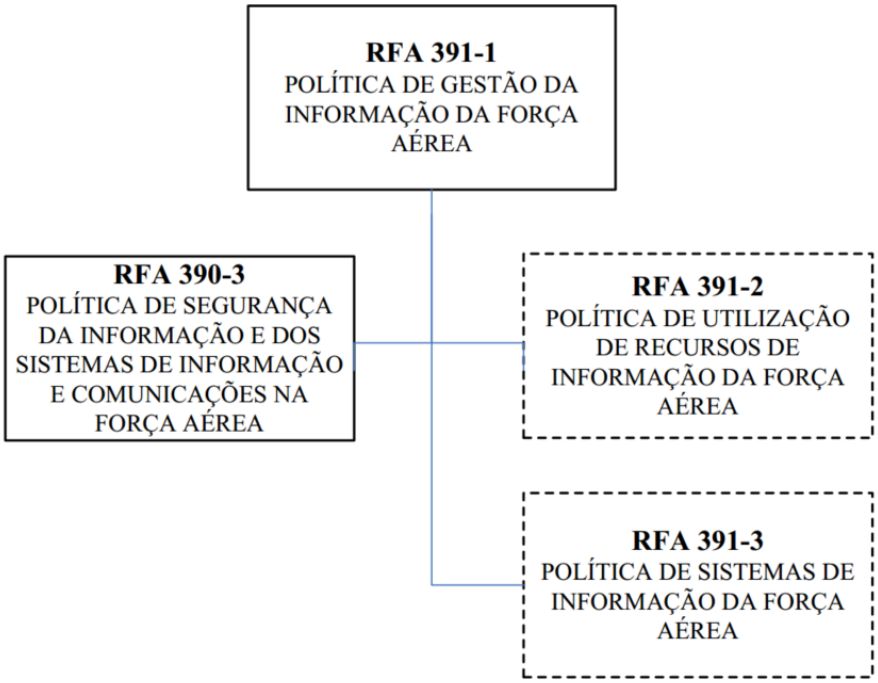
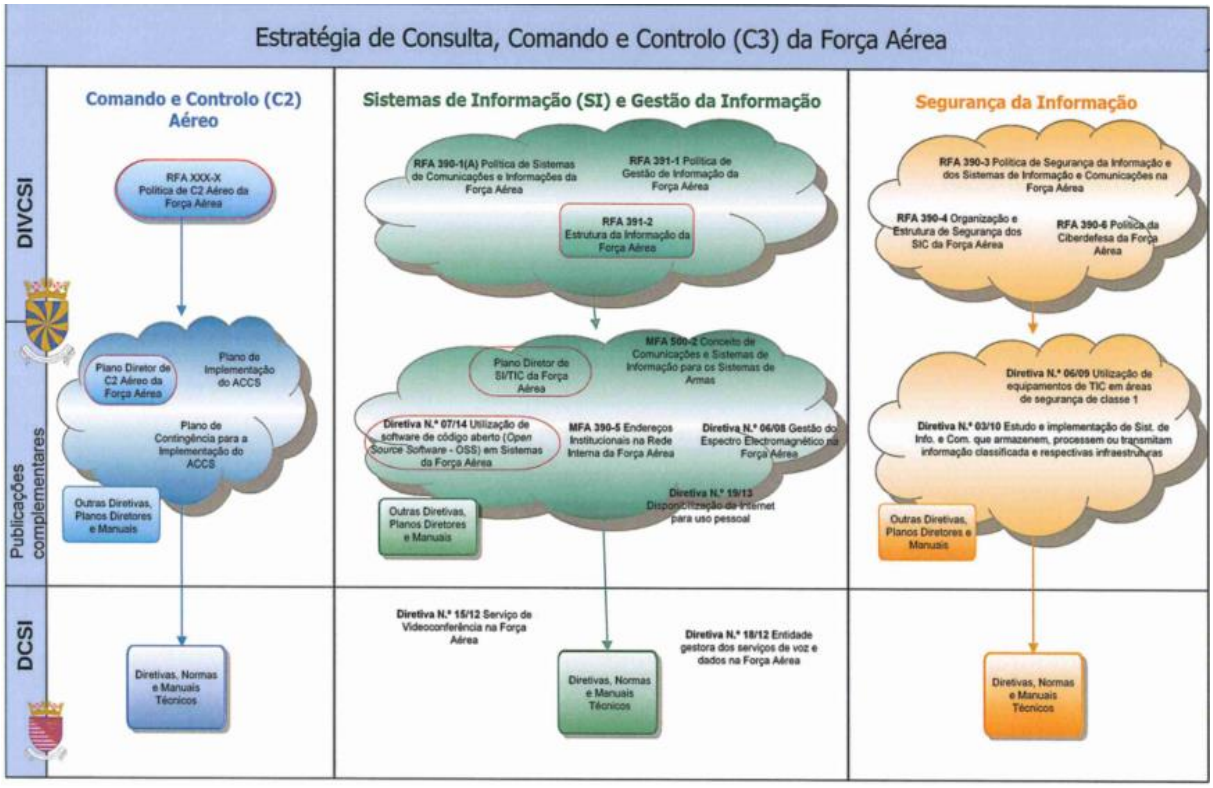


Figura 15 – Edifício de publicações referente à gestão da informação na Força Aérea (Força Aérea RFA 391-1 , 2011)

Na imagem seguinte é possível observar que as fontes de doutrina se dividem em três grandes correntes, uma mais operacional de Comando e Controlo (C2) Aéreo, que não será considerada nesta dissertação, uma corrente dedicada aos Sistemas de Informação e Gestão de Informação e ainda outra dedicada à Segurança de Informação. É, ainda, de salientar que diferentes planos organizacionais têm diferentes competências quanto à elaboração de doutrina.

Tabela 1 – Publicações sobre segurança de informação na FA (Diretiva Nº11/CEMFA, 2014)



2.19.1 Estrutura da informação da Força Aérea

As primeiras iniciativas para implementar uma estrutura organizacional da informação na FA remontam ao despacho do general CEMFA de 03 de Outubro de 1985, esta abordagem era vocacionada para as diferentes áreas funcionais. Com a emergência de novos sistemas e tecnologias o fluxo de informação aumentou e a falta de alinhamento entre as diferentes áreas funcionais tornou evidente que a estrutura estava desadequada e revelou a necessidade de existir uma entidade reguladora capaz de coordenar toda a informação na FA. (Força Aérea RFA 391-1 , 2011)

A atual estrutura de informação da FA é composta pelas seguintes entidades:

- **Diretor da informação.** O responsável legal pela informação da FA é do General CEMFA que delega o cargo ao MGen SubCEMFA. Compete-lhe dirigir toda a atividade relacionada à gestão de informação da FA. (Força Aérea RFA 391-1 , 2011)
- **Divisão de comunicações e sistemas de informação (DIVCSI).** A DIVCSI desempenha um papel consultivo nesta estrutura de informação. (Força Aérea RFA 391-1 , 2011)

- **Grupo coordenador da gestão da informação (GCGI).** Este grupo é composto pelos administradores da informação da área funcional (AdIAF), pelo chefe da DIVCSI, pelo adjunto para os sistemas de informação da DIVCSI e por um representante do SIG-DN na FA sendo presidido pelo diretor da informação. (Força Aérea RFA 391-1 , 2011)
- **Direção de comunicações e sistemas de informação (DCSI).** Compete-lhe definir e realizar as modificações necessárias para incorporar os requisitos de informação nos SI ao longo de todo o ciclo de vida da informação. (Força Aérea RFA 391-1 , 2011)
- **Gabinete de administração da informação da área funcional (GAdIAF).** Este gabinete é composto pelo Administrador da informação da área funcional e pelos adjuntos para a informação da área funcional (AdjIAF). (Força Aérea RFA 391-1 , 2011)
- **Administrador da informação da área funcional (AdIAF).** Resumidamente compete-lhe desenvolver e implementar a gestão de informação na sua área funcional, consoante as suas necessidades e tendo em vistas o estabelecido pelo diretor da informação. (Força Aérea RFA 391-1 , 2011)
- **Adjunto para a informação da área funcional (AdjIAF).** Entre outras funções, compete-lhe apoiar o AdIAF no desempenho das suas funções. (Força Aérea RFA 391-1 , 2011)
- **Delegado da informação.** Os delegados da informação são nomeados pelos comandantes, diretores, ou chefe de cada unidade, órgão ou serviço. Esta entidade deve possuir um conhecimento detalhado nos SI da sua unidade, por este motivo é possível que seja escolhido mais de um delegado da informação. (Força Aérea RFA 391-1 , 2011)

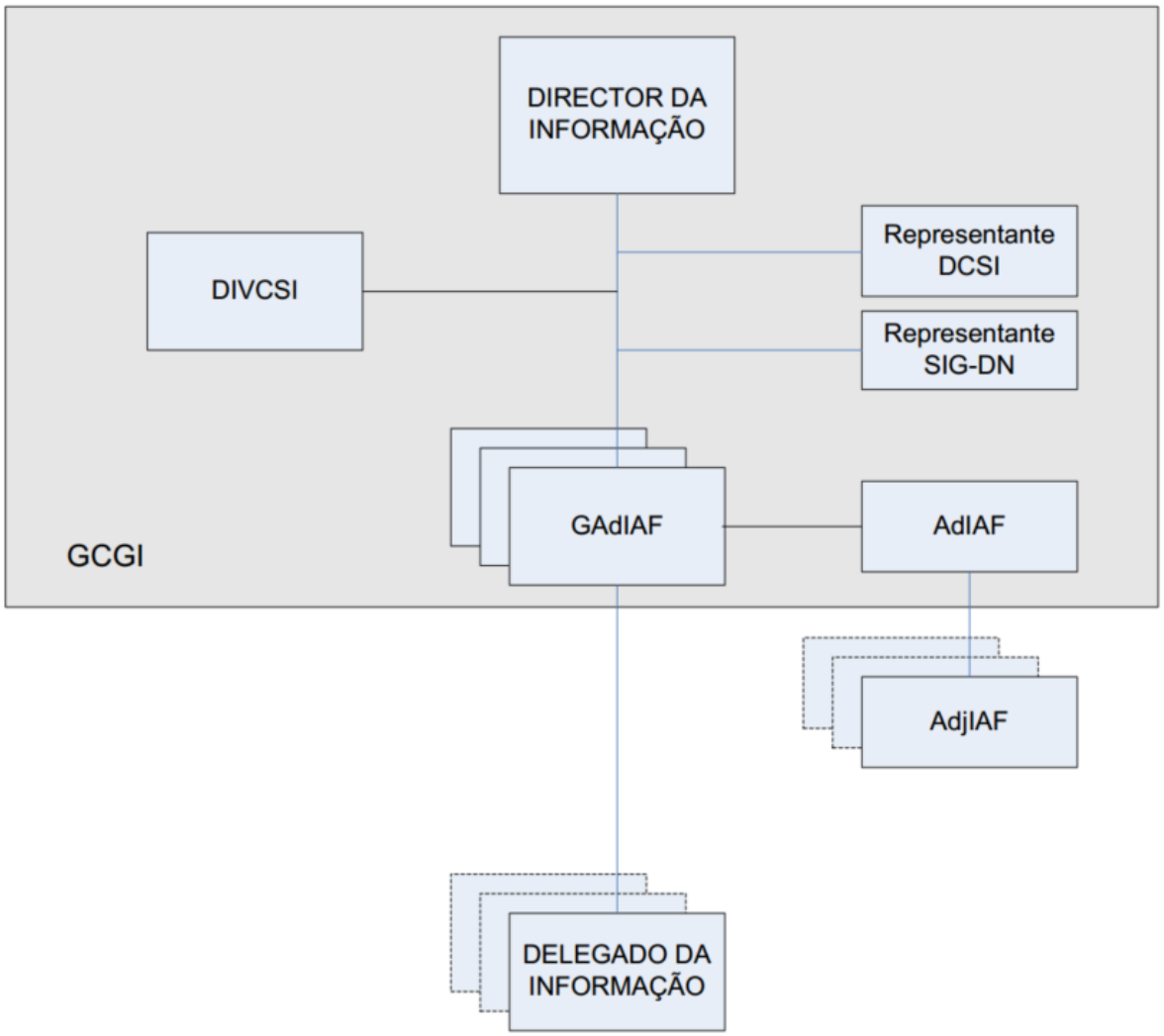


Figura 16 - Estrutura da informação da Força Aérea (Força Aérea RFA 391-1 , 2011)

3 Desenvolvimento do Modelo

3.1 Entrevistas

As entrevistas efetuadas tiveram um carácter exploratório, apesar de posteriormente terem sido úteis na validação de alguns fatores de alinhamento que tiveram como origem o BMM, isto porque no momento em que foram efetuadas o modelo de alinhamento ainda estava pouco desenvolvido.

Os maiores contributos na realização das entrevistas para esta dissertação foi a promoção de uma *«organizational self-awareness»* e de uma *«security awareness»* ao autor, que ainda pouco conhecia sobre este tema na FA. Para além disso, a identificação dos influenciadores, externos e internos, a ajuda na análise SWAT do BMM e algumas propostas como a visão da segurança computacional foram grandes mais-valias para este trabalho,

3.2 Contributo da Revisão Literária

A revisão literária efetuada permitiu em primeira instância solidificar alguns conceitos essências para compreender todo o enredo desta dissertação, começando gradualmente a aprofundar aquilo que é o tema central. Este processo foi crucial para desmitificar o tema numa primeira análise.

