Universidade Católica Portuguesa
Faculdade de Engenharia

O Impacto das Crenças Individuais dos Profissionais na Cultura de Segurança da Informação nas Organizações

– Estudo no sector da Água / Saneamento em Portugal

Maria Helena Ferreira da Cruz e Silva

Dissertação para obtenção do Grau de Mestre em Segurança em Sistemas de Informação

Júri

Prof. Doutor Manuel José Martinho Barata Marques (Presidente)
Prof. Doutor Rui Jorge Correia Mendes Alves Pires
Prof. Doutor Tito Santos Silva (Orientador)

Setembro de 2014

Uma gota num oceano …

Ao meu falecido pai.

À minha mãe,

irmãos e amigos.

Resumo

Este trabalho realizado no âmbito da finalização do mestrado em Segurança em Sistemas de Informação pela Faculdade de Engenharia da Universidade Católica Portuguesa, debruça-se sobre a temática da cultura organizacional em segurança da informação, segundo um dos pilares que é considerado de enorme relevância nas organizações – "o factor humano", no sector empresarial das Águas e Saneamento em Portugal.

Deste modo, partindo das questões de apoio "Q1-Quais as crenças individuais dos profissionais na cultura da segurança da informação?" e "Q2 – Qual o impacto das crenças individuais na cultura de Segurança da Informação?", este estudo, de carácter exploratório e descritivo, tem como objectivos:

1. Investigar quais os Factores Motivadores (FM), Inibidores (FI), Críticos de Sucesso (FCS) e de Boas Práticas (FBP) que dão suporte à adopção/implementação de um Sistema de Gestão de Segurança da Informação (SGSI) nas organizações do sector de Águas e Saneamento em Portugal, tendo em conta a perspectiva do próprio (PP) e a perspectiva do próprio face à organização (PPO).
2. Comparar as duas perspectivas por meio do cálculo do nível médio de importância para cada elemento dos factores acima referidos.
3. Analisar os efeitos obtidos através do cruzamento do nível médio de importância dos elementos dos diferentes factores (FM, FI, FCS, FBP) com o mapeamento segundo a orientação do ISACA [1] que indica que «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*».

A necessidade evidente da utilização da "informação" como um recurso estratégico nas organizações em geral e deste sector, em particular, bem como a imprescindibilidade de abordar a "gestão eficaz e eficiente dos recursos hídricos" de uma forma holística, tendo por base a "gestão da segurança" através de uma abordagem de avaliação de risco, em que o recurso "informação" deverá ser considerado, em paralelo com o recurso "água", como factor de alinhamento à estratégia da organização, de forma a contribuir para a resolução de problemas, criação de valor e garantia da continuidade dos serviços em situação de contingência, coloca o "factor humano" indubitavelmente como um ponto-chave, pelo que "criar uma cultura de segurança" nas organizações torna-se num desafio para as mesmas, devendo ser um foco da

atenção da governação corporativa, bem como um objectivo prioritário da governação da segurança da informação nas organizações.

Assim, no presente estudo identificou-se primeiramente os Principais Conceitos-Chave que possibilitaram a realização da revisão bibliográfica sobre o Estado da Arte desta problemática, onde se procurou encontrar respostas metodológicas para a abordagem da avaliação da cultura organizacional em segurança da informação nas organizações, mas também descobrir contributos que auxiliassem na execução deste trabalho. Seguidamente, descreve-se o trabalho realizado expondo o racional, detalhando os objectivos e apresentando a abordagem efectuada, tendo por base a elaboração e divulgação de um questionário que serviu de apoio ao «*Diagnóstico da Cultura em Segurança da Informação – Sector: Água e Saneamento em Portugal*», cujo público-alvo foram os gestores de topo, de nível intermédio, das TI, consultores das TI, gestores/funcionários de segurança e funcionários das organizações neste sector, tais como entidades gestoras, entidades reguladoras, etc. … Depois, revela-se o detalhe do tratamento e análise dos dados obtidos, designadamente a caracterização da amostra, abordando os quatro sectores (FM, FI, FCS e FBP) segundo a PP e a PPO, assim como a análise comparativa entre as duas perspectivas e, ainda, a análise resultante do mapeamento dos elementos dos factores segundo orientação do ISACA [2], mostrando-se os respectivos resultados. Finalmente, tecem-se as conclusões e apresentam-se notas finais.

Palavras chave:

Informação, Segurança da Informação, Governação Corporativa, Governação das TI, Governação da Segurança da Informação, Cultura de Segurança da Informação.

Abstract

This work performed under the finalization of the MA in Security in Information Systems from the Faculty of Engineering, Catholic University, focuses on the theme of organizational culture in information security, according to one of the pillar which is considered extremely relevant in organizations – " human factor" in the business sector of Water and Sanitation in Portugal .

Thus, leaving the issues of support "Q1 - What are the beliefs of individual professionals in the culture of information security?" and "Q2 - What is the impact of individual beliefs in the culture of Information Security?" This study exploratory in nature and descriptive aims to:

1. Investigate what the Motivating Factors (FM) Inhibitors (FI), Critical Success (FCS) and Good Practice (FBP) that support the adoption / implementation of a Management System of Information Security (ISMS) in the organizations Water and Sanitation sector in Portugal, taking into account the perspective of their own (PP) and face the prospect own organization (PPO) .
2. Compare the two approaches by calculating the average level of importance for each element of the above factors.
3. To analyze the effects obtained by crossing the middle level of importance of the various factors elements (FM, FI, FCS, FBP) with the mapping according to the orientation of ISACA [3] indicating that «*from a governance perspective there are six major outcomes that security programme should work to achieve, namely: 1) strategic alignment; 2) risk management; 3) value deliver; 4) resource management; 5) performance management and 6) assurance process integration*».

The obvious need for the use of "information" as a strategic resource in organizations in general and this sector, in particular, as well as the indispensability of addressing the "effective and efficient management of water resources" in a holistic way, based on the "safety management" through a risk assessment approach, in which the application "information" should be considered in parallel with the resource "water" as alignment with the organization's strategy factor, in order to contribute to the resolution of problems, creating value and ensuring the continuity of services in a contingency situation, puts the "human factor" as undoubtedly a key point at which "create a safety culture" in organizations becomes a challenge for them, should be a focus of attention of corporate governance, as well as a priority objective of the governance of information security in organizations.

Thus, in this study we identified the first Major Key Concepts that made possible the realization of the literature review on the state of the art of this problem, where we tried to find answers to the methodological approach to the assessment of organizational culture in information security in organizations, but also find contributions that aided in the execution of this work. Next, we describe the work done by exposing the rational, detailing the objectives and presenting the approach taken, based on the preparation and dissemination of a questionnaire which was used to support the "*Diagnosis of Culture in Information Security - Sector: Water and Sanitation in Portugal*" audience, which were top managers, middle-level, IT, IT consultants, managers / security officials and employees of organizations in this sector, such as operators, regulators, etc. … Then it turns out the detail of the processing and analysis of data, including sample characterization, addressing the four sectors (FM, FI, FCS, FBP) according to PP and PPO, as well as comparative analysis between the two perspectives and furthermore, the analysis of the resulting mapping of the elements of the second orientation factors of ISACA [4], showing off the results. Finally, weave the findings are presented and endnotes.

Key words

Information, Information Security, Corporative Governance, IT Governance, Information Security Governance, Information Security Culture.

Agradecimentos

Finalizar este mestrado foi um objectivo árduo de concretizar. Assim, expresso os meus sinceros agradecimentos aos que directa ou indirectamente contribuíram para o cumprimento de tal desiderato, nomeadamente:

Aos Serviços Municipalizados de Água e Saneamento de Sintra, referência no sector das Águas e Saneamento em Portugal, nas pessoas do Ex-Presidente Eng.º José Manuel Baptista Alves e da Directora Delegada Eng.ª Maria Guadalupe Sereno Gonçalves pelo incentivo e apoio demonstrado.

A todas as instituições e respondentes do questionário '*on-line*', pedra angular deste trabalho, pela participação célere e gratuita.

Aos meus colegas de trabalho e das pós-graduações integrantes deste mestrado, pela disponibilidade e pelo ambiente agradável de trabalho proporcionado.

Aos meus familiares e amigos pelo incentivo e paciência demonstrada.

Aos meus professores, especialmente o professor Tito Santos Silva (orientador) e o Eng.º Bruno Horta Soares (co-orientador), pelo incentivo, pelos contributos e valiosas apreciações, comentários e conhecimentos, ajudando-me a reflectir e a realizar este trabalho.

Muito obrigada a todos pelo contributo prestado, o qual permitiu o meu enriquecimento técnico e humano.

Índice

Índice de Figuras

Índice de Tabelas

Índice de GráFicos

SIGLAS Utilizadas

AMEGA – Associação de Municípios de Estudos e Gestão de Água

APDA – Associação Portuguesa de Distribuição e Drenagem de Águas

ASIS – American Society for Information Science

BMIS – The Business Model for Information Security

COBIT – Control Objectives for Information and Related Technology

CTI – Consultor das TI

DI – Dynamic Interconexion (interconexão dinâmica – usada pelo BMIS)

ENISA – European Network and Information Security Agency

ERSAR – Entidade Reguladora de Serviços de Águas e Resíduos

FBP – Factores de Boas Práticas

FCS – Factores Críticos de Sucesso

FI – Factores Inibidores

FM – Factores Motivadores

GNS – Gabinete Nacional de Segurança

GTI – Gestor das Tecnologias de Informação

IEEE - Institute of Electrical and Electronics Engineers, Inc.

ISACA - Information Systems Audit and Control Association

ISO/IEC – International Organization for Standardization / International Electrocnical Commission

ITGI – IT Governance Institute

ITIL - Information Technology Infrastructure Library

I&D – Inovação e Desenvolvimento

NIST – National Institute of Standards and Tecnology

NMI – Nível Médio de Importância

OCDE – Organisation for Economic Cooperation and Development

PC – Computador Pessoal

PP – Perspectiva do Próprio (respondente)

PPA – Parceria Portuguesa para a Água

PPO – Perspectiva do Próprio face à Organização (respondente)

PSA – Plano de Segurança da Água

SEGNAC – Segurança Nacional

SGSI – Sistema de Gestão da Segurança da Informação

SI – Sistemas de Informação

SIG – Sistema de Informação Geográfica

SCADA – Supervisory Control and Data Acquisition

SMAS – Serviços Municipalizados de Água e Saneamento

TI – Tecnologias de Informação

UE – União Europeia

1. INTRODUÇÃO

Actualmente, a sobrevivência e o crescimento progressivo das organizações dependem do seu "engenho" em se relacionarem com o meio que as rodeiam, bem como da forma como vão actuando e/ou respondendo às mudanças provocadas pela conjuntura que as rodeiam: requisitos, *standards*, normas, *guidelines*, tecnologia, medias, accionistas, clientes, fornecedores …

Por isso, adequar e melhorar o desempenho organizacional, satisfazer os seus clientes, reduzir e/ou minimizar os riscos e garantir a continuidade dos serviços prestados são "fins" que tornam as organizações cada vez mais "tecno dependentes" e, por isso, mormente subordinadas à existência dos Sistemas de Informação (SI) que, por sua vez, apresentam níveis de complexidade crescente. Desta forma, a palavra-chave – Informação, torna-se num recurso crítico e estratégico, uma vez que a recolha de dados e o seu tratamento influenciará – de forma vital – a tomada de decisão nas organizações.