Existem dois conceitos que numa dissertação vocacionada com o alinhamento são cruciais: *Organizational Self-Awareness* e *Security Awareness.* O primeiro, mais generalista, traduz a importância dos colaboradores conhecerem a organização para cumprir eficazmente os processos que lhe são destinados. O segundo conceito, bastante mais vocacionado para a área da segurança computacional, revela a necessidade de existir uma cultura de *Security Awareness* presente em toda a organização, sendo que esta foi uma necessidade particularmente destacada durante as entrevistas realizadas. A *Security Awareness,* dada a sua importância pode vir a tornar-se num fator de alinhamento.

O *Business Motivation Model* é um modelo com grande potencial de promover o alinhamento, por esse motivo, uma análise exaustiva à sua composição, como a que foi apresentada, revelou-se uma grande mais-valia para o seguimento desta

dissertação. Dado o seu detalhe, torna-se um excelente ponto de partida na definição de vários conceitos importantíssimos a todos os níveis organizacionais.

A revisão literária contribuiu, também, para o autor tomar conhecimento da situação ao nível de segurança computacional na FA, por ser à partida uma área nova. Só através da leitura de muita doutrina e entrevistas, foi possível ir conhecendo melhor a organização neste âmbito, o que foi essencial para elaborar uma dissertação sobre o tema. À medida que a investigação se aprofundou foi possível compreender as fragilidades existentes na FA e a necessidade de propor um modelo que pudesse, de alguma forma, melhorar essas falhas.

Analisando a revisão literária e tendo em conta o tema desta dissertação, a segurança computacional como fator de alinhamento entre planos organizacionais, é possível retirar algumas conclusões pertinentes para a elaboração de um modelo que permita o alinhamento da segurança computacional através dos diferentes planos organizacionais. Com a investigação desenvolvida, identificaram-se algumas semelhanças entre estes dois grandes temas, sendo que, estes fatores materializar-se-ão no ponto de partida para definir os critérios de alinhamento do modelo que será desenvolvido.

3.3 Meta-modelo de alinhamento

O meta-modelo proposto nesta dissertação é representado de seguida, tal como demonstrado na figura, existem dois conceitos fundamentais que devem ser estudados: os planos organizacionais e os atributos da camada de alinhamento.

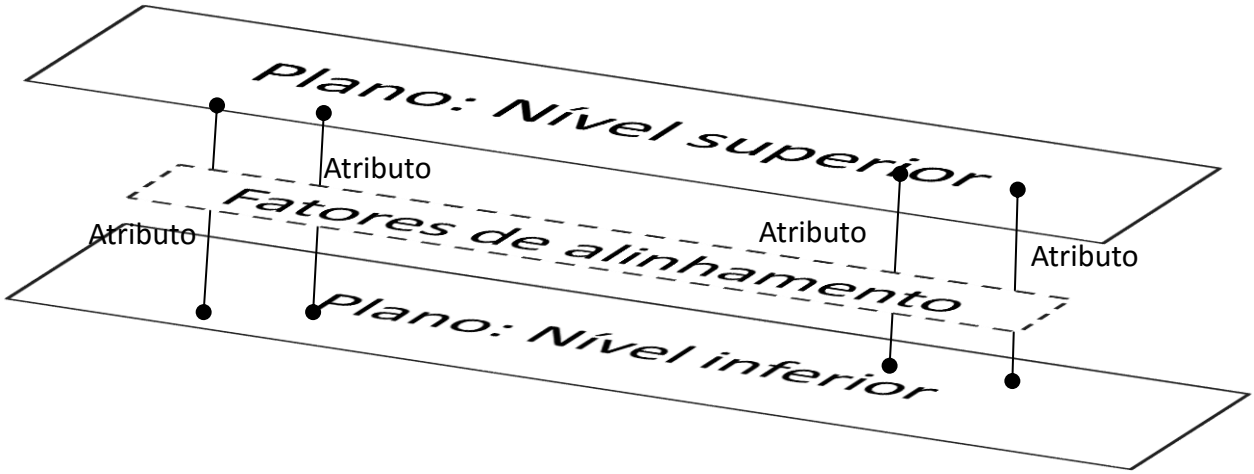


Figura 17 - Alinhamento entre planos organizacionais (Fonte: Autor)

Partindo deste modelo, serão detalhados estes dois conceitos. O primeiro irá contribuir na construção do segundo, pois os atributos de qualquer plano organizacional são os mesmos, logo este é um ponto de partida para o alinhamento entre dois planos diferentes. De seguida serão explicados estes dois conceitos.

3.4 Planos Organizacionais

Neste capítulo pretende-se definir claramente «planos organizacionais». Este conceito torna-se essencial pois relaciona-se intimamente com o tema central desta dissertação e, para isso, é necessário identificar todos os atributos que o constituem. Foi necessário estudar os conceitos da revisão da literatura, nomeadamente as definições de plano, organização/empresa e às teorias de Thompson, Mintzberg e Chiavenato, tal como é sugerido no seguinte modelo:

Figura 18 - Planos organizacionais (Fonte: Autor)

Num plano não existem desigualdades nem ondulações, logo um plano organizacional tem de ser aplicado universalmente a qualquer nível organizacional sem alterações dos seus atributos (COSTA & MELO, 1999). A partir desta ilação conclui-se que um dos atributos de planos organizacionais é o seu «nível organizacional», logo, a hipótese de estes dois conceitos serem confundidos como sendo iguais não deve ser válida. Um plano organizacional é anterior a nível organizacional e este faz parte dos atributos que ajudam a defini-lo.

Outro atributo para a caraterização inequívoca de um plano organizacional é a sua «designação», como é facilmente compreendido, não podem existir dois planos com a mesma designação para garantir o alinhamento pretendido, sendo que esta refere o nome do plano organizacional.

A cada plano deverá estar associada uma ou mais «Entidades Organizacionais». Este atributo já foi estudado e encontra-se bem definido, com características e atributos próprios, nomeadamente: missão, competências, estrutura, quadro orgânico, designação, dependência e posições organizacionais.

Apesar de cada entidade organizacional ter a sua missão específica, não faz sentido existir um plano organizacional sem uma missão atribuída e, por este motivo, «missão» é também um atributo. Ao considerar a missão deve ter-se em conta que desta deriva uma linha de ação, que inclui estratégias e táticas, bem como diretivas com as respetivas políticas e regras de negócio de cada plano organizacional. Portanto, a missão, segundo o BMM, é representada através dos meios.

As «posições organizacionais», devido à sua elevada importância, para além de serem atributos das entidades organizacionais, também são por si só atributos. Portanto ocupam lugar nas entidades organizacionais e representam os recursos humanos associados a cada plano organizacional, são dotadas de um conjunto de atributos tal como as qualificações, funções e uma designação.

A «estrutura» está, necessariamente, presente em qualquer plano organizacional. Uma estrutura que relaciona as diferentes entidades organizacionais pode ser bastante complexa ou, em última instância, resumir-se a uma única entidade, podendo também variar em termos de verticalidade ou horizontalidade.

Os planos organizacionais estão alinhados verticalmente através de uma «dependência hierárquica» que contribui para o alinhamento pois garante que, em nenhuma circunstância existem saltos indevidos. A correspondência dever ser feita com os planos organizacionais imediatamente acima ou abaixo e, por norma, nas

organizações militares, esta dependência hierárquica está bem delineada. Para garantir que os processos de negócio fluem sem obstáculos ou incompatibilidades dentro de qualquer plano de organizacional, é estritamente necessário que exista uma «semântica» em comum, isto significa que a linguagem falada deve ser a mesma e compreensível por todos. A semântica é um fator de alinhamento praticamente universal, logo não poderia deixar de estar presente como atributo de plano organizacional.

Todo o plano existente só faz sentido se tiver um «fim», caso contrário seria inútil. Segundo o modelo BMM explicitado na revisão literária, um fim é constituído por uma visão, metas e objetivos. Qualquer plano organizacional deve ter o seu fim definido e alinhado com os planos superiores e serve de guia aos planos inferiores.

Figura 19 - Atributos de um Plano Organizacional (Fonte: Autor)

Assim, um plano organizacional é um conceito universal que possibilita a manutenção de uma linha estratégica comum em toda a empresa e estabelece relações com os planos imediatamente superiores e inferiores. É caraterizado por um conjunto de atributos que o identificam inequivocamente: designação, missão, nível

organizacional, dependência hierárquica, entidades organizacionais, posições organizacionais, estrutura, semântica e fim.

3.4.1 Instanciação de um plano organizacional

Estando identificados os atributos que caracterizam os planos organizacionais, a melhor forma de compreender como estes se aplicam e se relacionam, validando também a aplicabilidade deste modelo, é através de um exemplo prático e, para isso, considere-se o plano de nível operacional da FA para fazer uma instanciação:

- **Designação:** Plano operacional;
- **Nível Organizacional:** Nível operacional;
- **Dependência hierárquica:** Superiormente a dependência hierárquica situa-se no plano imediatamente acima, nomeadamente através do CEMFA. Quanto ao plano inferior, cada entidade organizacional tem as suas dependências específicas, tal como sugerido na figura abaixo;
- **Missão:** A missão deste plano consiste em comandar a diferentes unidades funcionais, para isso utiliza os meios descritos nas diferentes entidades organizacionais.
- **Entidades organizacionais:** Neste plano são consideradas três entidades organizacionais: CPESFA, CLAFA e CA.
- **Posições organizacionais:** Estas posições são o somatório das que estão definidas em cada uma das entidades organizacionais;
- **Estrutura:** O plano operacional encontra-se estruturado horizontalmente através de três entidades organizacionais, tal como sugerido na figura seguinte;
- **Semântica:** A semântica é definida através da doutrina existente para este nível organizacional, bem como a doutrina próprias das entidades organizacionais existentes neste plano.
- **Fim:** A visão, metas e objetivos é o somatório das visões, metas e objetivos das diferentes entidades organizacionais.

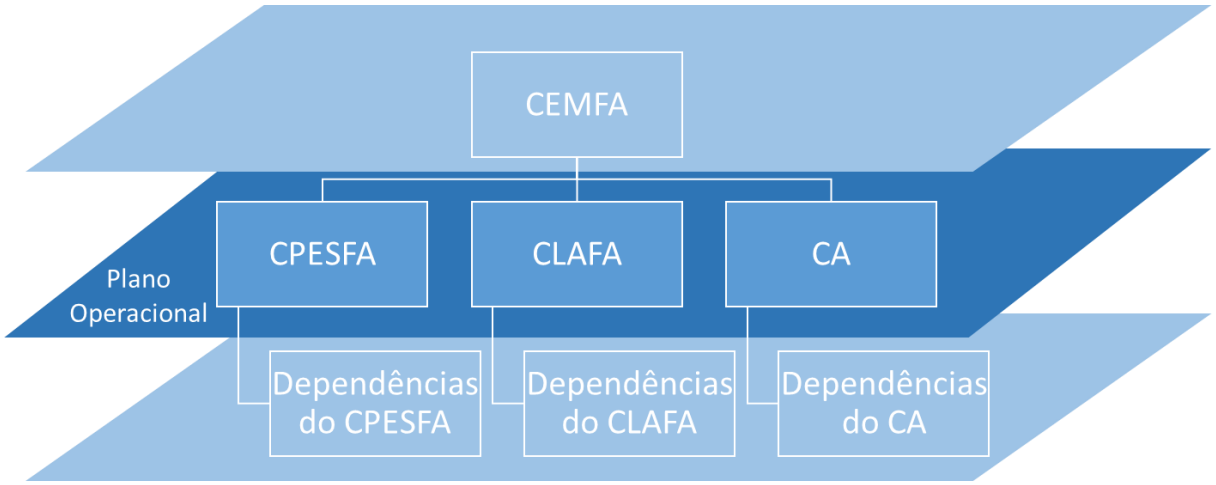


Figura 20 - Plano operacional, estrutura e dependências hierárquicas (Fonte: Autor)

3.5 Modelo de alinhamento entre planos organizacionais

Neste capítulo será proposto um modelo que possibilite o alinhamento entre diferentes planos organizacionais, diz respeito à camada intermédia de alinhamento, pretende-se um modelo universal capaz de ser aplicado a qualquer domínio. Nesta dissertação a validação será efetuada utilizando uma instanciação para o domínio da segurança computacional.

Para a identificação dos fatores de alinhamento foi essencial o contributo da revisão literária, nomeadamente com o conhecimento mais profundo do BMM, ontologias e dos atributos definidos para caraterizar «planos organizacionais». Alguns destes atributos tornam-se praticamente os fatores de alinhamento como é facilmente compreensível. No entanto, é também evidente que cada um destes fatores contribui com pesos distintos para o alinhamento e, para além disso, as caraterísticas de uma organização militar também proporcionam diferentes níveis de maturidade sendo que esta realidade se deve, por exemplo, à estrutura militar bem definida e conhecida intrinsecamente por todos. Assim, não será preciso dedicar a mesma atenção a todos eles, realçando que alguns já se encontram bem definidos e alinhados, outros podem precisar de mais trabalho de desenvolvimento.

Através da análise dos atributos de planos organizacionais foram identificados os seguintes fatores de alinhamento: a «missão», que faz parte dos meios e, por isso, também inclui as «diretivas», os «fins», a «estrutura». A «semântica» através das ontologias e, por fim, com recurso à revisão bibliográfica, nomeadamente através do

BMM, para além dos já indicados, foram identificados ainda os seguintes fatores: os «influenciadores», o «*assessment*» (para efeitos desta dissertação inclui o «*potencial impact*»), e os «meios». Este último reveste-se de elevada importância pois contém a missão, que por si mesma já é um fator de alinhamento, mas irá ser abordada dentro dos «meios» juntamente com as linhas ação, devido à elevada dependência relacional. As diretivas, tratadas à parte, resultam na doutrina da organização e, dada esta importância, os meios serão expandidos durante o estudo dos fatores de alinhamento.

A escolha destes fatores recai no facto de alguns dos atributos definidos para plano organizacional se aproximarem do BMM e assim para a proposta de um modelo de alinhamento coerente, faz sentido utilizar os atributos de «planos organizacionais» utilizando o BMM para os completar ou acrescentar, construindo um modelo mais completo.

A figura seguinte deixa bem explícita a proposta deste modelo de alinhamento, ou seja, o fluxo entre planos organizacionais não pode ser feito aleatoriamente e sem qualquer critério, devendo existir uma ponte bem definida que garanta o alinhamento. O modelo que será apresentado neste capítulo pretende precisamente fazer essa ponte, constituída pelos fatores identificados.

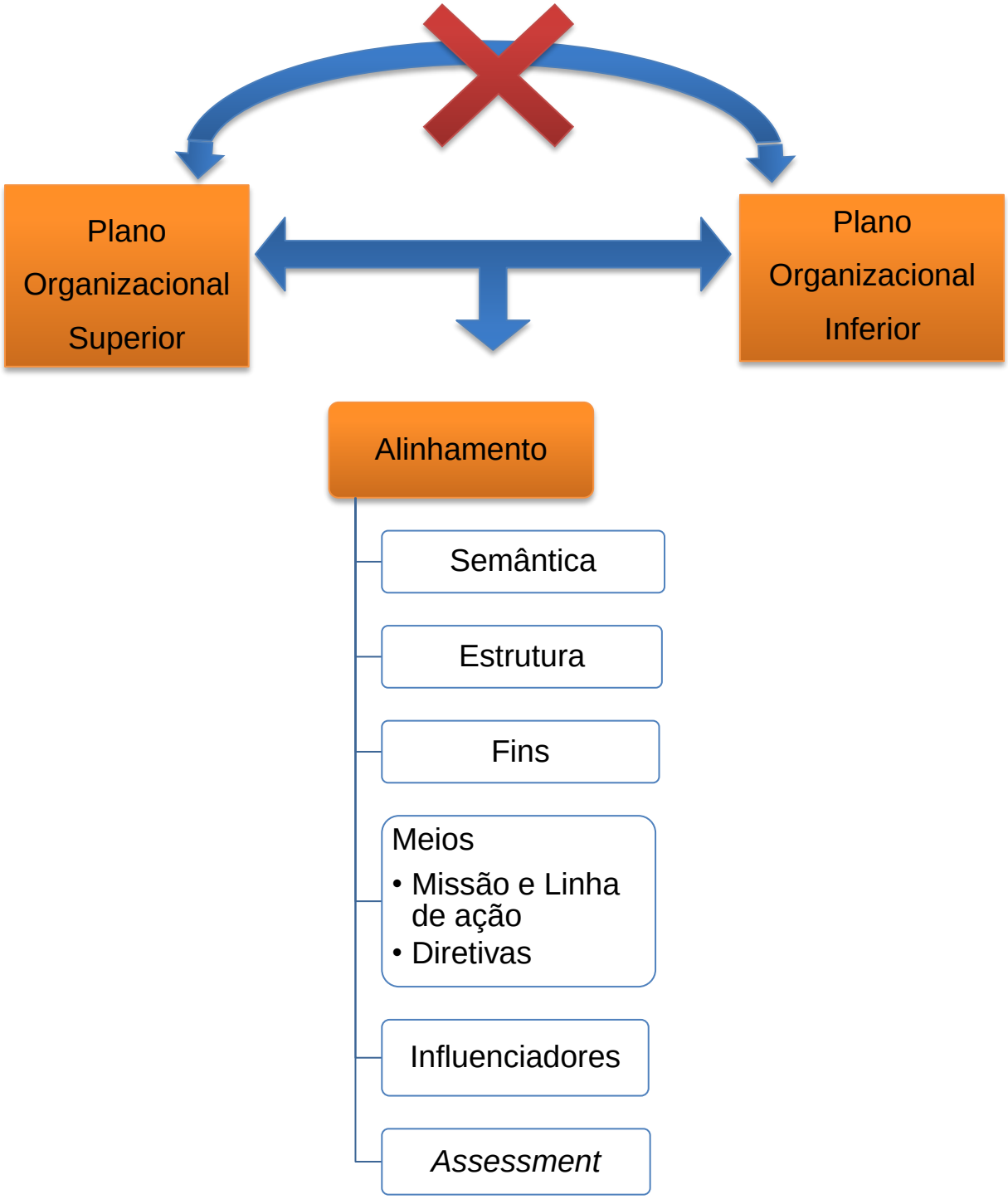


Figura 21 - Modelo de alinhamento entre planos organizacionais (Fonte: Autor)

3.5.1 Semântica

Este fator já é, por si mesmo, universal a qualquer modelo de alinhamento e, no caso desta dissertação, aparece ainda referenciado como sendo um atributo de «plano organizacional».

Estando explícita a sua importância, é necessário encontrar uma forma de garantir a uniformização da semântica em qualquer organização ou domínio desta. Na revisão literária encontra-se a solução, das teorias das ontologias podemos retirar que a existência de uma ontologia é essencial para garantir a semântica, sendo que qualquer organização que pretenda o alinhamento deve possuir um dicionário de termos da empresa, onde esteja definido o que significa cada referência necessária aos processos de negócio.

A falta de uma semântica comum pode levar a falhas no alinhamento entre planos organizacionais com origens, por exemplo, em falhas na comunicação entre diferentes planos. É necessário que um plano inferior saiba exatamente o que lhe é pedido superiormente.

3.5.2 Estrutura

Entenda-se este fator como uma ferramenta de coordenação, planeamento e responsabilização pelo domínio em questão. A existência de uma estrutura bem definida, com responsabilidade nessa área, conduz a uma reflexão, nem que periódica, do tema em questão, fazendo uma avaliação que permite encontrar oportunidades de melhoria.

A existência de uma estrutura proporciona também um fluxo de informação tanto *top-down* como *down-top,* ou seja, uma corrente de informação que tanto pode fluir no sentido descendente, partindo de planos de nível organizacional superior para os inferiores, como no sentido oposto (ascendente), o que por vezes é mais difícil de acontecer devido à cultura extremamente hierarquizada das organizações militares. A existência de representantes dos vários planos nessa estrutura bem como das diferentes entidades organizacionais do mesmo plano potencia esse alinhamento.

Na figura seguinte está exemplificada uma estrutura simples e transversal aos três planos organizacionais comuns em instituições militares. É chefiada por um diretor do domínio da área em questão, e constituída por outros cinco representantes, dois pertencentes ao plano operacional e outros três ao tático, note-se que poderiam

existir variações caso existissem, por exemplo, mais entidades organizacionais ou mais planos.

Para garantir a aplicabilidade deste modelo não basta a existência da estrutura por si só, é necessário que esta funcione corretamente e esta garantia pode ser obtida de duas formas: através de doutrina, que regulamente a sua existência, a periodicidade de reunião, os poderes e responsabilidades que esta detém, e através de uma auditoria externa ao domínio de aplicação que garanta o cumprimento desta doutrina.

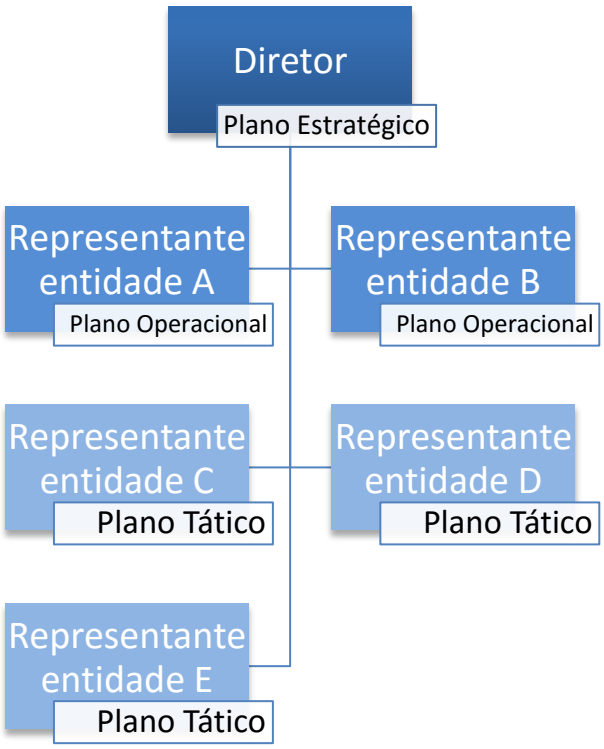


Figura 22 - Estrutura de alinhamento de um domínio (Fonte: Autor)

3.5.3 Fins

Este fator define uma visão, depois de definida estabelece metas e objetivos que concorram para alcançar a visão da organização. Para garantir o alinhamento é necessário que os objetivos concorram para alcançar as metas e estas para alcançar a visão. Por outras palavras, o somatório dos objetivos num plano organizacional deve garantir que as metas sejam alcançadas num plano superior e por sua vez, o somatório das metas deve promover o alcance da visão.

A figura seguinte ilustra este exemplo:

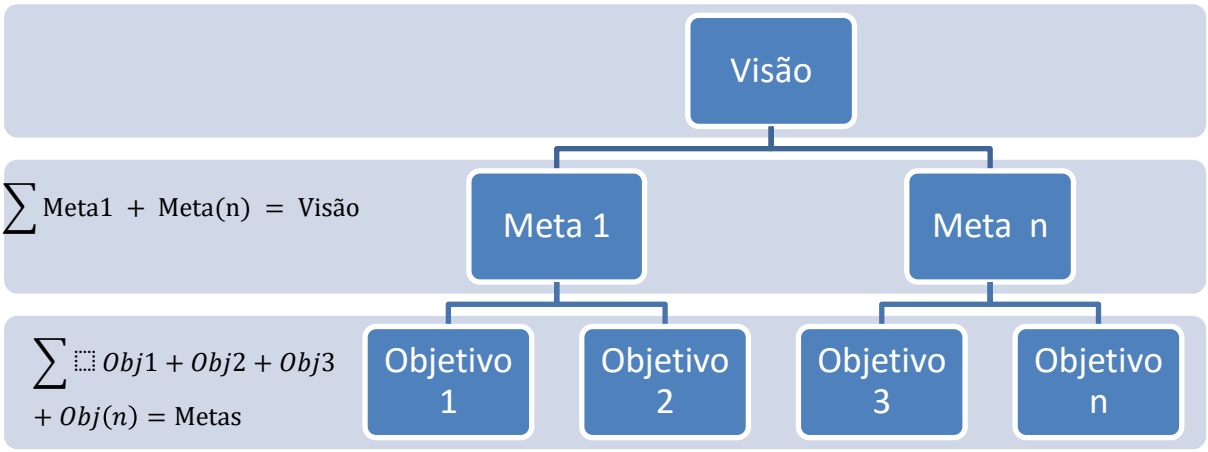


Figura 23 - Modelo dos «fins» (Fonte: Autor)

Este modelo não se esgota numa estrutura de três planos organizacionais pois as metas de um plano podem ser os objetivos de um outro plano superior e assim sucessivamente. De salientar que um objetivo num plano inferior tem de concorrer para satisfazer uma ou mais metas do plano superior, caso contrário existe desalinhamento. Cada meta deve, também, ter mais que um objetivo para a completar garantindo assim o modelo da estrutura da FA.

Para tudo isto ser possível é necessário que tanto a visão como as metas e os objetivos estejam bem especificados na organização, caso contrário torna-se impossível fazer este tipo de deduções para concluir se existe ou não alinhamento.

3.5.4 Meios

Os meios são um fator de alinhamento que devido à elevada pertinência dos seus constituintes foi repartido para melhor se compreender em que medida este tem potencial no modelo proposto e de que forma contribui para o alinhamento entre planos organizacionais.

3.5.4.1 Missão e Linha de ação

A missão é um atributo de plano organizacional mas, para existir alinhamento, a missão dos planos organizacionais inferiores tem de concorrer para a missão dos planos superiores e todas estas para a missão da empresa ou domínio em questão.

Para alcançar a missão é escolhida uma linha de ação que se decompõe em estratégias e táticas. As estratégias são planeadas através da missão e depois implementadas pelas táticas, sendo aqui possível encontrar diferentes planos organizacionais com funções específicas.

A missão está definida pelos planos de topo e, de seguida, num plano inferior de forma a garantir o alinhamento, são formuladas estratégias para que todas elas, sem exceção, concorram para o sucesso da missão. Por último, noutro plano ainda mais abaixo, elaboram-se as táticas e, mais uma vez, todas elas devem promover o sucesso de uma ou mais estratégias.

Não existe nenhuma estratégia ou tática que não concorra para satisfazer alguma outra e tal é demonstrado na figura seguinte, ou seja, todas têm uma dependência. Neste exemplo, o somatório das táticas 1 e 2 vai contribuir para alcançar a estratégia 1, da mesma forma que o somatório de todas as estratégias contribui para a missão.