Neste contexto, a utilização racional do recurso Informação torna-se num domínio estratégico dentro das organizações e obrigam à necessidade de uma arquitectura integrada dos sistemas de informação com um forte alinhamento aos objectivos do "negócio".

Por outro lado, a evolução tecnológica decorre a um ritmo "alucinante" pelo que se consolida a necessidade de "rever" periodicamente todo o SI das organizações, de forma a assegurar a sua eficácia e eficiência. Contudo, a mediatização dos incidentes de segurança alerta para os "riscos", consequentemente para a necessidade de implementar mais "controlos".

Assim, neste ambiente de globalização em que cada vez mais as organizações colaboram e partilham recursos informacionais, é certo que se expõem a mais vulnerabilidades existentes dentro e fora da organização, pelo que a segurança da informação deve ir para além da perspectiva tecnológica.

Segundo, Oliveira, Wilson [5] «*A segurança da informação não é uma questão técnica, mas uma questão estratégica e humana. Não adianta adquirir uma série de dispositivos de hardware e software sem formar e consciencializar o nível administrativo da empresa e todos os seus funcionários*».

Okere, Irene et al. [6] também referem que «*Os seres humanos são em grande parte o centro da protecção dos recursos informacionais numa organização através dos seus comportamentos na interacção com a informação e sistemas de informação*».

Do mesmo modo, Malcolmson, Jo [7] refere que «*Recentes estudos conduzidos por QinetiQ têm demonstrado que o sistema de segurança, embora possa utilizar tecnologia de rastreio*

sofisticada, pode ser, significativamente, influenciado pelas atitudes e comportamentos do pessoal e pelas políticas de segurança que lhe dão suporte».

Esta problemática da segurança da informação está cada vez mais na ordem do dia das organizações, das entidades reguladoras, dos governos e da sociedade científica e civil em geral, pelo que se considerou interessante dissertar sobre o tema, abordando a questão pela perspectiva do "factor humano":

- Que crenças individuais têm os profissionais e como é que isso se reflecte na cultura organizacional de segurança da informação nas organizações?
- Quais os desafios na definição e na implementação de uma cultura organizacional, em particular no domínio da segurança da informação - Que Factores Motivadores, Inibidores, Críticos de Sucesso e de Boas Práticas constituem ou não *drivers* na implementação de um sistema de gestão da segurança da informação?

e considerando um sector de actividade empresarial em Portugal.

O sector das Águas e Saneamento em Portugal foi seleccionado por:

1. Representar um quadrante significativo de organizações públicas e privadas que têm como missão o fornecimento de produto e serviços críticos de segurança para a sociedade portuguesa.
2. Envolver elevados requisitos de segurança, nomeadamente nos processos de abastecimento e distribuição da água, destacando-se a necessidade de todas as partes envolvidas no sector estarem cada vez mais atentas aos riscos relacionados. Segundo Grey, David et al. [8] «*A escala do desafio sempre presente da sociedade de alcançar a sustentabilidade da segurança da água é determinada por muitos factores, entre os quais se destacam … o ambiente sócio-económico – a estrutura da economia e o comportamento dos seus actores – que reflectem legados naturais e culturais…*».
3. Ser um sector cada vez mais orientado à inovação e às abordagens alinhadas às boas práticas de referenciais internacionais, fazendo sentido este tipo de estudo.

Este trabalho realizado no âmbito da finalização do mestrado em Segurança em Sistemas de Informação pela Faculdade de Engenharia da Universidade Católica Portuguesa, debruça-se sobre a temática da cultura organizacional em segurança da informação, segundo um dos pilar que é considerado de enorme relevância nas organizações – "o factor humano", no sector empresarial das Águas e Saneamento em Portugal.

Deste modo, partindo das questões de apoio "Q1-Quais as crenças individuais dos profissionais na cultura da segurança da informação?" e "Q2 – Qual o impacto das crenças individuais na cultura de Segurança da Informação?", este estudo, de carácter exploratório e descritivo, tem como objectivos:

1. Investigar quais os Factores Motivadores (FM), Inibidores (FI), Críticos de Sucesso (FCS) e de Boas Práticas (FBP) que dão suporte à adopção/implementação de um Sistema de Gestão de Segurança da Informação (SGSI) nas organizações do sector de Águas e Saneamento em Portugal, tendo em conta a perspectiva do próprio (PP) e a perspectiva do próprio face à organização (PPO).
2. Comparar as duas perspectivas por meio do cálculo do nível médio de importância para cada elemento dos factores acima referidos.
3. Analisar os efeitos obtidos através do cruzamento do nível médio de importância dos elementos dos diferentes factores (FM, FI, FCS, FBP) com o mapeamento segundo a orientação do ISACA [9] que indica que «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*».

Para cumprimento de tal desiderato e, conforme se apresenta na figura (Figura 1.1) seguinte, primeiramente identificaram-se os Principais Conceitos-Chave (Capítulo 2) que possibilitaram a realização da revisão bibliográfica sobre o Estado da Arte (Capítulo 3) desta problemática, onde se procurou encontrar respostas metodológicas para a abordagem da avaliação da cultura organizacional em segurança da informação nas organizações, mas também descobrir contributos que auxiliassem na execução deste trabalho. Seguidamente, descreve-se o trabalho realizado (Capítulo 4), expondo o racional, detalhando os objectivos e apresentando a abordagem efectuada, tendo por base a elaboração e divulgação de um questionário que serviu de apoio ao "*Diagnóstico da Cultura em Segurança da Informação – Sector: Água e Saneamento em Portugal*", cujo público-alvo foram os gestores de topo, de nível intermédio, das TI, consultores das TI, gestores/funcionários de segurança e funcionários das organizações neste sector, tais como entidades gestoras, entidades reguladoras, etc.. Depois, revela-se o detalhe do tratamento e análise dos dados obtidos (Capítulo 5), designadamente a caracterização da amostra, abordando os quatro sectores (FM, FI, FCS e FBP) segundo a PP e a PPO, assim como a análise comparativa entre as duas perspectivas e, ainda, a análise resultante do mapeamento dos elementos dos factores segundo orientação do ISACA [10], mostrando-se os

respectivos resultados. Finalmente, tecem-se as conclusões (Capítulo 6) e apresentam-se as notas finais (Capítulo 7).

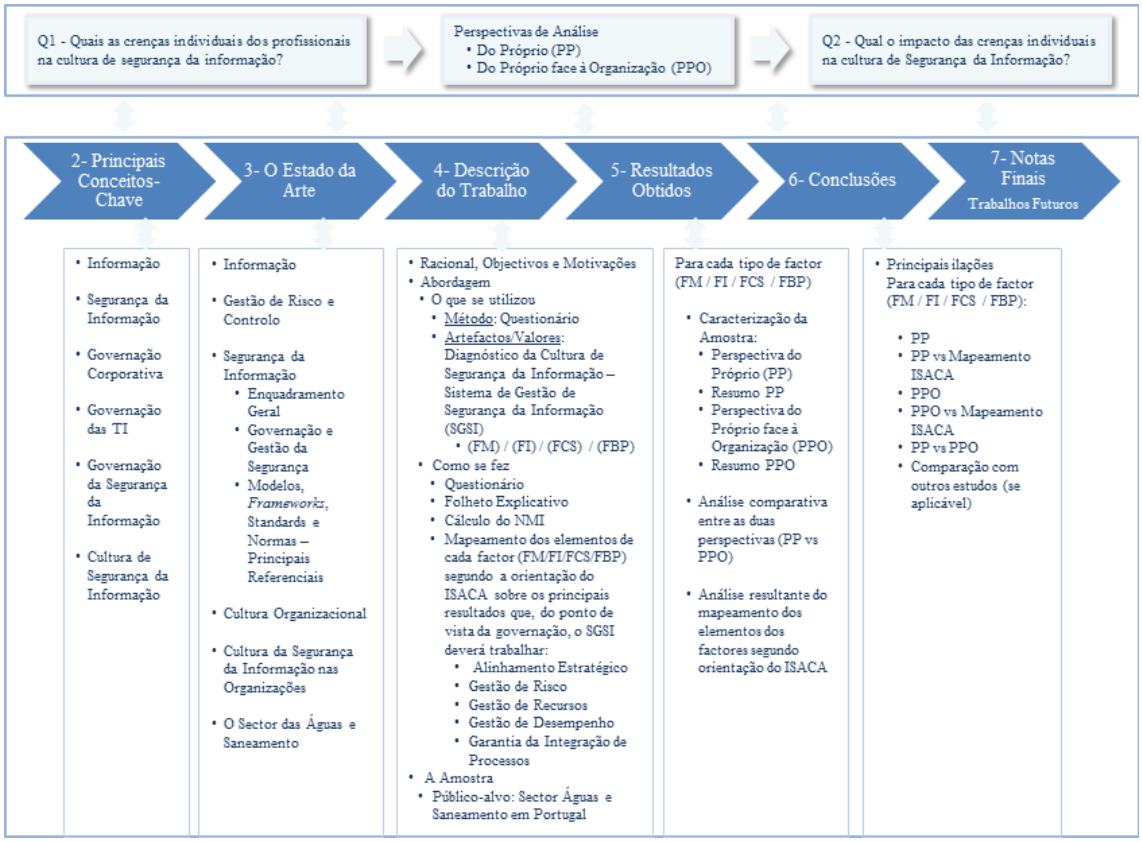


Figura 1.1- Modelo do Trabalho Realizado

2. OS PRINCIPAIS CONCEITOS - CHAVE

Neste capítulo, introduz-se os principais conceitos que estão na base do desenvolvimento deste trabalho, balizando as diferentes formas e variações que possam estar associadas aos mesmos.

- Principais palavras-chave: Informação, Segurança da Informação, Governação Corporativa, Governação das TI, Governação da Segurança da Informação e Cultura de Segurança da Informação.

2.1 - Informação

Segundo Serra, J. Paulo [11] a "Informação" é «*o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe*».

2.2 - Segurança da Informação

A ISO27000 [12] define "Segurança da Informação" como a «*preservação da confidencialidade, integridade e a disponibilidade da informação, podendo incluir outras propriedades como a autenticidade, a responsabilidade, o não-repúdio e a confiança*».

Também Oliveira, Wilson [13] explica-a como o «*processo de protecção dos sistemas de informação e que tem como finalidade garantir a disponibilidade, o sigilo, a integridade, a autenticidade, o controlo de acesso e o não-repúdio das informações*».

2.3 - Governação Corporativa

Recorrendo ao dicionário Priberam da Língua Portuguesa verifica-se que o mesmo indica como sinónimo de Governação: «*exercer governo, dirigir os seus negócios*».

Gonçalves, Hélder [14] aponta a definição de "Governação Corporativa" indicada pela OCDE como «*o sistema pelo qual as organizações são dirigidas e controlada*». Contudo, num artigo sobre a governação corporativa e o papel das tecnologias de informação Hamaker, Stacey et al. [15] e *Sandrino-Arndt* [16] citam a definição sobre "Governação Corporativa", indicada pelo IT Governance Institute [17] como «*o conjunto de responsabilidades e práticas exercidas pela gestão de topo e gestores executivos com a meta de fornecer directivas estratégicas, assegurando que os objectivos são atingidos, verificando que os riscos são propriamente geridos e que os recursos empresariais / organizacionais são usados com responsabilidade*».

2.4 - Governação das TI

O IT Governance Institute [18], citado por Grembergen, Wim Van et al. [19] descrevem "Governação das TI" como sendo «*uma actividade da responsabilidade da Gestão de Topo e da Gestão Executiva e parte integrante da governação corporativa, consistindo na liderança e estruturas e processos organizacionais capazes de garantir que a organização das TI suportam e estendem-se à estratégia e objectivos da organização*».

Por outro lado, os mesmos autores citam Grembergen, Van (2002) que define "Governação das TI" como sendo «*a capacidade organizacional exercitada pela gestão de topo, gestão executiva e gestão das TI para controlar a formulação e a implementação de estratégias de tecnologias de informação de forma a assegurar a fusão entre o 'negócio' e as 'tecnologias de informação'*». Assim, defendem ainda que «*as tecnologias de informação tornaram-se, não só num factor de sucesso para a sobrevivência e prosperidade organizacional, mas também numa oportunidade para 'fazer a diferença' e alcançar vantagens competitivas*». Deste modo, é de realçar que ambas as definições mostram a importância da interligação entre os objectivos de 'negócio' e as tecnologias de informação, revelando-se, segundo citação dos mesmos autores, o que o IT Governance Institute [20] defendeu: «*a governação corporativa dirige e configura a governação das TI e vice-versa, bem como as actividades organizacionais requerem informação das actividades das TI e vice-versa*», constatando-se que as tecnologias de informação permitem, assim, à organização tirar o máximo partido da 'sua informação' tornando-se, desta forma, num "*driver*" da governação corporativa.

2.5 - Governação da Segurança da Informação

Sendo a informação um activo estratégico nas organizações, a sua protecção tornou-se numa prioridade do negócio, uma vez que os negócios daquelas encontram-se numa convergência digital e crescem numa complexa rede onde surgem continuamente novos riscos.

Citando a ISO27000 [21] a governação da segurança da informação «*envolve a supervisão e a tomada de decisão necessárias para alcançar os objectivos organizacionais através da protecção dos seus activos de informação. A gestão da segurança da informação é expressa através da formulação e utilização de políticas de segurança, standards, procedimentos e orientações, que são aplicadas a toda a organização por todos os indivíduos pertencentes à mesma*».

2.6 - Cultura de Segurança da Informação

A exposição à emergência contínua de novos riscos, quer de origem interna (funcionários) ou externa, a que as organizações estão cada vez mais sujeitas, coloca em causa a segurança da informação, bem como a continuidade do negócio.

Assim, segundo Helokunnas, Tuija et al. [22], a cultura de segurança da informação é vista «*como um sistema composto pela interacção de uma estrutura e componentes de conteúdo. Estrutura contém uniformização, certificação e medição de segurança da informação. Conteúdo inclui atitude das pessoas, motivação, conhecimento e modelos mentais acerca da segurança da informação*».

3. O ESTADO DA ARTE

Neste capítulo identificam-se, através de revisão literária, teorias, terminologias, conceitos políticas e metodologias em torno das temáticas da "Segurança da Informação", tendo em conta o enfoque do "factor humano" nas organizações, nomeadamente da "Cultura da Segurança da Informação nas Organizações".

Assim, partindo do conceito "Informação" e resumidamente da sua natureza como ciência, abordam-se desígnios com ela relacionada, como sejam a Gestão de Risco e Controlo – considerada como a pedra angular da problemática da Segurança da Informação. Neste ponto, faz-se um enquadramento geral, mostram-se as ideias de governação e gestão da segurança como principais alicerces para a segurança da informação e apresentam-se os principais referenciais – modelos, *frameworks*, *standards* e normas que permitem identificar onde estamos e definir para onde devemos caminhar.

Todavia, e uma vez que este trabalho tem como foco o impacto do "factor humano" na Segurança da Informação, expõe-se, num sentido mais geral, os princípios de "cultura", "cultura organizacional" e "cultura da segurança da informação nas organizações".

Por fim, não menos importante e porque o estudo do presente trabalho desenvolve-se no sector das Águas e Saneamento em Portugal, enquadra-se a importância do mesmo na utilização do recurso "informação", bem como da necessidade da priorização da segurança da informação como factor de alinhamento estratégico de suporte à alavancagem de realização do objectivo estratégico: Água Segura.

3.1- Informação

Em conformidade com Le Coadic, Yves-Francois [23] «*A informação é um conhecimento inscrito (gravado) sob a forma escrita (impressa ou numérica), oral ou audiovisual*». Ainda, de acordo com o mesmo autor «*Um conhecimento (um saber) é o resultado do ato de conhecer, ato pelo qual o espírito apreende um objecto. Conhecer é ser capaz de formar a ideia de alguma coisa; é ter presente no espírito. Isso pode ir da simples identificação (conhecimento comum) à compreensão exata e completa dos objectos (conhecimento científico). O saber designa um conjunto articulado e organizado de conhecimentos a partir do qual uma ciência – um sistema de relações formais e experimentais – poderá originar-se*».

Continuando, ainda, a citar o mesmo autor «*A CIÊNCIA da informação é ciência, produção consciente da espécie humana com origens bem precisas, um objecto e conteúdo bem definidos e especialistas facilmente identificáveis. Suas origens são recentes:1968, data de nascimento da*

primeira grande sociedade científica nos Estados Unidos, a American Society for Information Science (ASIS) … o seu objecto é uma matéria, a informação, que permeia o espaço das profissões. Trata-se de recurso vital do qual ainda não se mediu suficientemente a extensão dos usos e não-usos, por falta de atenção com seus usuários. Seu conteúdo, marcado pelo selo da interdisciplinaridade, é uma sábia dosagem de ciências matemáticas e físicas, bem como ciências sociais e humanas. Técnicas audaciosas e os imperativos de sua tecnologia a impulsionam irresistivelmente e a fazem passar do universo do papel para o universo electrónico. Nesse universo, informações de toda a natureza podem ser armazenadas e transmitidas sob forma digital. Após tê-las convertido, representamos qualquer texto, som ou imagem na forma de bit e de bytes. Uma vez digitalizadas, essas informações podem ser veiculadas por diferentes meios, nas redes de transmissão, por difusão hertziana, em (micro, mini, super) computadores, e até mesmo em livros electrónicos».

Também, Barreto, Aldo de Albuquerque [24] defende que «*A informação sintoniza o mundo. Como onda ou partícula, participa na evolução e da revolução do homem em direcção à sua história. Como elemento organizador, a informação referencia o homem ao seu destino. … A importância que a informação assumiu na actualidade pós-industrial recoloca para o pensamento questões sobre a sua natureza, seu conceito e os benefícios que pode trazer ao indivíduo e no seu relacionamento com o mundo em que vive. Associada ao conceito de ordem e de redução de incerteza, a informação identifica-se com a organização de sistemas de identidades inanimadas ou de seres vivos racionais*».

Contudo, Varajão, João Eduardo Quintela [25] define «*informação como sendo um conjunto de dados, colocados num contexto útil e de grande significado que, quando fornecido atempadamente e de forma adequada a um determinado propósito, proporciona orientação, instrução e conhecimento ao seu receptor, ficando este mais habilitado para desenvolver determinada actividade ou decidir. Numa definição empírica, podemos dizer que informação é tudo aquilo que reduz incerteza sobre um dado facto, lugar ou acontecimento, passado, presente ou futuro. Um instrumento de compreensão do mundo e de acção sobre ele*».

3.2- Gestão de Risco e Controlo

De acordo com o dicionário Priberam da Língua Portuguesa “Segurança” é o «*conjunto das acções e dos recursos utilizados para proteger algo ou alguém*».

No contexto do presente trabalho, aquele “algo” é a “Informação” que é considerada um recurso estratégico dentro das organizações. Como tal, será um Activo, ou seja - «*qualquer coisa que*

tenha valor para a organização», em conformidade com o conceito definido pela ISO27000 [26].

Contudo, em todas as "coisas", em todos os "algos", em todos os "activos" existem pontos fracos, isto é, existem Vulnerabilidades - «*fraqueza de um activo ou de um controlo que pode ser explorado por uma ameaça*» ISO27000 [27], sendo a Ameaça «*a causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização*» ISO27000 [28]. Assim, incidentes indesejados levam-nos à noção de Ataque que a ISO27000 [29] define como a «*tentativa para destruir, expor, alterar, incapacitar, roubar ou adquirir acesso não autorizado ou efectuar uso não autorizado de um activo*».

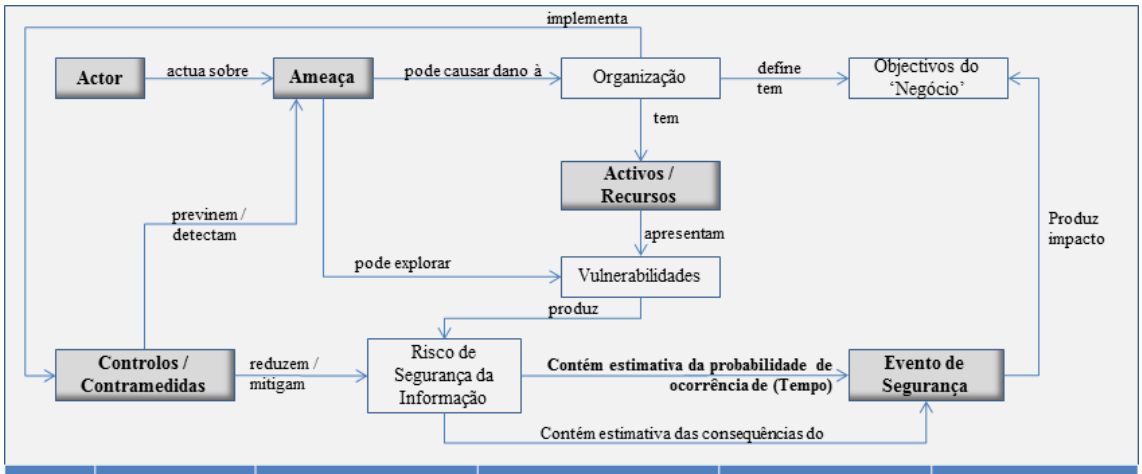
Todavia, os incidentes indesejáveis não acontecem sempre, pelo que deveremos introduzir o conceito de Risco que a ISO27000 [30] define como a «*combinação da probabilidade da ocorrência de um conjunto particular de circunstâncias e as suas consequências*».