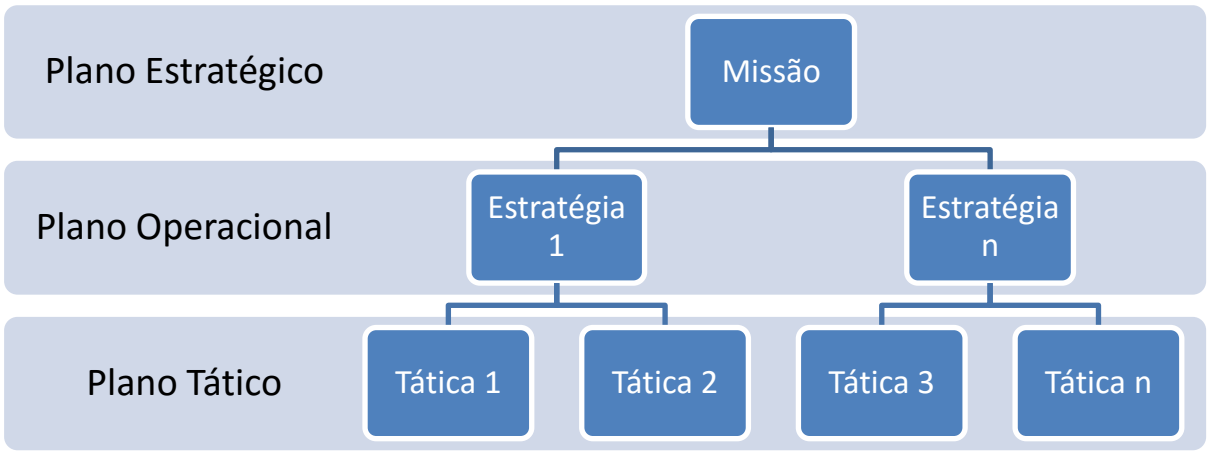


Figura 24 – Modelo dos «meios» (Fonte: Autor)

Este modelo não se esgota nos três planos exemplificados. Numa organização mais segmentada é possível que a estratégia de um plano seja a tática do plano imediatamente superior.

Numa organização com elevada maturidade de *organizacional self-awareness* cada posição organizacional sabe perfeitamente em que medida é que o processo que desempenha - que pertence a determinada tática, por exemplo – contribui para alcançar a missão da organização, ajudando assim a melhorar o alinhamento.

3.5.4.2 Diretivas

Tal como já foi abordado nesta dissertação, a informação é um dos recursos mais perenes nas organizações e alguma desta é espelhada na biblioteca de doutrina produzida. É responsável por descrever todos os processos da empresa bem como a própria estrutura, dependências hierárquicas, níveis de decisão, entidades e posições organizacionais existentes. É na doutrina que todos estes atributos estão descritos e detalhados, o que revela a sua importância acrescida como fator de alinhamento.

Devido à complexidade que é criar este elemento chave, tendo em conta a sua vastidão, é crucial garantir o alinhamento entre as diferentes publicações da organização. Diferentes planos organizacionais são responsáveis por criar diferentes níveis de diretivas e este crescimento é exponencial, o que pode conduzir ao desconhecimento das publicações já existentes, levando a informações duplicadas ou a lacunas devido a pontas esquecidas na legislação. Segundo os princípios da engenharia organizacional, este problema traduz a falta de um critério de alinhamento básico.

As políticas de negócio e as regras de negócio tem funções diferentes, no entanto umas derivam de outras logo torna-se evidente que as políticas têm de se alinhar e concorrer para as regras de negócio. Mais uma vez é aqui estabelecida uma relação de dependência entre dois planos, um responsável por emitir regras e outro, inferior, responsável pelas políticas. Mais uma vez esta pode não se esgotar em dois planos apenas.

É também nas diretivas que se encontram definidos os conceitos fundamentais para a compreensão dos processos de negócio. Isto significa que estas devem conter a semântica da organização, ou seja, a linguagem que deve ser compreendida e falada em qualquer plano organizacional, esse documento deve ser basilar para a organização.

3.5.5 Influenciadores

Existem diferentes tipos de influenciadores que afetam vários planos organizacionais, um exemplo simples é a doutrina proveniente de entidades externas, como o EMGFA, que influencia diretamente os planos superiores mas terá repercussões em toda a organização. No exemplo oposto, existem influenciadores que afetam os planos mais táticos e, caso seja necessário adotar alguma medida, é

necessário que essa informação chegue aos planos capazes de criar diretivas. Estes dois exemplos básicos demostram bem que deve existir alinhamento e que tem de funcionar nos dois sentidos: *top-down* e *down-top.* Para isso, é necessário que todos os influenciadores estejam identificados e sempre que pertinente deve ser feita a sua atualização.

Este fator de alinhamento não está incluído nos atributos de plano organizacional, pois se assim fosse, os próprios planos da organização seriam influenciadores e isso já está previsto na estrutura e dependência hierárquica. No entanto, este é considerado um fator de alinhamento, devido à necessidade de contribuir para que o plano responsável por compilar os influenciadores da organização tenha toda a informação que necessita, sendo todos os planos responsáveis por este processo.

3.5.6 Assessment

O *assessment* é responsável por fazer uma análise de risco e, para isso, precisa de informação sobre os pontos fortes, fracos, ameaças e oportunidades. À semelhança dos influenciadores, este não é atributo de plano organizacional. O plano organizacional responsável por esta tarefa localiza-se num nível superior e para obter um *assessment* consistente tem de recolher informação de todos os planos organizacionais. Assim compreende-se que não faz sentido existir um *assessment* para cada plano mas sim um para a organização, elaborado com o contributo de todos os planos e que todos saibam o que nele está elencado.

Mais uma vez, é necessário garantir o alinhamento para que isto aconteça. Todos os planos têm de ter uma *organizacional self-awareness* que lhes permita perceber a importância desta análise de risco e compreender as informações relevantes a fornecer e posteriormente interiorizar o *assessment.*

3.6 Fatores e matriz de alinhamento

O modelo de alinhamento que é proposto pretende estabelecer a relação entre dois planos organizacionais segundo uma série de fatores de alinhamento já enumerados. Estas relações são válidas para quaisquer dois planos entre qualquer nível organizacional.

Para este alinhamento ser facilmente implementado, os fatores de alinhamento já propostos foram resumidos e compilados em regras de alinhamento representadas na seguinte matriz em forma de *checklist*:

Tabela 2 **- Matriz de alinhamento (Fonte: Autor)**

Fatores		Regras de alinhamento	
A1	**Semântica**	**RA 1.1**	O PS deve ter um dicionário de semântica elaborado
		RA 1.2	O PI deve referenciar o dicionário de semântica do PS
A2	**Estrutura**	**RA 2.1**	Deve existir um estrutura bem definida por um PS
		RA 2.2	Todos os planos devem ter um representante na estrutura
		RA 2.3	Todas as entidades organizacionais devem ter um representante na estrutura
A3	**Fins**	**RA 3.1**	Deve existir uma visão no PS
		RA 3.2	As metas do PI devem ser coerentes com a visão do PS
		RA 3.3	Todas as metas do PI, sem exceção, devem concorrem para a visão do PS
		RA 3.4	O somatório das metas num PI deve cumprir a visão do PS
		RA 3.5	Os objetivos do PI devem ser coerentes com as metas do PS
		RA 3.6	Todos os objetivos de um PI, sem exceção, devem concorrer para as metas do PS
		RA 3.7	O somatório dos objetivos do PI deve cumprir as metas do PS
A4	**Missão e Linha de ação**	**RA 4.1**	Deve existir uma missão no PS
		RA 4.2	As estratégias do PI devem ser coerentes com a missão do PS
		RA 4.3	Todas as estratégias de um PI, sem exceção, devem concorrer para a missão de um PS
		RA 4.4	O somatório das estratégias num PI deve cumprir na missão do PS
		RA 4.5	As táticas do PI devem ser coerentes com as estratégias do PS
		RA 4.6	Todas as táticas do PI, sem exceção, devem concorrer para as estratégias do PS
		RA 4.7	O somatório das táticas do PI deve cumprir as estratégias do PS
A5	**Diretivas**	**RA 5.1**	O PS deve ter uma biblioteca de doutrina, atualizada e de fácil leitura
		RA 5.2	As políticas de negócio de um PI devem concorrer para as regras de negócio de um PS
A6	**Influenciadores**	**RA 6.1**	O PS deve ter uma lista de influenciadores da organização
		RA 6.2	Os PI devem indicar os influenciadores que os afetam ao PS
		RA 6.3	Os PI devem conhecer a lista de influenciadores
A7	***Assessment***	**RA 7.1**	O PS deve ter um *assessment* da organização
		RA 7.2	Os PI devem indicar as fragilidades, ameaças, oportunidades e pontos fortes ao PS
		RA 7.3	Os PI devem conhecer o *assessment* da organização

3.7 Validação

Esta dissertação tem como objeto de estudo o alinhamento dos diferentes planos organizacionais e, após a proposta do modelo apresentado, importa validá-lo através de uma instanciação, utilizando uma área tão complexa como a segurança computacional. Para isso é necessário ter um conhecimento minimamente aprofundado sobre este domínio na FA, recorrendo-se à revisão bibliográfica efetuada no capítulo dois.

A figura seguinte deixa bem explicita a proposta deste modelo de alinhamento, ou seja, o fluxo entre os planos organizacionais não pode ser feito aleatoriamente e sem qualquer critério, deve existir uma ponte bem definida que garanta o alinhamento de forma a não existir qualquer incompatibilidade ou pedaço de informação esquecido em toda a FA. Mas, a partir deste momento, o domínio em questão é o da segurança computacional e as relações efetuam-se entre planos pertencentes à segurança computacional. O modelo que será apresentado neste capítulo pretende precisamente fazer essa ponte.

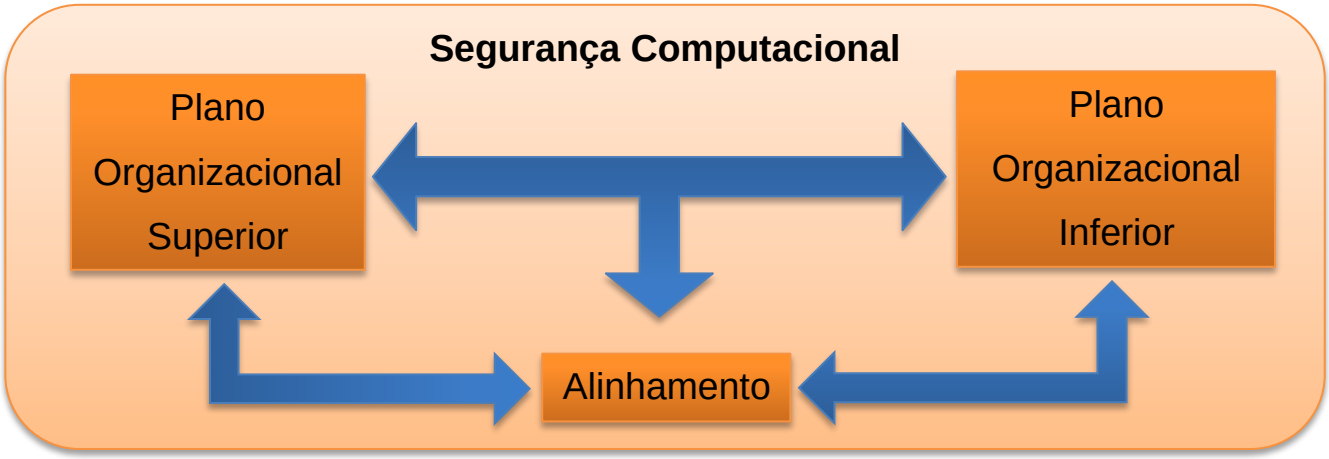


Figura 25 - Modelo de alinhamento entre planos (Fonte: Autor)

Recorrendo à «matriz de alinhamento» e utilizando-a como um *checklist,* é possível fazer uma avaliação inicial daquilo que já existe ou precisa de ser trabalhado no domínio da segurança computacional. De seguida, será feita uma análise mais detalhada destes fatores de alinhamento com algumas propostas para aqueles que estão em falta.

Tabela 3 - Matriz de validação (Fonte: Autor)

Fatores		Regras de alinhamento		Estado
A1	**Semântica**	RA 1.1	O PS deve ter um dicionário de semântico elaborado	X
		RA 1.2	O PI deve referenciar o dicionário de semântica do PS	X
A2	**Estrutura**	RA 2.1	Deve existir um estrutura bem definida por um PS	Sim
		RA 2.2	Todos os planos devem ter um representante na estrutura	Sim
		RA 2.3	Todas as entidades organizacionais devem ter um representante na estrutura	Sim
A3	**Fins**	RA 3.1	Deve existir uma visão no PS	Sim
		RA 3.2	As metas do PI devem ser coerentes com a visão do PS	Sim
		RA 3.3	Todas as metas do PI, sem exceção, devem concorrem para a visão do PS	Sim
		RA 3.4	O somatório das metas num PI deve cumprir a visão do PS	Sim
		RA 3.5	Os objetivos do PI devem ser coerentes com as metas do PS	Sim
		RA 3.6	Todos os objetivos de um PI, sem exceção, devem concorrer para as metas do PS	Sim
		RA 3.7	O somatório dos objetivos do PI deve cumprir as metas do PS	Sim
A4	**Missão e Linha de ação**	RA 4.1	Deve existir uma missão no PS	Sim
		RA 4.2	As estratégias do PI devem ser coerentes com a missão do PS	Sim
		RA 4.3	Todas as estratégias de um PI, sem exceção, devem concorrer para a missão de um PS	Sim
		RA 4.4	O somatório das estratégias num PI deve cumprir a missão do PS	Sim
		RA 4.5	As táticas do PI devem ser coerentes com as estratégias do PS	Sim
		RA 4.6	Todas as táticas do PI, sem exceção, devem concorrer para as estratégias do PS	Sim
		RA 4.7	O somatório das táticas do PI deve cumprir as estratégias do PS	Sim
A5	**Diretivas**	RA 5.1	O PS deve ter uma biblioteca de doutrina, atualizada e de fácil leitura	X
		RA 5.2	As políticas de negócio de um PI devem concorrer para as regras de negócio de um PS	Sim
A6	**Influenciadores**	RA 6.1	O PS deve ter uma lista de influenciadores da organização	X
		RA 6.2	Os PI devem indicar os influenciadores que os afetam ao PS	X
		RA 6.3	Os PI devem conhecer a lista de influenciadores	X
A7	***Assessment***	RA 7.1	O PS deve ter um *assessment* da organização	Sim
		RA 7.2	Os PI devem indicar as fragilidades, ameaças, oportunidades e pontos fortes ao PS	X
		RA 7.3	Os PI devem conhecer o *assessment* da organização	X

Durante a construção do modelo foram identificadas três origens para a escolha dos fatores de alinhamento, os atributos de planos organizacionais, as ontologias e o BMM. Por este motivo, uma maneira prática de contribuir para a promoção este alinhamento é a construção do BMM para o domínio da segurança computacional em cada um dos fatores de alinhamento e, fazendo isto, uma vez que é um modelo bastante consistente e com provas dadas, garantimos que nada fica esquecido.