Igualmente para Oliveira, Wilson [31] aquele conceito é «*a possibilidade de uma determinada ameaça explorar vulnerabilidades de um activo ou grupo de activos para causar perdas ou danos a estes*».

Assim, para conseguirem cumprir o desiderato de "proteger o que de valor existe nas organizações", estas recorrem ao Controlo que a ISO27000 [32] determina como os «*meios da gestão do risco, incluindo políticas, procedimentos, directrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, de gestão, técnica, ou de natureza jurídica*».

Do mesmo modo, Gonçalves, Hélder [33] apresenta a ideia de "Controlo" como «*uma forma de gerir um risco, garantindo que um objectivo de negócio é atingido, ou que um processo seja seguido. É a medida posta em prática para regular, orientar e monitorizar um risco*».

Na figura (Figura 3.1) resume-se, em forma de diagrama, os conceitos acima mencionados.



Actor	Ameaça (Tipo)	Activos / Recursos	Tempo	Evento de Segurança	Controlo / Contramedidas para:
Interno	Maliciosa	Pessoas / Organização	Duração	Divulgação	Reduzir
Externo	Acidental / Erros	Processo	Cronometragem da ocorrência (Crítica, Não-Crítica)	Interrupção	Mitigar
	Falha	Infra-estrutura (instalações)	Cronometragem para detecção	Modificação	Transferir
	Natural	Infra-estrutura de TI		Roubo	
	Exigência Externa	Informação		Destruição	
		Aplicações		Desenho ineficaz	
				Execução ineficaz	
				Regras e Regulamentação	
				Uso inapropriado	

Figura 3.1- Diagrama Conceptual - Gestão de Risco e Controlo. Adaptado Fernandes, J.H.C. e ISACA [34]

3.3- Segurança da Informação

Balizando para o âmbito do presente trabalho, a protecção do bem "informação" leva-nos à procura do conceito de "segurança da informação" que Wiander, Timo et al. [35], citando a ISO, definem como «*a protecção da informação numa larga gama de vulnerabilidades de modo a assegurar a continuidade do negócio, a minimização de riscos e a maximização do retorno do investimento e oportunidades de negócio*». Os mesmos autores continuam referindo no mesmo artigo que a «*Segurança da Informação é necessária para assegurar as acções legítimas e confiáveis num sistema de automatização, bem como a respectiva protecção dos dados no sistema. Uma perspectiva clássica da segurança da informação apresenta o modelo CIA (confidencialidade, integridade e disponibilidade dos dados), o qual é largamente adoptado na indústria e em vários standards (como ISO) e boas práticas*».

3.3.1 – Enquadramento Geral

O acto ou efeito de segurar a informação tem vindo a ser debatido e analisado pela comunidade científica, académica, por grupos sociais, empresariais e/ou pela sociedade em geral, principalmente, na identificação daquilo que serve de base para diminuir os riscos ou os perigos

de “violação” da mesma. São exemplo disso o manancial de teorias, modelos, metodologias, políticas, *standards*, normas, leis e/ou ferramentas desenvolvidas e em constante actualização como o BMIS, o NIST, a *ISO da série 27000*, o COBIT, etc. Por outro lado, o avanço tecnológico também tem proporcionado valor acrescentado na implementação de controlos dissuasores, preventivos, de detecção e/ou correctivos, abrangendo áreas como o controlo de acessos, as comunicações, a segurança física e/ou operacional, a criptografia, a arquitectura de sistemas, etc.

O enorme progresso existente nas áreas da Internet e das comunicações electrónicas tornou estes domínios centrais para a economia e sociedade em geral. Ao contrário do eventualmente esperado pelo avanço tecnológico, a perda de informação é, nos dias de hoje, um facto incontornável, transformando-se este feito num agente prioritário e mobilizador para a sua protecção dentro das organizações.

A *European Network and Information Security Agency* – ENISA [36] reporta cinco exemplos de incidentes cibernéticos com grande impacto nos utilizadores individuais, na economia e na sociedade em geral. São eles:

> *«1. Em Junho de 2012 – violação de 6,5 milhões (SHA-1) hashed passwords de um grande negócio focado numa rede social. O impacto da violação não é totalmente conhecida, mas milhões de utilizadores foram convidados a alterar as suas senhas, porque os seus dados pessoais poderiam estar em risco.*
>
> *2. Em Dezembro de 2011 - a tempestade Dagmar afectou o fornecimento de energia para redes de comunicações electrónicas, na Noruega, Suécia e Finlândia. O resultado foi que milhões de utilizadores ficaram sem telefonia ou internet durante duas semanas.*
>
> *3. Em Outubro de 2011 - houve uma falha no centro de dados do Reino Unido de um grande fornecedor de smartphone. O resultado foi que milhões de utilizadores em toda a UE e no mundo não puderam enviar ou receber e-mails, o que afectou severamente o sector financeiro.*
>
> *4. Durante o verão de 2011 – violação de segurança numa autoridade de certificação holandesa possibilitou a emissão de certificados falsos.*
>
> *5. Em Abril de 2010 - um fornecedor de telecomunicações chinês foi atacado, desviando, durante 20 minutos, 15% do tráfego mundial de internet através de servidores chineses. Como resultado, as comunicações de Internet de milhões de utilizadores foram expostas (à escuta).»*

Também, no estudo de *benchmark* realizado pelo Ponemon Institute [37] a empresas norte americanas sobre o custo anual do crime cibernético, a "perda de informação" (Information loss), apesar de ter diminuído (2%) face aos resultados de 2010, ainda se encontra no top do espectro, acumulando (40%) dos custos totais externos, conforme se pode verificar na (Figura 3.2).

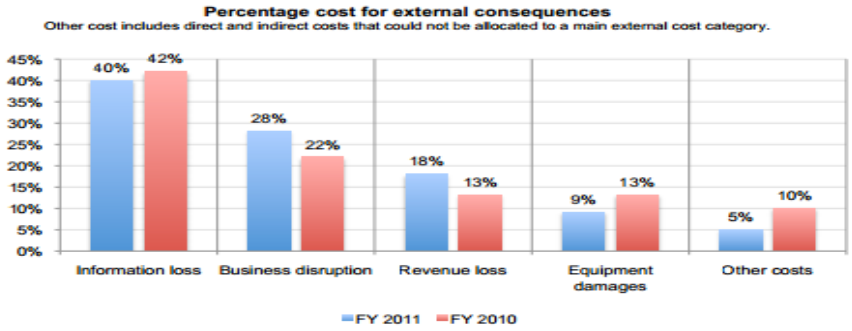


Figura 3.2-Custo anual do crime cibernético. Fonte: *Penomen Institute*

Com impacto também significativo, considerando o aumento percentual de (6%) e de (5%), respectivamente, face aos valores de 2010, estão os ataques para a disrupção de serviço e as perdas de receitas, conforme se constata na figura (Figura 3.2).

Assim, as mudanças tecnológicas, redes de comunicações globais e o intenso uso das tecnologias de informação, obrigam a que haja, cada vez mais, a necessidade de efectivamente implantar sistemas que acautelem o risco e possibilitem a gestão da segurança da informação.

Contudo, conforme Oliveira, Wilson [38] defende «*devemos ter como premissa básica que: não existe nenhum sistema seguro em todos os aspectos*». Assim, e ainda segundo o mesmo autor [39], «*a segurança da informação deve ser tratada como uma actividade contínua, pois existirão sempre novas técnicas de ataques da informação e consequentemente teremos de estar sempre atentos e prontos para o contra-ataque. A melhor arma para nossa defesa é estarmos sempre actualizados e nunca descurarmos a segurança …*», acrescentando que «*A gestão é o factor chave de todo o processo de implementação de segurança*».

3.3.2 – Governação e Gestão da Segurança

A segurança da informação é uma área disciplinar que remonta desde há séculos, com enfoque no âmbito das organizações de defesa e governamental. A informação é classificada segundo critérios de acessibilidade e são definidas as regras de acesso, conservação e as respectivas normas de protecção da mesma.

Todavia, como parte integrante dos processos organizacionais e com o impacto que a "perda de informação" representa actualmente nas organizações, muitos são os autores que defendem que a segurança da informação deverá integrar o sistema de governação corporativa das organizações.

Entre outros, Wiander, Timo, et al. [40] referem que «*a assimilação das acções de segurança da informação no sistema de gestão corporativo e suas componentes cria uma base bem projectada para uma gestão da segurança da informação*».

Igualmente Poole, Vermon [41] indica que «*… a efectiva governação requer que o conceito de responsabilidade partilhada seja construído sobre uma estrutura de segurança da informação capaz de estabelecer resiliência operacional e de negócio*».

Assim, de forma a cumprirem as suas missões e a alcançarem os objectivos estratégicos a que se propõem, as organizações necessitam de identificar e realizar, com eficácia e eficiência, um conjunto de actividades. Qualquer actividade que utilize recursos necessita de ser gerida de forma a ser capaz de transformar entradas em saídas, usando um conjunto de acções interligadas e /ou interrelacionadas.

A transmissão da informação com garantia da sua integridade e a disponibilidade da mesma no tempo, local e destino requerido é crítica na execução da missão das organizações. Contudo, torna-se igualmente importante garantir a protecção da informação corporativa, visto que a mesma é considerada um dos activos mais "valiosos" das organizações.

Tendo em conta que os recursos existentes não são ilimitados e que a implementação da segurança a 100% não é fazível, como endereçar estes problemas?

Por outro lado, "segurar/proteger" significa muitas vezes "restringir". Por vezes, nem todos os atributos de segurança podem coexistir no mesmo sistema e por vezes é preciso efectuar escolhas: quais os atributos a utilizar e a que profundidade devemos efectuar a sua implementação? Mudanças num atributo podem implicar alterações positivas ou negativas noutros. Por exemplo, implementar mecanismos de segurança num sistema poderá degradar o seu desempenho, pelo que será necessário estabelecer o compromisso entre a política de segurança a seguir e os objectivos de negócio a alcançar. Isto leva-nos a pensar que a gestão da segurança da informação deverá fazer parte integrante da governação corporativa das organizações e que os profissionais de segurança da informação são todos aqueles que lidam e partilham este recurso nas organizações.

Porém, com a introdução das tecnologias de informação como suporte à recolha, armazenamento, processamento e divulgação da informação, tornou-se necessário acautelar

também a informação que corre sobre estes suportes, surgindo a necessidade de definir regras e procedimentos que sistematizassem as actividades de protecção da informação nos seus três vectores de intervenção: confidencialidade, integridade e disponibilidade.

No início da década passada, a segurança da informação era geralmente relacionada como uma actividade da função de suporte - gestão das tecnologias de informação. Esta surgia, na maioria dos casos, distinta dos objectivos da organização.

Contudo, a governação das tecnologias de informação é, provavelmente, uma das mais complexas e desafiadoras funções no contexto organizacional, uma vez que, para além das inúmeras mudanças e inovações tecnológicas, que contribuem para a emergência de novos riscos, acresce a necessidade da organização ter de se adaptar constantemente ao seu contexto de mercado.

Desta forma, a governação das tecnologias de informação carece, tal como os outros recursos da organização, de uma gestão sistematizada e repetitiva, obrigando à identificação de um conjunto formal e informal de regras e práticas.

Na opinião de Hamaker, Stacey et al. [42] «*As tecnologias de informação (TI) são um requisito fundamental e penetrante em muitas das modernas organizações. O enfoque incremental na governação corporativa organizacional levanta questões acerca do papel das TI na governação global do negócio. Uma melhor compreensão deste papel equiparará melhor as organizações para endereçar os actuais desafios emergentes*». Alegam ainda que «*as empresas vêem as TI como uma área de actuação que pode ajudá-las a fazer crescer e sustentar as suas organizações. A indústria das TI nos últimos 5 a 10 anos moveu-se de um lado predominantemente de manufactura para o outro lado predominantemente de fornecedor de serviços*». Continuam indicando que «*… é imperativo que as organizações alavanquem o uso das suas tecnologias de informação (TI) para maximizar a eficiência, a eficácia e a confiança da organização num ambiente de volatilidade actual e de intensificada expectativa na governação corporativa*».

Gonçalves, Helder [43] cita a definição sobre "Governação das Tecnologias de Informação" apresentada pelo COBIT Foundation Course, que a define como «*um conjunto de estruturas e processos que visam garantir que as TI suportam e maximizam adequadamente os objectivos e estratégias de negócio da Organização, adicionando valor aos serviços entregues, balanceando os riscos e obtendo o retorno dos investimentos*».

Porém, está demonstrado, que o tema da segurança da informação não passa só por uma questão técnica. De facto, Tashi, Igli et al. [44] citam Posthumus, Shaun et al. [45] relativamente à

identificação, formulada por estes últimos, «*das quatro vagas relacionadas com a Segurança da Informação: primeiramente a vaga das questões técnicas, segundo a vaga da gestão, terceiro a vaga da uniformização e a quarta a relacionada com a Governação da Segurança da Informação*».

Também Dodds, Rupert [46] defende que «*Segurança é gestão de risco e esta gestão de risco cobre oportunidades e ameaças. Consequentemente, a segurança do sistema de informação tem na proposição de valor dois componentes: a habilitação do negócio e a protecção de activos. Segurança cobre pessoas e questões de processos, bem como tecnologia, pelo que a Segurança precisa de ser integrada na estrutura da gestão de risco organizacional e cobrir toda a organização*».

Verifica-se, então, que a comunidade científica tem vindo a defender cada vez mais uma mudança de paradigma na forma de "olhar" para a Governação da Segurança da Informação: mais do que uma questão de protecção de activos, a governação da segurança da informação deverá suportar a criação de valor para as organizações.

Malik J. William [47] menciona que «*a operacionalidade efectiva da Governação da Segurança da Informação pode transformar as organizações. De repente e sem preocupações, domínios inteiros da actividade de negócio tornam-se claros e compreensíveis. Governação eficaz revela conexões profundas entre os elementos do programa de segurança da informação da organização*».

De forma a estruturar e a sistematizar as actividades de segurança dentro das organizações, a comunidade científica tem vindo a desenvolver e a apresentar modelos, *guidelines, standards*, que possibilitam o apoio à implementação do Sistema de Gestão de Segurança da Informação.

A ISO27000 [48] define aquele como «*parte do sistema global de gestão, baseado numa análise de risco do negócio, para estabelecer, implementar, monitorizar, rever, manter e desenvolver segurança da informação*».

Gonçalves, Hélder [49] defende que um «*Sistema de Gestão da Segurança da Informação é projectado para assegurar a selecção de controlos de segurança adequados para proteger os activos de informação e proporcionar confiança às partes interessadas. É um standard formal que permite a certificação independente de organizações no Processo de Gestão da Segurança da Informação*».

O NIST [50] define também o "Plano do Programa da Segurança da Informação" como «*o documento formal de segurança da informação que fornece uma visão geral dos requisitos de segurança para um programa de segurança da informação global a toda a organização e que*

descreve os controlos do programa de gestão, em vigor ou os planeados, de forma a atingir as exigências traçadas». No entanto, Brotby, Krag [51] refere que «*… baseada na pesquisa/avaliação do ITGI, cerca de 70% a 80% das organizações globais claramente não têm implementado a governança da segurança da informação*».

Também, Pironti, John P. [52] refere que «*… num estudo disponibilizado pelo ISACA – Critical Elements of Information Security Program Success, os seis factores críticos mais reportados na pesquisa foram:*

1. *Compromisso da gestão de topo às iniciativas da segurança da informação.*
2. *Entendimento da gestão de topo para as questões da segurança da informação.*
3. *Planeamento da segurança da informação antes da implementação de novas tecnologias.*
4. *Integração entre o ´negócio` e a segurança da informação.*
5. *Alinhamento de segurança da informação com os objectivos da organização.*
6. *Responsabilização dos executivos e/ou dos gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança»*.

Igualmente, Malik J. William [53] fazendo referência à segunda edição do "*Information Security Governance: Guidance for Boards of Directors and Executive Management*" publicada pelo IT Governance Institute (ITGI) chama a atenção para os principais *drivers* na implementação e operacionalização de um programa/Sistema de Gestão de Segurança da Informação citando «*os sete elementos chave que colectivamente garantem que o programa de gestão da segurança da informação seja operacionalmente eficaz: 1- Governação; 2 – Política; 3 – Arquitectura; 4- Conscientização e formação; 5 – Tecnologia; 6 - Registo, auditoria e relatórios; 7 – Revitalização*».

Todavia, o ISACA [54] refere que «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*».

Por outro lado, Tashi, Igli et al. [55] defendem a existência de quatro princípios de garantia da segurança no quadro da segurança da informação, a saber:

- *«O risco zero não existe, consequentemente uma segurança absoluta também não existe;*

- *Protecção em profundidade, ou seja, a criação de uma série de sobreposição de camadas de controlo e contramedidas, dando a garantia de que de alguma forma o ataque deve ser quebrado;*
- *Segurança da informação depende de dois tipos de requisitos: funcionais e de garantia; isto significa fazer as coisas certas e de forma correcta;*
- *Delimitação do âmbito da Segurança da Informação, abrangendo o modelo CIA (Confidencialidade, Integridade e Disponibilidade)».*

Contudo, para a implementação destes sistemas/programas, a comunidade científica tem demonstrado e defendido a aplicação de métodos/modelos, como por exemplo o PDCA [Plan, Do, Check, Act] [56], que obriga à realização de um ciclo de vida de quatro etapas (Figura 3.3): 1 – Planeamento; 2 - Implantação e operacionalização; 3 - Monitorização e revisão; 4 - Manutenção e melhorias, permitindo que as organizações possam evoluir positivamente para estados de maior eficácia e eficiência, consequentemente de melhor qualidade e em rumo à excelência.

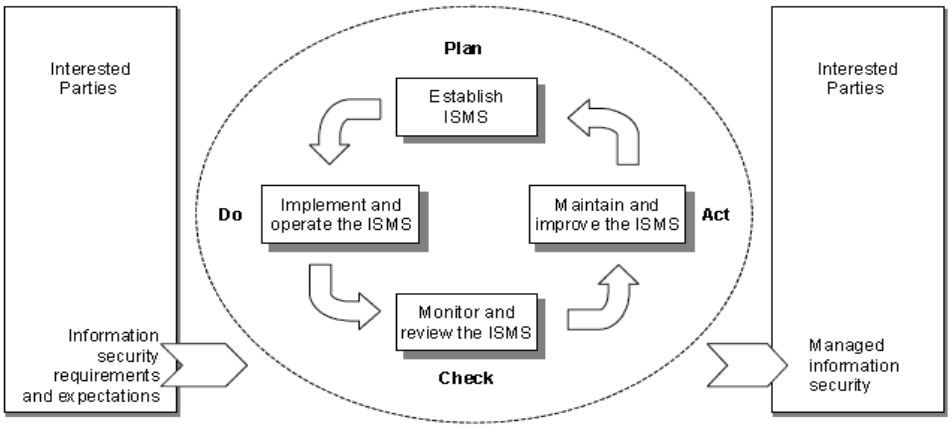


Figura 3.3- Modelo PDCA aplicado ao SGSI. Fonte: *ISO/IEC 27001:2005*

De facto, são métodos que obrigam às práticas de planeamento, operacionalização, monitorização, avaliação e revisão dos sistemas em causa, devendo aquelas formas de actuar tornarem-se, cada vez mais, uma parte integrante do modo de ser/estar nas actividades do dia-a-dia dos funcionários, dentro da organização.

3.3.3 – Principais Referenciais - Modelos, *Frameworks*, Standards e Normas

Neste contexto, a comunidade científica tem vindo a desenvolver e a disponibilizar *standards* para ajudar as organizações na implementação organizada e estruturada da Governação da

Segurança da Informação, relacionada com a Governação das TI e com a Governação Corporativa, incluindo modelos, *frameworks*, padrões e normas de segurança da informação de que são exemplo: BMIS, COBIT, ISO/IEC- 27001/2, etc. Assim, o ISACA [57] publicou o modelo BMIS, que «*apresenta uma solução holística e dinâmica para o desenho, implementação e gestão da segurança da informação. Em alternativa a aplicar controlos de segurança resultantes de análise de 'padrões causa-efeito', o BMIS examina todo o sistema empresarial, permitindo à gestão endereçar as verdadeiras fontes dos problemas, enquanto maximiza os elementos do sistema que podem melhorar e beneficiar a empresa. Através do estudo de todos os factores que introduzem incerteza e correlacionando-os todos para uma melhor compreensão das actuais necessidades organizacionais, o BMIS complementa qualquer framework ou standard já existente. Ajudará a empresa na efectiva gestão de risco informacional de modo a minimizar as ameaças e assegurar confidencialidade, integridade e disponibilidade dos activos de informação empresarial, aproveitando-os para a criação de valor*», endereçando assim, de acordo com a mesma fonte, «*o programa de segurança ao nível estratégico ou de negócio*».