De seguida, e ainda como forma de validação será interpretada a análise feita para o domínio da segurança computacional na FA com algumas propostas de melhoria e alinhamento naqueles fatores que estão mais em falta.

3.7.1 A semântica como fator de alinhamento

Como ficou explícito na revisão literária, a existência de uma ontologia – semântica – é um fator de alinhamento universal e, para isso, é necessária a existência de uma lista de conceitos ou dicionário de semântica que defina bem a organização. Na FA não existe uma lista pura de conceitos, no entanto algumas publicações refletem definições que lhes dizem respeito. Isto é uma prova da falta de alinhamento, pois pode resultar em faltas ou duplicação de conceitos. A proposta para melhorar o alinhamento da semântica na área da segurança computacional na FA é, assim, a criação de uma lista de conceitos, de forma a garantir que é utilizada a mesma linguagem em todos os planos organizacionais.

Deste modo, seria possível satisfazer o ponto FA 1 da matriz de alinhamento proposta.

3.7.2 A estrutura como fator de alinhamento

A necessidade da estrutura como fator de alinhamento provém dos atributos de «plano organizacional». Da investigação realizada e das entrevistas efetuadas, constatou-se que a estrutura da segurança computacional é o fator que apresenta um maior grau de maturidade, estando já bem definida, talvez pelo caráter de instituição militar. A estrutura atualmente definida, que constitui um fator de alinhamento, é a seguinte:

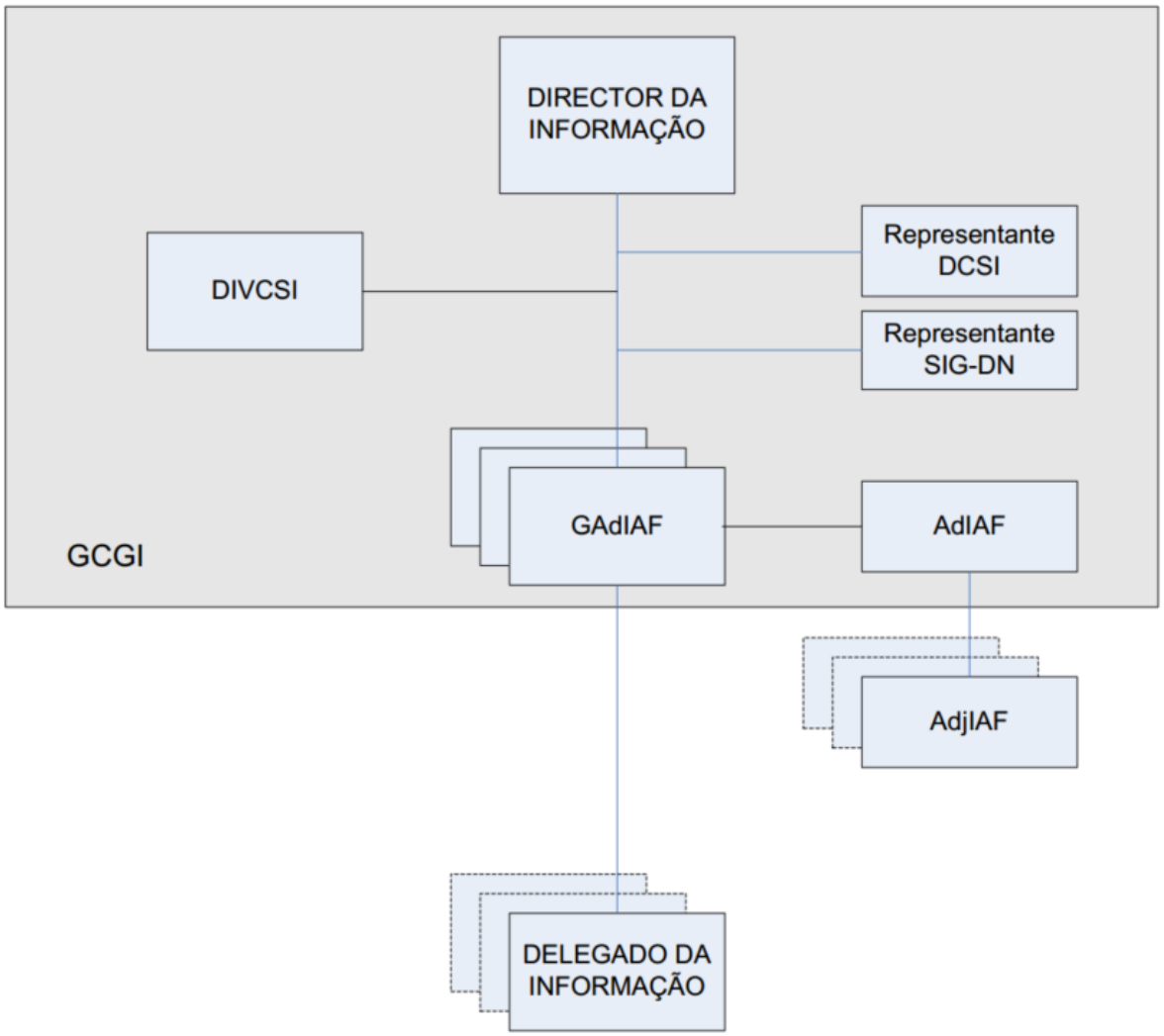


Figura 26 - Estrutura da segurança computacional na FA (Força Aérea RFA 391-1 , 2011)

Como é possível ver através da figura, esta satisfaz todos os fatores de alinhamento da estrutura (FA 2.1, FA 2.2, FA 2.3) pois, através do grupo coordenador de gestão de informação existe uma estrutura para a segurança computacional bem definida, com representantes de todos os planos e entidades organizacionais pertinentes para este domínio.

3.7.3 Os fins como fator de alinhamento

Os **fins** incluem a visão e os resultados desejados e são retirados da construção do BMM para o domínio da segurança computacional na FA.

A **visão** da segurança computacional encontra-se no plano diretor de sistemas de informação e é definida como:

- Ter reconhecidas capacidades C3 e serviços SI/TIC orientados para a missão, interoperáveis, seguros e resilientes, que sustentem os objetivos estratégicos da Força Aérea (Força Aérea, 2015)

Com esta proposta de visão fica satisfeito o ponto FA 3.1 da matriz de alinhamento.

Os **resultados desejados** incluem as metas e os objetivos:

As **metas** encontram-se presentes no Plano Diretor dos Sistemas de Informação.

Os **objetivos** são construídos com base nas metas definidas e, encontram-se definidos no plano de atividades, contribuindo assim para os fatores de alinhamento FA 3.

3.7.4 Missão e Linha de ação

Os **meios** incluem a missão, as linhas de ação e as diretivas.

A **missão** encontrada para completar este modelo é proveniente do plano diretor dos sistemas de informação da FA e vem referida como:

- Gerir e preservar os produtos de informação envolvidos nos processos de negócio que suportam as diversas capacidades operacionais necessárias para o cabal cumprimento da missão da Força Aérea, através do estudo, desenvolvimento e disponibilização de serviços SI/TIC orientados para a missão, interoperáveis, seguros e resilientes (Força Aérea, 2015).

As linhas da ação incluem as estratégias e as táticas.

As estratégias encontram-se presentes no Plano Diretor dos Sistemas de Informação.

As táticas baseiam-se no Plano Diretor dos Sistemas de Informação e estão espelhadas no plano de atividades contribuindo assim para os fatores de alinhamento FA 4.

3.7.5 As diretivas como fator de alinhamento

As diretivas incluem as regras de negócio e as políticas de negócio, estas incluem-se nos meios do BMM, mas dada a sua importância como fator de alinhamento foi importante destacá-las nesta dissertação.

Para garantir o alinhamento entre os planos organizacionais, é necessário que as políticas e as regras de negócio sejam pertinentes ao plano em questão e que estejam atualizadas e bem identificadas para serem facilmente acedidas em caso de necessidade. Diferentes planos podem ser responsáveis por elaborar diferentes níveis de publicações mas, por norma, planos superiores são responsáveis por políticas e planos inferiores por regras de negócio tendo, no entanto, a certeza que as regras se alinham para cumprir as políticas estabelecidas.

Durante a revisão bibliográfica ficou notória a falta de alinhamento detetada ao nível do edifício das publicações sobre a segurança computacional na FA, sendo igualmente destacado durante a realização de entrevistas. Foi proposta a seguinte alteração:

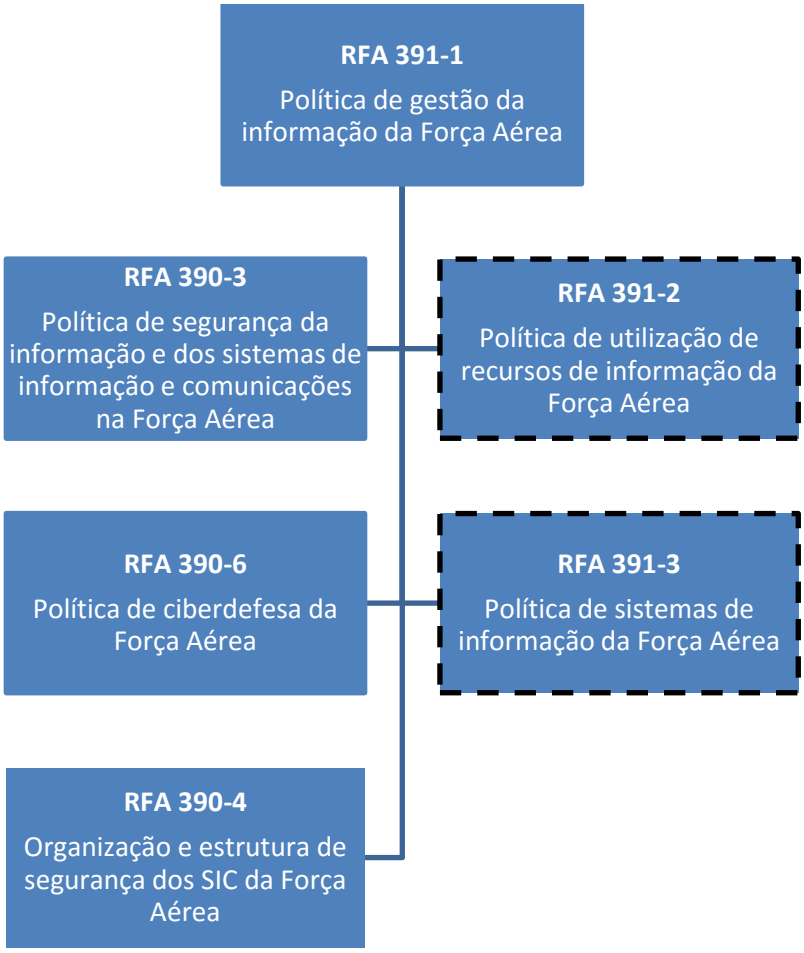


Figura 27 - Proposta de edifício de publicações da FA (Fonte: Autor)

A alteração resulta da inclusão do RFA 390-6 e do RFA 390-4. Fica também a nota de urgência na elaboração dos manuais em falta, sinalizados a tracejado na figura.

Apesar desta proposta, aqui encontra-se apenas uma pequena parte da doutrina deste domínio e por isso um pequeno contributo para o alinhamento, existindo ainda mais a incluir. A existência de uma arquitetura que englobe todas as diretivas poderia satisfazer o fator de alinhamento FA 5.1 e ajudar no FA 5.2

As políticas de negócio são diretivas generalistas cujo propósito é governar a empresa, fornecendo as linhas orientadoras básicas para as regras de negócio. Elas existem para controlar as estratégias, táticas e processos e, em comparação com as regras de negócio, são menos precisas e objetivas. Estas diretivas têm origem em planos hierarquicamente superiores.

As regras de negócio são, por norma, bastante específicas e estruturantes e fornecem, por exemplo, restrições, autorizações e linhas orientadores em áreas específicas da empresa ou organização. Estas têm origem em planos hierárquicos inferiores comparativamente às políticas de negócio, no entanto têm de estar alinhadas no sentido de satisfazer estas últimas. Durante a investigação não foi detetado nenhum caso onde existisse esta falta de alinhamento portanto, considera-se que o fator de alinhamento FA 5.2 se cumpre, mas que seria necessário um estudo mais exaustivo de todas as diretivas referentes a este domínio para obter a exatidão necessária e para a construção de uma arquitetura de publicações mais completa.