Tendo, ainda, como referência a mesma fonte, o BMIS, conforme representado na figura (Figura 3.4) «*é principalmente um modelo tridimensional. É composto por quatro elementos e seis interconexões dinâmicas (DI's). … podendo ser rodado ou distorcido dependendo do ponto de vista do observador. Como regra, todas as partes do BMIS interagem umas com as outras. Elementos estão interligados uns com os outros via as DI's. Se uma qualquer parte do modelo muda, as outras partes sofrerão também uma mudança. Num universo abrangente e bem gerido de segurança da informação, o modelo é visto como estando em equilíbrio. Se parte do modelo muda, ou se a vulnerabilidade persiste, o equilíbrio do modelo fica distorcido. As interdependências entre as partes do BMIS são o resultado da abordagem sistémica global. O modelo endereça os três elementos considerados tradicionais nas TI (Pessoas, Processos e Tecnologia) e adiciona um quarto elemento crítico (Organização). Em termos do programa de segurança da informação, a flexibilidade e influência dos elementos e DI's variam. … As DI's são: cultura, administração, arquitectura, emergência/surgimento, habilitação e suporte e factores humanos*».

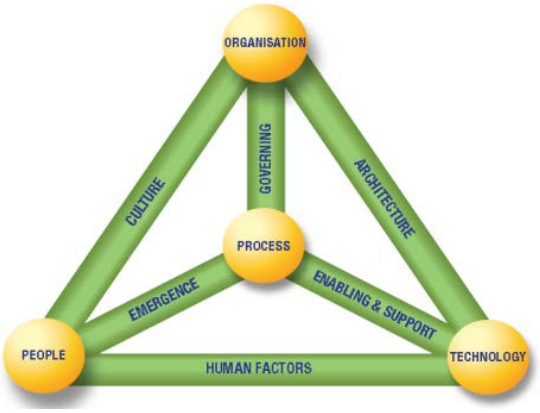


Figura 3.4 - Modelo BMIS - ISACA [58]

Citando, ainda, de forma adaptada Gonçalves, Hélder [59] «*A Governação das TI não é uma disciplina isolada, pois ela é parte da Governação Corporativa. As suas práticas de governação devem estar alinhadas com os objectivos estratégicos da Organização, contribuindo para que as TI sejam um veículo de adição de valor …*» e promotor «*… da melhoria contínua*». Neste contexto e, ainda segundo o mesmo autor «*o CobiT é, das frameworks que pretendem dar suporte à governação das TI, a que maior consenso reúne e está mais divulgada …*» sendo «*utilizado para avaliar o alinhamento estratégico de TI com as áreas de negócio da empresa, melhoria dos processos e controlos associados*».

De facto, o ISACA [60] refere que «*o COBIT 5 oferece um quadro abrangente que ajuda as empresas a atingir suas metas e a agregar valor através de uma governação e gestão corporativa eficaz das TI*». A mesma fonte, conforme se visualiza na figura (Figura 3.5) seguinte, mostra que «*os princípios e os facilitadores do COBIT 5 são genéricos e úteis para empresas de todos os tamanhos, seja comercial, de fins não lucrativos ou do sector público*».

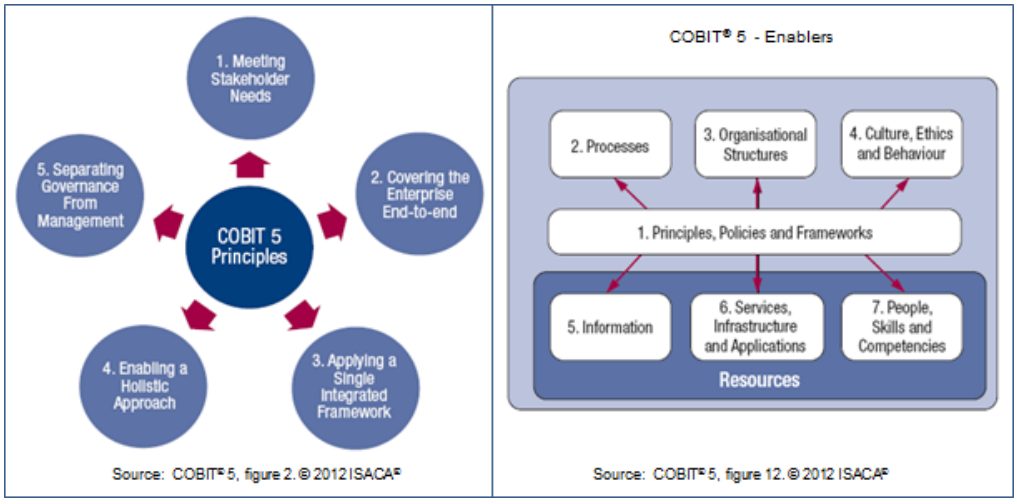


Figura 3.5- COBIT 5 - Princípios e Facilitadores. ISACA [61].

É, de realçar ainda que, de acordo com Gonçalves, Hélder [62] «*O CobiT é uma framework de governação e controlo que está focada em 'o que precisa de ser atingido' e não em 'como atingir'*».

Por outro lado, Santos, Luís [63] cita Solms, R. (1999) e indica que «*a conformidade com as normas e standards internacionais fornece uma base comum para todas as empresas desenvolverem, executarem e medirem efectivamente as práticas de segurança, e utilizá-las para melhorar a confiança entre as organizações*».

Ao longo das últimas décadas, têm sido desenvolvidas várias normas na área da segurança da informação. Visto que a família de normas da ISO/IEC 27000 apresenta a possibilidade de certificação possuindo, ainda, um leque alargado de orientações, cobrindo as mais variadas áreas/sectores de actuação e dada a sua importância e relevância a nível europeu e nacional, na figura seguinte (Figura 3.6) identifica-se essa diversidade.

Figura 3.6 - A Família ISO/IEC 27000 - Conjunto de normas relacionadas com a segurança da informação. Adaptado Gonçalves, Hélder [64]

Em Portugal, de acordo com o arquivo de certificações da ISO27001 [65] http://www.iso27001certificates.com/ (consultado a 21/02/2013) existem 18 empresas certificadas na ISO/IEC 27001:2005 e cujo registo foi efectuado.

Também nos EUA, fundada em 1901, o National Institute of Standards and Tecnology [66] (NIST) «*é uma agência federal não regulamentar dentro do Departamento de Comércio dos EUA. A missão do NIST é promover a inovação dos EUA e da competitividade industrial através do avanço da ciência de medição, padrões e tecnologia de forma a aumentar a segurança económica e melhorar a nossa qualidade de vida*».

Desta forma, o NIST através de uma das suas seis divisões do Laboratório de Tecnologia de Informação (ITL) - Divisão de Segurança Informática (CSD) [67] - tendo como missão «*estabelecer normas e tecnologia para proteger os sistemas de informação contra ameaças à confidencialidade da informação, integridade da informação e processos, e da disponibilidade de informação e serviços, a fim de construir a confiança em Sistemas de Tecnologia da Informação*» desenvolve e divulga, de entre outras, a Série 800 de Publicações Especiais do ITL/NIST [68] «*de interesse geral para a comunidade de segurança de tecnologias de informação e reportam a investigação da ITL, as directrizes e os esforços de sensibilização/divulgação em segurança de computadores, bem como as suas actividades de colaboração com a indústria, governo e organizações académicas*». Contudo, as normas e orientações produzidas «*sobre segurança da informação incluindo os requisitos mínimos para os sistemas de informação federais, não serão aplicados aos sistemas de segurança nacional sem a aprovação expressa dos oficiais federais a exercer funções sobre tais sistemas. Porém, estes standards e orientações podem ser utilizados de forma gratuita, por organizações não-governamentais*» [69]. Por outro lado, a mesma publicação do NIST indica, ainda, que «*está também a desenvolver 'bases/alicerces', colaborando com entidades dos sectores público e privado, nomeadamente através do estabelecimento específico de mapeamento e interligação entre standards de segurança e orientações desenvolvidos pelo NIST e pelo ISO/IEC*».

Dada a vasta gama de informação disponibilizada por aquela organização a figura (Figura 3.7) seguinte mostra as principais edições publicadas, considerando o que Gonçalves, Hélder [70] defende: «*Só conhecendo bem as ameaças a que a sua Organização está sujeita, é que a Gestão está em condições de gerir os riscos associados a essas ameaças de forma eficiente, pelo que é importante dotá-la do conhecimento e dos instrumentos que lhe permitem tomar as decisões adequadas*», afirmando, ainda, que «*o balanceamento entre riscos e controlos é, em termos financeiros e de imagem, fundamental numa boa gestão*».

De facto, também o NIST [71] considera a «*avaliação de riscos como uma componente chave de uma abordagem holística do processo de gestão de riscos em toda a organização, conforme definido na Publicação Especial 800-39, 'Gestão de Risco em Segurança da Informação: Organização, Missão e Perspectiva do Sistema de Informação'*».

Figura 3.7 – Adaptado [72] - *Standards* SP/NIST versus ISO/IEC

Por outro lado, face à actual importância da confiabilidade das redes e serviços de comunicações no bem-estar público e na estabilidade da economia e, sem a perda de relevância de outras áreas de segurança da informação, a segurança cibernética tem vindo a impor-se como uma prioridade naquele domínio.

Para cumprir tal propósito, alguns países elevaram a questão da "segurança cibernética" ao mais alto nível, definindo uma "estratégia nacional de segurança cibernética".

Segundo artigo publicado pela ENISA [73], as várias comunicações difundidas pela Comissão Europeia têm apontado para «*a criação de um espaço único de informação da Europa*». Indica, ainda, que a «*segurança cibernética é cada vez mais vista como uma questão horizontal e de estratégia nacional afectando todos os níveis da sociedade*» e refere que «*uma Estratégia Nacional de Segurança Cibernética (NCSS) é uma ferramenta que melhora a segurança e a resiliência de serviços e infra-estruturas nacionais*». Assim, indica ainda, que «*encontra-se em desenvolvimento um Guião de Boas Práticas que apresentará as boas práticas e recomendações de como desenvolver, implementar e manter uma estratégia de segurança cibernética*».

Ainda de acordo com o mesmo documento e, resumidamente, temos como principais referências as seguintes notas:

- *«As primeiras estratégias nacionais em segurança cibernética iniciaram nos primeiros anos da década passada, tendo os Estados Unidos da América sido um dos primeiros países a reconhecer essa matéria, resultado ainda dos ataques do 11 de Setembro de 2001.*
- *Em 2005, a Alemanha adopta o "National Plan for Information Infrastructure Protection (NPSI).*
- *Em 2006, a Suécia desenvolve a "Estratégia para melhorar a segurança na Internet na Suécia".*
- *Em 2007, e após vários ataques de severa gravidade a Estónia torna-se no primeiro país da União Europeia a publicar uma ampla estratégia nacional de segurança cibernética em 2008.*
- *Desde daí tem sido efectuado um trabalho considerável na área, a nível nacional e nos últimos quatro anos, mais dez estados membros publicaram as suas Estratégias em Segurança Cibernética, a saber: Estónia (2008), Finlândia (2008), Eslováquia (2008), República Checa (2011), França (2011), Alemanha (2011), Lituânia (2011), Luxemburgo (2011), Holanda (2011) e Reino Unido (2011).*
- *Fora da União Europeia muitos outros países, tais como Estados Unidos da América, Canadá, Japão, India, Austrália, Nova Zelândia e Colômbia, têm publicado as suas estratégias nesta área, o que ilustra que a importância da segurança cibernética é globalmente reconhecida».*

De facto, esta é uma área que se encontra em evolução e é cada vez mais pertinente na esfera da sociedade da informação. Para além dos ataques terroristas, as crises financeiras que tiveram lugar nos Estados Unidos da América e na União Europeia vieram reforçar a necessidade de regulamentar os diversos sectores (financeiro, saúde, …), obrigando as organizações a assumirem compromissos de conformidade. A tendência na União Europeia é clara conforme podemos consultar na sua *Estratégia Digital* [74], onde se inscreve a *Agenda Digital* [75] cujo «*objetivo é definir um roteiro que maximize o potencial das Tecnologias da Informação e da Comunicação (TIC), promovendo a inovação, o crescimento económico e o progresso, dando seguimento às iniciativas i2010, eEurope 2005, eEurope 2002 e eEurope*».

Em Portugal, o Gabinete Nacional de Segurança [76] é «*a entidade que tem como competência garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal faz parte, através do seu director-geral, que é por inerência a Autoridade Nacional de Segurança, a de autoridade de credenciação de pessoas e empresas para o acesso e manuseamento daquele tipo de informação*». No seu site [77] pode encontrar-se

a proposta de Portugal (ainda não aprovada), referente à Estratégia Nacional de Cibersegurança, onde são considerados três objectivos principais: «*Garantir a Segurança no Ciberespaço; Fortalecer a Cibersegurança das Infraestruturas críticas nacionais e Defender os Interesses Nacionais e a Liberdade de Ação no Ciberespaço*». Para cada um deles, foram identificadas as principais linhas de acção estratégica.

A figura (Figura 3.8) abaixo ilustra as principais "*Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas em Portugal*", já publicadas, realçando-se que também estas mencionam a "Importância do factor humano" SEGNAC 1 [78] referindo que «*Por mais rigorosas que sejam as medidas de segurança física e de manuseamento de documentos, não serão totalmente eficazes se não tiverem em conta a importância do factor humano. Esta circunstância envolve a avaliação contínua da idoneidade do pessoal autorizado a manusear matérias classificadas e ainda a conjugação daquelas medidas com a protecção obtida através de revistas, rondas, vigilância e inspecções, executadas por pessoal credenciado e devidamente preparado para o efeito*».

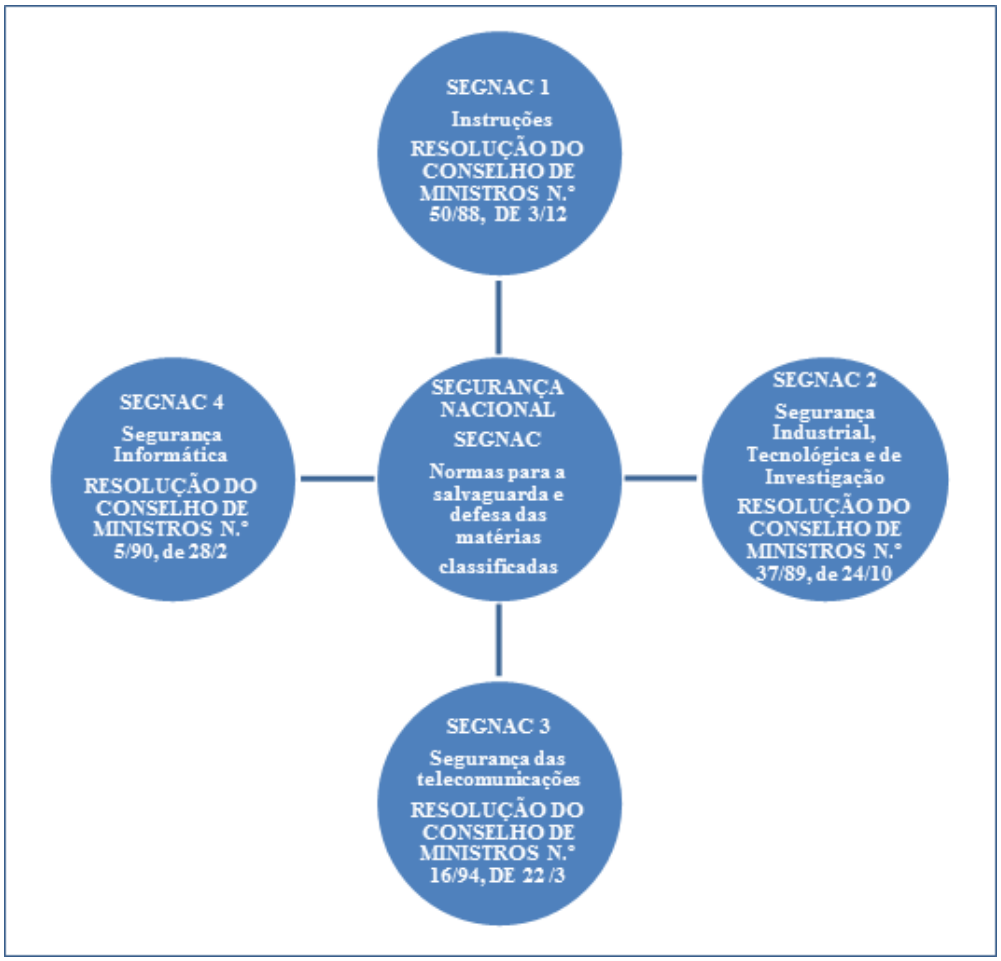


Figura 3.8- Legislação SEGNAC

Neste contexto, as normas e as estratégias definidas nesta área, não só contribuem para a sensibilização à tomada de consciência do impacto que a governação da segurança da informação pode trazer para as organizações, como facilitam o trabalho das mesmas na implementação, monitorização, manutenção do Sistema de Gestão de Segurança da Informação numa organização, contribuindo ainda para a normalização e melhoria contínua dos processos e procedimentos organizacionais.

Por outras palavras, é de referir o que Pironti, John P. [79] defende: «*a governação da segurança da informação devidamente dirigida pode bem ser um bom trunfo para o sucesso de uma organização*».

3.4 - Cultura Organizacional

Segundo Tavares, Fernanda Pereira [80] «*A palavra cultura surgiu a partir da antropologia social, ou seja, quando grupos de estudiosos, no final do século XIX e início do século XX, começaram a pesquisar sobre as sociedades primitivas e verificaram que os modos de vida de*

cada sociedade se diferiam entre si e entre regiões. O conceito de cultura foi, assim, criado para representar, em um sentido muito amplo e holístico, as qualidades de qualquer grupo humano específico que passem de uma geração para a seguinte. A cultura organizacional de uma empresa, por sua vez, manifesta-se, através da resistência à mudança, resistência essa consequente dos valores, crenças, mitos e tabus que encontram-se enraizados nessa empresa; manifesta-se, também, através de padrões de comportamentos ou estilo de uma organização assumido pelos funcionários, os quais incentivam novos colegas a seguirem».

A autora defende, ainda, que «*A cultura organizacional tem consequências poderosas…*» e no mesmo artigo tenta caracterizar a «*cultura organizacional como um instrumento de poder em relação às transformações ocorridas dentro do ambiente empresarial…*».

Contudo, para um conceito interpretativo de "cultura" a antropóloga Barbosa, Lívia Neves de Holanda [81] cita Geertz, C. [82] indicando que «*Cultura não é algo que se produz no interior de uma empresa ou se carrega para dentro dela. É um sistema de símbolos e significados de domínio público, no contexto do qual as tarefas e práticas administrativas podem ser descritas de forma inteligível para as pessoas que delas participam ou não. Do ponto de vista mais pragmático pode ser entendida como regras de interpretação da realidade, que necessariamente não são interpretadas univocamente por todos, de forma a permanentemente estarem associados seja a homogeneidade ou ao consenso. Essas regras podem e são reinterpretadas, negociadas e modificadas a partir da relação entre a estrutura e o acontecimento, entre a história e a sincronia*».

Todavia, esta autora patrocina que «*Até o momento, o conhecimento que a antropologia possui acerca dos processos culturais, da produção e circulação simbólica, da mudança e das relações entre diferentes sistemas está longe de permitir a produção de tecnologias que permitam intervenções, manejos e mudanças de forma tão controlada e orientada a corresponder às expectativas pragmáticas dos administradores em geral*».

Porém, conforme mencionado por Fleury, Maria Tereza Leme et al. [83] «*uma das definições mais conhecidas de cultura organizacional é a desenvolvida por Shein (1985):´Cultura organizacional é o conjunto de pressupostos básicos que um grupo inventou, descobriu ou desenvolveu ao aprender como lidar com os problemas de adaptação externa e integração interna e que funcionaram bem o suficiente para serem considerados válidos e ensinados a novos membros como a forma correta de perceber, pensar e sentir em relação a esses problemas.' … Segundo o autor, existem diferentes níveis através dos quais a cultura de uma organização pode ser apreendida:* ***artefactos visíveis****, como os produtos visíveis: layout da organização, comportamento das pessoas – fáceis de serem percebidos, mas difíceis de serem*

interpretados; ***Valores*** *- aqui o autor aponta o problema da diferença existente entre os valores aparentes e os valores em uso;* ***pressupostos básicos****, normalmente inconscientes, mas que na realidade determinam como os membros do grupo percebem, pensam e sentem*».

Também, Malcolmson, Jo [84] citando vários autores, refere que «*Cultura é essencialmente 'um conjunto de entendimentos expressos numa linguagem´, ou ´padrões de significado partilhado´, ou 'valores e crenças partilhados que interagem com as estruturas organizacionais e sistemas de controle para produzir normas comportamentais´*».