3.7.6 Os influenciadores como fator de alinhamento

Os **influenciadores** podem ser externos ou internos. Durante a investigação foram feitas algumas referências a influenciadores em publicações e outras nas entrevistas efetuadas, contudo não espelham a importância que estes devem ter como um fator de alinhamento.

Os influenciadores externos são todos aqueles que indiretamente influenciam a Força Aérea. No RFA 390-6, Política de Ciberdefesa da Força Aérea, são identificados os seguintes:

- Polícia Judiciária através da secção central de investigação da criminalidade informática e telecomunicações;
- Autoridade Nacional de Comunicações (ANACOM);
- Comissão Nacional de Proteção de Dados (CNPD);
- Gabinete Nacional de Segurança (GNS);
- Centro de Coordenação da CRISI (CC-CRISI) conjunto aos três ramos;

- Grupo de Resposta a Incidentes de Segurança Informática (GRISI) conjunto aos três ramos.

Outros influenciadores externos identificados através das entrevistas são:

- NATO, pela sua política de ciberdefesa;
- União Europeia;
- EMGFA, através dos PEMGFA

Os influenciadores internos não se encontram definidos na doutrina existente na FA portanto, os influenciadores internos identificados, resultam das entrevistas efetuadas e foram definidos os seguintes:

- Constrangimentos operacionais;
- Estrutura hierárquica;
- Infraestruturas.

Esta resumida compilação de influenciadores vem ajudar a satisfazer os pontos FA 6.1 e FA 6.3, no entanto não se revela suficiente. Seria necessário dedicar a devida importância a este fator, elaborando diretivas que promovessem a partilha dos influenciadores dos diversos planos organizacionais com a finalidade de construir uma lista detalhada, responsabilidade de um plano superior, para ser difundida e interiorizada por toda a organização, numa verdadeira cultura de *organizacional self-awareness* e, mais especificamente, de *security awareness* possibilitando assim que se cumprissem claramente os pontos FA 6.2 e FA 6.3.

3.7.7 O *assessment* como fator de alinhamento

O *assessment* é um julgamento sobre os influenciadores que podem afetar a utilização dos meios ou o alcance dos fins, isto é, o *assessment* expressa uma conexão lógica entre os influenciadores e os meios e fins, indicando quais são relevantes. O *assessment* é feito através de uma análise SWOT a cada influenciador, concluindo quais são os pontos fortes e fracos, as oportunidades ou ameaças da empresa.

A doutrina da FA, através do RFA 390-3 ponto 303 aborda o tema da análise de risco ou o *assessment* apesar de, na opinião do autor, não ser dado o devido destaque para que este sirva de fator de alinhamento.

Qualquer sistema que processe, armazene ou transmita informação classificada deve ser sujeito a um processo de análise de risco durante todo o seu

ciclo de vida. Este processo traduz-se na identificação das ameaças e vulnerabilidades dos SIC, na determinação da sua magnitude e na identificação das áreas que necessitem da implementação de contra medidas. O objetivo deste *assessment* é encontrar uma solução que seja o equilíbrio entre os requisitos de utilização, o custo e o risco de segurança. Após todas as medidas terem sido implementadas considera-se sempre que existe um risco residual, atribuído a ameaças não conhecidas e vulnerabilidades que não poderão ser eliminadas ou reduzidas (Força Aérea RFA 390-3, 2008).

Presente no capítulo 2 do RFA 390-6, Política de Ciberdefesa da Força Aérea, podemos encontrar a tipificação das ameaças à instituição de onde podemos extrair as ameaças e vulnerabilidades da FA.

Deste modo, para fazer o *assessment* através de uma análise SWOT devemos considerar as seguintes ameaças:

- Ataque *botnet*. Permite a um atacante, localizado remotamente, o controlo de uma rede virtual constituída por computadores ”infetados” (*zombies)* e manipulá-la para a execução de ações maliciosas (Força Aérea RFA 390-6, 2011);
- *Software* malicioso. Aplicações que são instaladas sem o conhecimento do utilizador e que executam ações destinadas a provocar danos (Força Aérea RFA 390-6, 2011);
- *Hoaxes* (embustes). Divulgação de supostas vulnerabilidades ou ocorrência de falsos incidentes de segurança que poderão aumentar a ameaça num fenómeno de imitação, fragilizando as defesas da organização e sobrecarregando as redes; (Força Aérea RFA 390-6, 2011)
- *Phising.* Esta ameaça consubstancia-se no envio de *e-mails* forjando uma identidade falsa com o intuito de obter informação privada do utilizador (Força Aérea RFA 390-6, 2011);
- Incidentes de segurança informática. É uma expressão genérica para abranger um grande e diversificado número de ameaças aos sistemas. Poderá envolver qualquer ação ou conjunto de ações que comprometam a confidencialidade, integridade ou o desempenho de uma rede de comunicações de dados ou sistema computacional. (Força Aérea RFA 390-6, 2011) Os incidentes mais comuns são:

- Falsidade informática. A intenção de provocar engano, introduzir, modificar, apagar ou suprimir dados informáticos ou interferir num tratamento informático de dados (Força Aérea RFA 390-6, 2011);
- Interferência em sistema informático. A ação intencional e não autorizada ou a tentativa de impedir ou interromper gravemente o funcionamento do sistema informático, introduzindo, transmitindo, danificando, apagando, deteriorando, alterando, suprimindo ou tornando inacessível qualquer componente de *software* ou *hardware* (Força Aérea RFA 390-6, 2011)*;*
- Acesso ilegítimo a sistema. Acesso ou tentativa de acesso intencional e não autorizado à totalidade ou a parte do sistema informático (Força Aérea RFA 390-6, 2011);
- Interferência em dados. Ato intencional e não autorizado ou a tentativa de apagar, danificar, deteriorar, alterar, suprimir ou tornar inacessíveis dados do sistema informático (Força Aérea RFA 390-6, 2011);
- Recolha não autorizada de informação sobre sistema informático. Ato intencional e não autorizado de reunir informação sobre redes e sistemas informáticos (Força Aérea RFA 390-6, 2011);
- Violação de direitos de autor. Violação de propriedade intelectual, independentemente dos conteúdos serem constituídos por informação, código fonte, gráficos ou quaisquer outros elementos do sistema informático protegidos por direitos de autor (Força Aérea RFA 390-6, 2011);
- Mensagem de correio eletrónico não solicitada (spam). Receção ou o envio de mensagens de correio eletrónico não solicitadas, quer sejam produzidas para efeitos de marketing direto ou sem motivação aparente (Força Aérea RFA 390-6, 2011);
- Outras violações de segurança. Outra alegada violação da política de segurança informática aprovada (Força Aérea RFA 390-6, 2011).

Para além destas são ainda identificadas ameaças no PDSI, nomeadamente:

- Cortes Orçamentais (Força Aérea, 2015);
- Impacto na organização SI/TIC da FA da Restruturação da Estrutura Superior das Forças Armadas (Força Aérea, 2015);
- Falta de estratégia conjunta sobre os SI/TIC (Força Aérea, 2015);

- Dependência de SI/TIC não controlados pela FA (SIG-DN) (Força Aérea, 2015).

No RFA 390-6 são identificadas algumas fragilidades que devem ser tidas em conta na análise SWOT, são elas:

- *Cloud computing.* Consiste na utilização de recursos de computadores e servidores partilhados e interligados por meio da *Interne*t. O armazenamento de dados é feito em servidores que poderão ser acedidos de qualquer parte, bem como a programas e serviços formando uma "nuvem de informação" permanentemente *online;* (Força Aérea RFA 390-6, 2011)
- Redes sociais. A partilha de informações, mesmo que de forma inadvertida, poderá constituir um grave comprometimento de operações militares. Fotografias de grupo, de teatros de operações, dos locais de trabalho com a revelação das funções e localização de infraestruturas, a divulgação de comentários pessoais sobre situações políticas ou operacionais, poderão provocar danos sem que o utilizador tenha consciência desse facto; (Força Aérea RFA 390-6, 2011)
- Engenharia social. Esta vulnerabilidade é das mais importantes para o tema desta dissertação, o fator humano é o elo mais fraco numa cadeia complexa constituída por equipamentos, aplicações e procedimentos de operação e manutenção. A engenharia social consiste no conjunto de práticas usadas para obter acesso a informação ou aos sistemas que a processem, por meio de engano ou exploração da confiança das pessoas. Apenas uma formação de segurança adequada e contínua poderá preparar os utilizadores para lidar com quebras suspeitas de protocolo e procedimentos. (Força Aérea RFA 390-6, 2011)

No PDSI são identificadas as seguintes fraquezas:

- Falta de maturidade dos processos internos da área dos SI/TIC (Força Aérea, 2015);
- A organização SI/TIC não responde às necessidades atuais da FA (Força Aérea, 2015);
- Alta rotatividade no desempenho das funções (Força Aérea, 2015);
- Quantidade insuficiente de profissionais da área TIC e difícil retenção dos mesmos (Força Aérea, 2015);

- Falta de formação contínua para os profissionais da área SI/TIC; Parque Informático de postos de trabalho desatualizado (Força Aérea, 2015);
- Desenvolvimento *ad hoc* de SI/TIC, fora do controlo da organização SI/TIC;
- Inexistência de uma arquitetura empresarial de referência na FA (Força Aérea, 2015);
- Falta de ferramentas de apoio à análise de informação para o suporte à decisão (*Business Intelligence*) (Força Aérea, 2015);
- Baixa maturidade da Gestão da Informação e do seu ciclo de vida (Força Aérea, 2015);
- Falta de plano de continuidade de serviços, bem como de testes recuperação a falhas (Força Aérea, 2015);
- Várias gerações de SI em produção (*legacy*) (Força Aérea, 2015);
- Número muito vasto de SI em produção (Força Aérea, 2015);
- Falta de publicitação interna dos serviços TIC disponível, bem como falta de *feedback* dos utilizadores sobre esses mesmos serviços (Força Aérea, 2015);
- Falta de largura de banda e redundância nas comunicações entre unidades (Força Aérea, 2015);
- Falta de ferramentas de gestão e administração das TIC (Força Aérea, 2015);
- Falta de estratégia clara sobre as TIC (Força Aérea, 2015);
- Falta de manuais, circulares e diretivas técnicas (Força Aérea, 2015);

Com recurso às entrevistas foi possível identificar outra fragilidade identificada claramente pelos entrevistados:

- Recursos financeiros**.** Este é o recurso básico e necessário para manter ou adquirir novos sistemas de segurança, investir na formação.

Ainda parte do *assessment* podemos identificar os pontos fortes da segurança computacional na FA:

- Formação e qualificação do pessoal da área dos SI/TIC (Força Aérea, 2015);
- Adaptabilidade a novas situações decorrente da especificidade militar (Força Aérea, 2015);
- Existência de algum enquadramento doutrinário sobre os SI/TIC (Força Aérea, 2015);
- Edificação de novas funcionalidades SI/TIC (Força Aérea, 2015);

- Conhecimento acumulado no desenvolvimento de SI organizacionais de acordo com os requisitos funcionais (Força Aérea, 2015);
- Utilização da metodologia SCRUM no desenvolvimento de SI (Força Aérea, 2015);
- Definição clara de dois ambientes de desenvolvimento: *OutSystems* (Java) e PHP (Força Aérea, 2015);
- Estrutura tecnológica consolidada (Força Aérea, 2015);
- Não dependência de entidades externas para manter as TIC (Força Aérea, 2015);
- Bom nível de equipamento nas TIC na generalidade (Força Aérea, 2015);
- Capacidade de adaptação a novas realidades e tecnologias TIC (Força Aérea, 2015);
- Existência de sistemas TIC complexos, seguros e com boa prestação na disponibilização de serviços a vários níveis (Força Aérea, 2015);
- Utilização preferencial de *software open source* (Força Aérea, 2015);
- Não dependência de fabricantes específicos de *hardware* e de *software* (Força Aérea, 2015);
- Existência de uma plataforma (*Easy* Vista) que implementa o ITIL (Força Aérea, 2015).

Para além destes pontos fortes, através das entrevistas realizadas foram ainda encontrados os seguintes:

- Tecnologia e sistemas decriptação atuais;
- GNS como entidade externa que audita a própria estrutura de segurança;
- Disponibilidade do pessoal.

Para terminar a análise SWOT falta identificar as oportunidades, no PDSI são identificadas as seguintes:

- Surgimento de novas tecnologias (Força Aérea, 2015);
- Aumento da qualidade, disponibilidades e suporte das soluções *open source* (Força Aérea, 2015);
- Efeitos da Resolução de conselho de Ministros (RCM) 12/2012, sobre a governação e racionalização das TIC (Força Aérea, 2015);
- Efeito positivo junto da Sociedade Civil das missões de índole não militar da FA (Força Aérea, 2015);

- Programa Portugal 2020 (Força Aérea, 2015);
- Ênfase que a NATO tem atribuído à consolidação doutrinária no âmbito do C3, da GI e das TIC (Força Aérea, 2015);
- Maior predisposição de colaboração quer com outras entidades do MDN, quer de outros ministérios (Força Aérea, 2015);
- Portugal como *leading nation* do Grupo de Trabalho NATO "Multinacional *Ciber Defence Education and Training Project* (MN CD E&T)" que faz parte da NATO *Smart Defence Initiative* (Força Aérea, 2015);
- Predisposição da sociedade civil e das autoridades civis para a problemática da cibersegurança e ciberdefesa (Força Aérea, 2015);
- Lei de Programação Militar (LPM) (Força Aérea, 2015).

4 Conclusão e Recomendações

No último capítulo desta dissertação é sintetizado todo o trabalho desenvolvido. Serão apresentadas as conclusões finais e recomendações a aplicar na Força Aérea bem como propostas de novos trabalhos de investigação relacionados com o tema.

4.1 Conclusão

Segundo o processo de investigação de Raymond Quivy e Luc Van Campenhoudt (1998), seguido nesta dissertação, as conclusões são o culminar do projeto. A tabela seguinte resume o desenvolvimento da metodologia adotada:

Tabela 4 - Comparação entre metodologia de investigação e trabalho realizado (Fonte: Autor)

Fase	Etapa	Atividades realizadas
Rutura	Pergunta de Partida	Esta etapa, tal como o próprio nome indica, marca o início do trabalho. A escolha de uma pergunta relacionada com o tema mas sendo abrangente o suficiente foi essencial para definir uma linha orientadora de todo o trabalho.
	Exploração	Após a temática estar definida, foi necessário construir uma base de conhecimentos enquadradores para a dissertação. Este passo representa o início da investigação.
	Problemática	Nesta fase é feita a ponte entre a fase de rutura e o início da elaboração de uma linha de pensamento. Foi definido o âmbito e o objetivo do trabalho. A partir deste momento o projeto começou a ganhar mais alguma forma no pensamento do autor.
Construção	Construção do Modelo de Análise	Esta fase representa grande parte do trabalho dedicado a esta dissertação, constituída pela Revisão Literária e desenvolvimento do modelo. Na primeira parte foram identificados e interiorizados os conceitos que depois viriam a revelar-se pertinentes para o início da construção do modelo de alinhamento.
Verificação	Observação	Esta etapa, a par com a anterior, foi o momento de construção e finalização do modelo de alinhamento.
	Análise das Informações	Construído o modelo proposto foi necessário procurar uma validação e, para isso recorreu-se a uma instanciação no domínio da segurança computacional na FA.
	Conclusões	Por último, para terminar a dissertação, o autor expõem as conclusões retiradas da elaboração deste trabalho. É também o momento de identificar futuras propostas de trabalho que se tenha revelado pertinentes.

Recordando o trabalho realizado, no capítulo um foi definido o caminho para esta dissertação através do objetivo, âmbito, pergunta de partida e perguntas derivadas. Assim, é importante destacar:

Objetivo: Construção de um modelo que permita alinhar os diferentes planos organizacionais de um domínio ou empresa.

Âmbito: Transversal a todos os planos organizacionais da Força Aérea, posteriormente, durante a validação, será restringido ao domínio da segurança computacional.

Pergunta de partida: Até que ponto é possível identificar um modelo na FA que permita o alinhamento de processos nos diferentes planos organizacionais?

Para ajudar na investigação, a pergunta de partida foi decomposta nas seguintes questões derivadas:

Q1 – Existe na Força Aérea um modelo holístico de alinhamento sobre a segurança computacional?

Q2 – O *Business Motivation Model* pode ser um modelo que permite modelar qualquer organização ou parte dela, promovendo o alinhamento entre os vários planos organizacionais?

As hipóteses formuladas para responder às questões foram as seguintes:

H1 – Não existe um modelo holístico, apenas alguma doutrina, em determinadas áreas de maior interesse, que pode ser utilizada para construir um modelo mais abrangente.

H2.1 – É possível utilizar o BMM para modelar corretamente qualquer organização, limitando assim a existência de falhas não previstas.

H2.2 – Devido à especificidade de determinados modelos de negócio, o BMM não pode ser aplicado universalmente.

No capítulo dois foi identificado um conjunto de conhecimentos que permitiu adquirir uma base consistente para o desenvolvimento do modelo, sendo aqueles que mais se destacam os seguintes:

- Empresa/Organização: Consiste numa coleção de organizações com um conjunto comum de objetivos e/ou uma linha estratégica comuns.
- Caraterísticas da organização FA: Onde a organização é subdividida em duas grandes áreas, entidades organizacionais e posições organizacionais.
- *Ontology:* Que consiste no conjunto de conhecimentos que resolve qualquer problema de descrição de um domínio.
- *Security Awareness:* Mais específico que o *Organizational Self-Awareness,* a *Security Awareness* consiste no conhecimento e na consciência que os colaboradores de uma organização devem possuir sobre a importância de proteger a informação e os cuidados a ter com o manuseamento da mesma.

- Domínio: Uma esfera de ação dentro de uma empresa.
- Informação: Conjunto de dados, ordenados, processados e trabalhados de modo a serem compreendidos e inteligíveis.
- Segurança da informação: Necessidade básica de qualquer organização devido ao elevado valor da informação atualmente. A segurança da informação pressupõe a confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio.
- Fator social: Os recursos humanos assumem um papel de fragilidade na cadeia de segurança da informação.
- Gestão da informação: Sucintamente a gestão da informação envolve não só a componente tecnológica como também as pessoas e os processos.
- *Business Motivation Model:* Consiste num modelo que ajuda no desenvolvimento, comunicação e gestão dos planos de negócio. Dado a sua abrangência e universalidade foi uma das principais fontes para a construção do modelo de alinhamento.
- Plano: Este conceito elaborado através das definições provenientes do dicionário e das definições matemáticas ajudou à definição de plano organizacional.
- Estrutura organizacional: Conjunto das teorias sobre níveis organizacionais, de Chiavenato (2004), Thompson (2003) e Mintzberg (2003). Úteis para a construção da definição de plano organizacional.
- Estrutura organizacional da FA: A estrutura da FA está dividida em três níveis: estratégico, operacional e tático.
- Segurança computacional: A segurança computacional, um conceito central neste trabalho, define-se como a proteção conferida a um sistema de informação, a fim de atingir os objetivos aplicáveis à preservação da integridade, disponibilidade e confidencialidade.
- Estrutura da informação da FA: Resume a forma como está disposta a estrutura da informação na FA e como esta é gerida através do seu grupo coordenador da gestão da informação.

Feita a revisão literária, foi o momento de desenvolver o modelo que seria a resposta ao problema desta investigação. Para isso foram seguidos os seguintes passos:

- Definição de «planos organizacionais» tendo em conta a revisão literária feita. Ao definir os planos com os seus atributos possibilitou que posteriormente fossem escolhidos quais seriam os fatores de alinhamento.
- Construção do modelo de alinhamento utilizando alguns atributos dos planos organizacionais, juntamente com as ontologias e o *Business Motivation Model* revistos na revisão literária. Foram encontrados fatores de alinhamento e regras de alinhamento serão aplicáveis a qualquer empresa ou domínio.
- Validação do modelo de alinhamento foi efetuada através da instanciação do modelo no domínio da segurança computacional da FA. Assim foi possível demonstrar a aplicabilidade do modelo identificando, ainda, as regras que já são cumpridas ou que estão em falta, bem como algumas propostas para os fatores de alinhamento em falta.

Para finalizar a investigação é necessário rever as questões e hipóteses formuladas com o fim de concluir se serão validadas ou não. Para isso serão utilizadas tabelas de forma a ser mais intuitivo.

Tabela 5 - Pergunta de partida (fonte: Autor)

Pergunta de partida	**Até que ponto é possível identificar um modelo na FA que permita o alinhamento de processos nos diferentes planos organizacionais?**
Resposta	Não existe nenhum modelo de alinhamento na FA. No domínio da segurança computacional existem algumas diretivas escritas que o regulam em termos de segurança mas esquecem a parte do alinhamento que também é essencial para a própria segurança da informação.

Tabela 6 - Questão derivada 1 (fonte: Autor)

Questão 1	**Existe na Força Aérea um modelo holístico de alinhamento sobre a segurança computacional?**
Hipótese 1	Não existe um modelo holístico, apenas alguma doutrina em determinadas áreas de maior interesse que pode ser utilizada para construir um modelo mais abrangente.
Validação	Não existe qualquer modelo na FA neste domínio. Muita da doutrina existente foi utilizada para fazer a validação do modelo proposto nesta dissertação, portanto é possível considerar válida esta hipótese. Apesar da inexistência de um modelo encontra-se, em determinadas áreas, doutrinas a regular e definir os processos.

Tabela 7 – Questão derivada 2 (Fonte: Autor)

Questão 2	**O *Business Motivation Model* pode ser um modelo que permite modelar qualquer organização ou parte dela, promovendo o alinhamento entre os vários planos organizacionais?**
Hipótese 2.1	É possível utilizar o BMM para modelar corretamente qualquer organização, limitando assim a existência de falhas não previstas.
	O BMM é um modelo de desenvolvimento, comunicação e gestão dos planos de negócio, no entanto esgota-se aqui e é incapaz de servir de modelo de alinhamento entre planos organizacionais que era o objetivo desta dissertação. Portanto a hipótese não é válida apesar de o BMM ter sido uma ferramenta essencial na construção do modelo de alinhamento.
Hipótese 2.2	Devido à especificidade de determinados modelos de negócio o BMM não pode ser aplicado universalmente.
	O BMM pode ser aplicado universalmente, no entanto não faz sentido utilizá-lo como modelo de alinhamento de um domínio ou empresa pois não é para esse fim que foi desenhado. A validação desta dissertação demonstrou que o modelo apresentado pode ser aplicado numa área tão complexa como a da segurança computacional, logo poderá ser aplicado em qualquer outra área e o modelo é baseado em grande parte no BMM.

4.2 Recomendações

Terminada a investigação e consciente que muito mais haveria a fazer, o autor deixa algumas sugestões e recomendações:

- Testar alargadamente o conceito de planos organizacionais, quer na FA quer em outras empresas, para garantir que é um conceito universal e que pode ser adotado pela comunidade científica para futuras investigações;
- Aplicação do modelo de alinhamento a outros domínios e a outras organizações. Apesar da validação ter confirmado a sua aplicabilidade num caso, para obter um modelo robusto e coerente é necessário aplicá-lo e testá-lo mais vezes;
- Como recomendação para trabalho futuro, a construção ou compilação das regras de alinhamento em falta para a segurança computacional pode ser um grande contributo para a organização;
- A aplicação do modelo proposto à FA no domínio da segurança computacional. Depois de todo o trabalho aqui desenvolvido, com relativa facilidade se

operacionaliza o modelo na prática, proporcionando assim melhorias e obtendo-se uma maior qualidade no alinhamento da organização ao nível da segurança computacional;

- O autor recomenda também a difusão deste trabalho, de modo a aumentar a *security awareness* dentro da organização, consciencializando militares e civis que pertencem à FA.

5 Referências Bibliográficas

(4 de Abril de 2015). Obtido de Rfc-base.org: http://www.rfc-base.org/txt/rfc-2828.txt

(4 de Abril de 2015). Obtido de Iso.org: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

ALBERTS, D., & HAYES, R. (2003). *Power to the Edge – Command and Control in the Information Age;.* CCRP Publication Series.

BERNARDINO, T. S. (2012). A conceptual Framework to Support Information Security Risk Manegement. *Universidade do Minho Escola de Engenharia*.

BILHIM, J. A. (1988). *Cultura organizacional: Estudo do Instituto de Engenharia de Sistemas e Computadores.* Lisboa.

BURNS, P., NEUTENS, M., NEWMAN, D., & POWER, T. (2009). Building Value through Enterprise Architecture A Global Study. *booz&co.*

Business Rules Group. (25 de Novembro de 2015). Obtido de http://www.businessrulesgroup.org/bmm.shtml

CHIAVENATO, I. (2004). *Introdução à Teoria Geral da Administração.* Elsevier Editora Ltda.

COSTA, J. A., & MELO, A. S. (1999). *Dicionário da Lingua Portuguesa.* Porto Editora.

Decreto-Lei nº 187/2014. (2014). *LOFA.*

DIETZ, J., & HOOGERVORST, J. (2011). *Enterprise Engineering Manifesto: Advances in Enterprise Engineering I;.* LNBIP.

Diretiva Nº11/CEMFA. (2014). *Quadro Regulamentar das Publicações da C3 da Força Aérea.*

ENNIS, M. (2008). *Competency Models: A Review of the Literature and The Role of the Employment and Training Administration (ETA).* U.S. Department o Labor.

Fernandes, Benjamim; Páscoa, Carlos; Tribolet, José (2011): Two Level (strategic and operational) Objective Definition, Extended Abstract and Poster on Minutes of the CENTERIS 2011 Conference on ENTERprise and Information Systems, Viana do Castelo, Portugal, October 2011.

FONTE, C. (8 de Março de 2016). *Representação diédrica de ponto, tectas e planos.* Obtido de http://www.mat.uc.pt/~cfonte/docencia/Geometria%20_Descritiva/2_Representa%C3%A7%C3%A3o%20ponto%20recta%20plano.pdf

Força Aérea. (s.d.). Plano Diretor dos Sistemas de Informação.

Força Aérea Portuguesa. (2015). *Plano Anual de Atividades 2015.*

Força Aérea RFA 390-3. (2008). *Política de segurança da informação e dos sistemas de informação ecomunicações na Força Aérea.*

Força Aérea RFA 390-6. (2011). *Política de Ciberdefesa da Força Aérea.*

Força Aérea RFA 391-1 . (2011). *Política de Gestão da Informação da Força Aérea.*

GAMA, N., SILVA, M. M., CAETANO, A., & TRIBOLET, J. (2006). Integrar a Arquitectura Organizacional na Arquitectura Empresarial.

Group, O. M. (02 de Dezembro de 2014). *Business Process Model and Notation*. Obtido de Object Management Group: http://www.bpmn.org/

GUEDES, P. C. (2013). *Construção de um Cockpit Organizacional para a Força Aérea.* Sintra.

HOOGERVORST, J. (2009). *On the Realization of Strategic Success: A Paradigm Shift Needed: Enterprise Governance and Enterprise Engineering as essential concepts.* Springer Science & Business Media.

HOOGERVORST, J. (2011). *A framework for enterprise engineering.* International Journal of Internet and Enterprise Management.

JESTON, J., & NELIS, J. (2014). *Business process management.* Routledge.

LANKHORST, M. (2005). *Enterprise Architecture at Work: Modeling, Comunication and Analysis.* New York: Springer Berlin Heidelberg.

LILES, D., JOHNSON, M., & MEADE, L. (1995). *Enterprise engineering: a discipline?*

MASLOW, A. H. (1943). *A Theory of Human Motivation.*

MCLEOD, G. (2011). *The Difference between Process Architecture and Process Modeling/design (and why you should care).*

Ministério da Defesa Nacional. (2013). *Defesa 2020.*

MINTZBERG, H. (1995). *Criando Organizações Eficazes: Estrutura em Cinco Configurações.* São Paulo: Editora Atlas.

MONTEIRO, M. B. (2014). *As Funções numa Unidade Aérea.* Sintra.

NIST. (1995). *The NIST Computer Security Handbook.*

Páscoa, C.; Pinto, S.; Tribolet, J. (2011): Ontology construction: Portuguese Air Force Headquarters Domain, Springer Lecture Notes in Business Information Processing (LNPIB) Series Volume 89, 2011, pp 83-109, Practice-driven Research on Enterprise Transformation (PRET) Third Working Conference, PRET 2011, Luxembourg-Kirchberg, Luxembourg, September 6, 2011. Proceedings, doi: 10.1007/978-3-642-23388-3_4.

PEISL, R. (02 de Dezembro de 2014). *The Process Architect: The Smart Role in Business Process Management.* Obtido de IBM Redbooks: http://www.redbooks.ibm.com/redpapers/pdfs/redp4567.pdf

PEREIRA, C., SOUSA, & Pedro. (2005). *Enterprise Architecture: Business and IT Alignment.*

QUIVY, R., & CAMPENHOUDT, L. V. (1998). *Manual de Investigação em Ciências Sociais.* Gradiva.

Rebelo, H., Rocha, R., & Martins, V. (3 de Abril de 2015). *ISR - Intelligence, Surveillence and Reconnaissance.* Obtido de http://www.emfa.pt/www/conteudos/galeria/comunicados/2015/presskit-isr-fap_2164.pdf

RFA 390-3. (2008).

Security Awareness Program Special Interest Group PCI Security Standards Council. (29 de Fevereiro de 2014). *Information Supplement: Best Practices for Implementing a Security Awareness Program.* Obtido de pcisecuritystandards: https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

SILVA, P. T., CARVALHO, H., & TORRES, C. B. (2003). *Segurança dos Sistemas de Informação.* V. N. Famalicão: Centro Atlantico.

Só Matemática. (08 de Março de 2016). Obtido de Geometria Espacial: http://www.somatematica.com.br/emedio/espacial/espacial3.php

STAIR, R. M., & REYNOLDS, G. W. (2006). *Princípios de Sistemas de Informação.* Thomson.

STALLINGS, W., & Brown, L. (2012). Computer security. Boston: MA: Pearson Education.

SunTzu. (s.d.). *A Arte da Guerra.*

TELHA, A., & GORGULHO, J. (2014). *Apontamentos das aulas de EO I.* Academia da Força Aérea.

The Global State of Information Security Managing cyber risks in an interconnected world. (4 de Abril de 2015). Obtido de http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

The ISO 27000 Directory. (05 de Novembro de 2015). Obtido de http://www.27000.org/index.htm

The Open Group. (19 de Outubro de 2015). Obtido de http://pubs.opengroup.org/architecture/togaf8-doc/arch/

THOMPSON, J. D. (2003). *Organizations in action: Social Sciende Bases Of Administrative Theory.* New Brunswick, New Jersey: Transaction Publishers.

USCHOLD, M., & GRUNINGER, M. (June de 1996). ONTOLOGIES: Principles, Methods and Applications. *Knowledge Engineering Review*.

VICENTE, D., & TRIBOLET, J. (2007). *Towards Organizational Self-awareness: A Methodological Approach to Capture and Represent Individual and Inter-Personal Work Practices.* Instituto Superior Técnico, Lisboa.

What is data broker (information broker). (4 de Abril de 2015). Obtido de http://whatis.techtarget.com/definition/data-broker-information-broker

WHITE, S. (02 de Dezembro de 2004). *Introduction to BPMN.* IBM Corporation. Obtido de www.bptrends.com

ZACARIAS, M., MAGALHÃES, R., CAETANO, A., PINTO, S., & TRIBOLET, J. (2008). Towards organizational self-awareness: An initial architecture and ontology. Em *Ontologies for Business Interactions* (pp. 101-121).

Anexo A – Entrevistas

MELO, Pedro (23/02/2016), Diretor da Direção de Comunicação e Sistemas de Informação do EMGFA

VICÊNCIO, José Vicêncio (22/02/2016), Chefe da Direção de Comunicação e Sistemas de Informação da FA

FERREIRA, Rui (22/02/2016), Chefe da Divisão de Comunicações e Sistemas de Informação da FA

Entrevistado: Cor Rui Ferreira

Posição Organizacional: Chefe da Divisão de Comunicações e Sistemas de Informação

Dia da Entrevista: 22 de fevereiro de 2016

P1 - Considera existir uma visão generalista para a segurança computacional da força aérea?

Na Força Aérea, tem-se sempre em conta a manutenção de uma cultura de segurança computacional. Para o conseguir faz-se o acompanhamento da tecnologia e dos desenvolvimentos na área e tenta-se sempre implementar as regras de boas práticas. Tal é feito através da participação em Fóruns da área assim como a frequência de cursos e formação. Igualmente está em fase de elaboração e aprovação várias políticas e planos de formação nesta área, com vista à sensibilização da problemática entre os militares e civis da Força Aérea.

P2 - No seu entender, deveria existir uma estrutura mais centralizada para trabalhar o tema da segurança computacional? Ou a atribuição de áreas específicas a determinadas entidades é uma solução mais viável?

Atualmente, na Força Aérea, estes temas são tratados a nível do Estado Maior, em termos de doutrina e política, pela Divisão de Comunicações e Sistemas de Informação (DivCSI) e a nível técnico e de implementação, pela Direção de Comunicações e Sistemas de Informação do Comando da Logística. Dentro destas existem Repartições e Secções encarregues especificamente da segurança informática e de resposta a incidentes.

Julga-se que em termos organizacionais a estrutura, está adequadamente definida, prendendo-se as dificuldades com os quantitativos de elementos e do nível de formação que possuem.

Na organização existem também normas e regras, que devem ser observadas e aplicadas pelas diversas Unidades, Órgãos e Serviços da Força Aérea, de forma a manter a segurança transversalmente.

P3 - Fará sentido e trará algum valor acrescentado à FA englobar toda a doutrina sobre segurança da informação e dos sistemas de informação numa só? (Por exemplo, na segurança computacional como proposto nesta dissertação)

Por princípio não se deve dissociar a segurança da informação dos sistemas de informação.
De forma a conseguir-se um adequado nível de segurança, é necessário que a doutrina da segurança da informação aplicada tenha em conta as especificidades dos sistemas de informação. Deve ter em conta principalmente as limitações a nível de segurança para o desenvolvimento de regras e normas que visem reduzir os riscos.

P4 - Conhece alguma lista de conceitos existente na FA que uniformize a linguagem falada sobre a segurança de informação e de sistemas de informação?

Conforme decorre da missão que tem atribuída, a DivCSI tem a seu cargo o estabelecimento e elaboração de estudos e planos, na área de Comunicações e Sistemas de Informação. Um dos aspetos incluído na missão, é a segurança da informação armazenada, processada ou transmitida nos sistemas de comunicações e de informação, bem como noutros sistemas eletrónicos. Estes planos e estudos traduzem-se em vários Regulamentos e Planos em vigor na Força Aérea, que definem entre outros os conceitos usados.
Portugal, como membro integrante da NATO, participa na elaboração e implementação da doutrina emanada por essa organização. Também a nível da segurança computacional existem várias diretivas, *standards* e normativos em vigor. A Força Aérea, assim como os restantes Ramos das Forças Armadas, implementa essas regras e diretivas, até por questões de interoperabilidade com os restantes parceiros. Também aí existe a definição de vários conceitos.

P5 - A minha dissertação pretende aplicar o Business Motivation Model na área da segurança computacional na FA. Sabendo que o BMM disponibiliza um esquema para ajudar ao desenvolvimento, comunicação e gestão dos planos de negócio de uma forma organizada, considera que o trabalho desenvolvido até agora faz sentido no panorama da nossa organização? (Anexo 2)

O presente trabalho, ao proporcionar o auxílio ao desenvolvimento, comunicação e gestão dos planos de negócio, traduz-se numa mais valia.
A área da segurança computacional reveste-se duma importância vital em qualquer organização. Atualmente as organizações, e principalmente no caso dos militares, estão completamente dependentes de sistemas de informação. É essencial que em

relação à informação, seja garantida a sua: confidencialidade, disponibilidade integridade, autenticidade e não-repúdio.
Quando descurada a segurança da informação, em caso de disrupção, pode traduzir-se num total impedimento e bloqueio ao negócio e à missão a cumprir pela organização, pelo que é essencial haverem mecanismos que permitam efetuar o desenvolvimento e comunicação dos planos de negócios.

P6 - Para os conceitos não identificados, e como especialista nessa matéria, é capaz de definir algum deles no âmbito da FA?

Um dos conceitos a ter em conta devem ser os modelos de continuidade de negócios. Esta é uma das partes basilares e integrantes da segurança computacional, devendo ser claro e conhecido por todos os elementos da organização, principalmente os diretamente ligados à área.

Entrevistado: Major-General Pedro Melo

Posição Organizacional: DIRCSI

Dia da Entrevista: 23 de fevereiro de 2016

P1 - Considera existir uma visão generalista para a segurança computacional da força aérea?

Não conheço bem o ramo para poder ajudar nessa pergunta.

P2 - No seu entender, deveria existir uma estrutura mais centralizada para trabalhar o tema da segurança computacional? Ou a atribuição de áreas específicas a determinadas entidades é uma solução mais viável?

A estrutura que trata a informação classificada deve estar separada da informação não classificada, se esta divisão for bem cumprida não há o perigo de existirem pedaços de informação esquecida.

P3 - Fará sentido e trará algum valor acrescentado à FA englobar toda a doutrina sobre segurança da informação e dos sistemas de informação numa só? (Por exemplo, na segurança computacional como proposto nesta dissertação)

Não conhecendo bem o ramo posso dar a opinião relativamente ao EMGFA, julgo que não é necessária uma doutrina mais englobadora pois já existe um bom alinhamento no tratamento tanto da informação classificada como não classificada.

P4 - Conhece alguma lista de conceitos existente na FA que uniformize a linguagem falada sobre a segurança de informação e de sistemas de informação?

Na FA não conheço mas existem alguns documentos, nomeadamente o SegMil 1 e 2 que aborda essas definições, no entanto entes documentos já são bastante antigos e encontram-se um pouco desatualizados.

P5 - A minha dissertação pretende aplicar o Business Motivation Model na área da segurança computacional na FA. Sabendo que o BMM disponibiliza um esquema para ajudar ao desenvolvimento, comunicação e gestão dos planos de negócio de uma forma organizada, considera que o trabalho desenvolvido até agora faz sentido no panorama da nossa organização? (Anexo 2)

P6 - Para os conceitos não identificados, e como especialista nessa matéria, é capaz de definir algum deles no âmbito da FA?

A visão pode ser a garantia que toda a informação necessária ao comando e controlo é segura e tem de existir um equilíbrio entre a sua segurança e a operacionalidade.

A missão traduz-se nas definições de missão de toda a estrutura que trabalha para garantir a visão.

Entrevistado: Brigadeiro-General José Vicêncio

Posição Organizacional: Diretor DCSI

Dia da Entrevista: 22 de fevereiro de 2016

P1 - Considera existir uma visão generalista para a segurança computacional da força aérea?

É difícil quantificar mas temos uma visão generalista mas pouco, por esse motivo é que existem várias iniciativas para promover a *security awareness.*

P2 - No seu entender, deveria existir uma estrutura mais centralizada para trabalhar o tema da segurança computacional? Ou a atribuição de áreas específicas a determinadas entidades é uma solução mais viável?

A informação está bem estruturada, o subregisto trata da parte de segurança de informação classifica, depois temos a centralização na área da cibersegurança da nossa direção que se preocupa com a segurança e proteção dos nossos sistemas computacionais. O subcemfa é o diretor da informação que abrange estas duas áreas, através do grupo coordenador de gestão de informação que tem a tutela de toda a informação da FA.

P3 - Fará sentido e trará algum valor acrescentado à FA englobar toda a doutrina sobre segurança da informação e dos sistemas de informação numa só? (Por exemplo, na segurança computacional como proposto nesta dissertação)

Existem falhas na estrutura que engloba todas as publicações sobre o tema, nomeadamente no que diz respeito ao RFA 390-6 que devia estar incluído no edifício de publicações.

Logo devia haver uma política mais enquadradora e bem representada a todas as outras políticas de segurança de informação, o que não significa que não exista alinhamento, este pode ser promovido através do grupo coordenador de gestão de informação.

P4 - Conhece alguma lista de conceitos existente na FA que uniformize a linguagem falada sobre a segurança de informação e de sistemas de informação?

Os únicos documentos promulgados que falam sobre estes conceitos na FA são os RFA presentes no edifício de publicações, nomeadamente: RFA 391-1, 390-3, 390-6.