Já Santos, Maribel Yasmina et al. [85] referem que «*A cultura organizacional define a sua identidade, distinguindo-a de organizações congéneres. Ela permite unir as pessoas em torno de valores, normas e ideias comuns, permitindo-lhes perceber a mesma realidade e agir de forma concertada*».

3.5 – Cultura da Segurança da Informação nas Organizações

Apesar disso, Malcolmson, Jo [86] defende que a «*Cultura tem interesse num contexto de segurança se se provar que a mesma tem impacto nos resultados da segurança*».

Assim, Okere, Irene et al. [87] indicam que a «*Ameaça interna está no top das questões de segurança da informação nas organizações, sendo o factor humano considerado o elo mais fraco da cadeia de segurança*». Continuam mencionando que «*para endereçarem este 'factor humano' pesquisas têm sugerido a promoção de uma cultura de segurança da informação para encaminhar/dirigir o comportamento humano para que a segurança da informação se torne numa segunda natureza para os funcionários*».

Todavia, Malcolmson, Jo [88] defende que «*Cultura de segurança é indicada nos pressupostos, valores, atitudes e crenças, detidas por membros de uma organização, e os comportamentos que eles executam, o que pode ter potencialmente impacto sobre a segurança da organização, podendo ou não ser conhecido, de forma explícita, o vínculo a esse impacto*».

No Modelo de Negócio para a Segurança da Informação (BMIS) o ISACA adopta, de Kiely, L. et al. [89] o seguinte conceito: «*Cultura é um padrão de comportamentos, crenças, suposições, atitudes e maneiras de fazer as coisas*». Refere, ainda, que: «*A palavra 'padrão' é chave nesta definição. Culturas são feitas de indivíduos, mas não representam necessariamente comportamentos individuais. É a cultura que influencia comportamentos individuais e de grupo. Na utilização do BMIS existem duas camadas de cultura a serem consideradas: a organizacional – que é formada ao longo do tempo pela concepção, estratégia organizacional e comportamento das pessoas no trabalho, e a segunda camada encontrada em pessoas de*

cultura individual que pode ser diferente e heterogénea. Desta forma, ambas as camadas devem ser tidas em conta quando considerada a perspectiva de visualização da interconexão dinâmica (DI)-'Cultura' pois, esta, influencia a segurança». A figura (Figura 3.9) representa o modelo BMIS, tendo em conta o enfoque no elemento – "Pessoas" (Recursos Humanos).

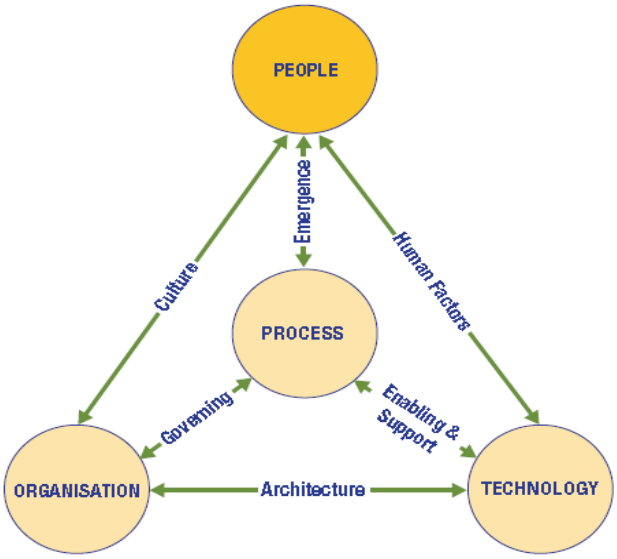


Figura 3.9- Modelo BMIS / Elemento 'Pessoas': representa os recursos humanos numa organização – funcionários, empreiteiros, fornecedores e prestadores de serviços. ISACA [90].

No âmbito da revisão bibliográfica efectuada verifica-se que a comunidade científica tem vindo a apontar a importância da cultura da segurança da informação como um pilar vital na implementação da segurança da informação nas organizações. Os estudos e pesquisas efectuados têm revelado que um dos elos mais fraco na cadeia da segurança numa organização é o "Factor Humano". Neste caso, tem sido demonstrado que a promoção de uma cultura de segurança da informação, integrada na cultura organizacional, é considerada uma ferramenta fundamental para a mitigação (minimização) do risco provocado por aquele factor.

Assim, o tema "cultura de segurança da informação" tem vindo a ser alvo de maior atenção da parte daquela comunidade e das organizações em geral, devido ao impacto que o "factor humano", tem manifestado ter nas questões de segurança, em geral e da informação, em particular.

Deste modo, Tashi, Igli et al. [91] propõem e descrevem um modelo para «*holisticamente avaliar a postura da segurança da informação. O modelo é inspirado em alguns bem-conhecidos standards de segurança. A ideia foi mapear os standards de segurança da engenharia com os modelos de não-engenharia de avaliação da função de Segurança da Informação, em ordem a formalizar o caminho para a avaliação da Segurança da Informação. O modelo permite o programa de Segurança da Informação através de preencher os requisitos*

de segurança tendo em conta duas principais características: Eficácia que significa que o sistema sob avaliação está a fazer a coisa certa e Eficiência que significa que o sistema sob avaliação está a fazer bem as coisas».

Porém, Helokunnas, Tuija et al. [92] tendo por base os estudos realizados por *Siponen*, sobre a conscientização da segurança da informação, defende a "cultura da segurança da informação" «*como um sistema que consiste na interacção de estrutura e categorias de componentes de conteúdos da segurança da informação*».

Citando Siponen, os mesmos autores indicam que «*Estrutura contém a informação formal e actividades como a normalização, certificação e medição da informação de segurança, ao passo que os conteúdos incluem as atitudes das pessoas, motivação e conhecimento, incluindo os modelos mentais acerca da segurança da informação*». Referindo ainda Siponen, aqueles autores reforçam a defesa do enfoque na «*importância das categorias de componentes de conteúdos (que incluem os aspectos humanos na era da institucionalização)*» mencionando que, «*se quase todas as medidas destinadas a aumentar a conscientização da segurança se concentrassem na categoria "estrutura", as deficiências sobre o conteúdo de segurança da informação são o que normalmente as invalida*».

Paralelamente, Okere, Irene et al. [93] defendem que «*A cultura em segurança da informação precisa de ser/estar embebida na cultura organizacional*».

Também Schlienger, Thomas et al. [94] são apologistas que a «*cultura de segurança deve suportar todas as actividades de tal modo que a segurança da informação se torne num aspecto natural nas actividades do dia-a-dia de cada funcionário. Cultura de segurança ajuda a construir a confiança necessária entre os diferentes actores*». Assim, afirmam, ainda, que «*a cultura de segurança da informação é uma parte da cultura organizacional*».

Como analisar, então, a "cultura de segurança" nas organizações? Recorrendo-se à pesquisa por revisão bibliográfica encontram-se várias abordagens. Ngo, Leanne et al. [95] citando Gerber e von-Solms indicam que «*Ocorreram três fases na evolução dos computadores. A primeira, a era centrada no Computador, focada nos controlos físicos que forneciam os mecanismos de protecção às localizações físicas dos ´mainframes`. A segunda, a era centrada nas TI, focada nos controlos técnicos tais como, proporcionar segurança ao nível do perímetro e da infra-estrutura tecnológica. A terceira, a era centrada na Informação, focada nos controlos operacionais, tais como, segurança e protecção da informação e recursos de TI*». Os autores referem, ainda, que «*alinhado com as três eras de evolução está a teoria de von Solms sobre as três vagas da segurança da informação. A primeira, a vaga Técnica, envolvendo o uso de ferramentas tecnológicas e métodos para endereçar a segurança da informação. A segunda, a*

vaga da Gestão, percebe-se que o suporte da gestão de topo é imperativo na segurança da informação. A terceira, a vaga da Institucionalização, preocupa-se com normalização, certificação, medição e aspectos humanos». Continuam, mencionando que «*von Solms propõe para discussão ainda uma quarta vaga – A do Produto*».

Contudo, Helokunnas, Tuija et al. [96] (Figura 3.10) - analisaram a teoria de *Von-Solms* sobre as vagas da segurança da informação e adicionaram uma perspectiva de convergência no tempo, defendendo que «*irá demorar mais tempo a verificar-se os efeitos da terceira vaga do que foi para as outras duas. A razão é porque esta vaga têm a ver com a atitude, conhecimento e percepção das pessoas face à segurança da informação. E isto leva mais tempo a mudar e a implementar do que os controlos técnicos e de gestão*».

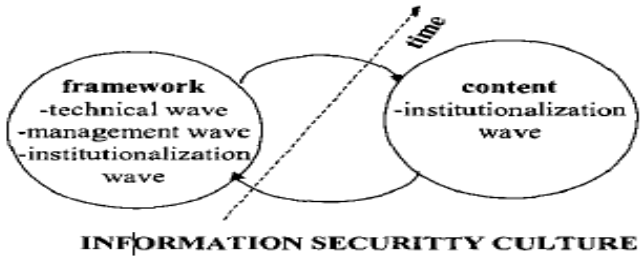


Figura 3.10- Componentes da Cultura da Segurança da Informação

Também, Schlienger, Thomas et al. [97] realçam que «*de modo a que a cultura da segurança possa contribuir, substancialmente, no campo da segurança da informação é necessário ter um conjunto de métodos para estudar a cultura da segurança. Infelizmente, não existe uma única ferramenta e método para estudar a organização mas a cultura existe*».

Assim, um passo importante na promoção de uma cultura de segurança da informação é a avaliação do seu estado, podendo trazer benefícios à organização, nomeadamente na forma como a mesma encara a governação da segurança da informação.

No mesmo artigo, os autores indicam, resumidamente, os vários métodos aplicados na avaliação da cultura da segurança da informação efectuados pelos diversos investigadores. Assim, citam três métodos:

- *«os primeiros métodos propostos pelos fundadores desta área de pesquisa Peters T.J. e Waterman, R.H., bem como Deal, T.E. e Kennedy, A.A., cuja abordagem consistiu na derivação dos valores através da execução de várias entrevistas conduzidas em algumas empresas ou dos estudos realizados, tendo em conta os indicadores culturais em empresas bem-sucedidas. Os resultados foram os quatro tipos culturais gerais de*

Deal/Kennedy e os oito princípios básicos de gestão de excelência de Peters/Waterman».

- *«o segundo método está muito ligado ao modelo de Schein (Figura 3.11). Este método tem em conta que a cultura não pode ser medida como um facto objectivo. A Cultura deve ser baseada no entendimento de pessoas envolvidas. Este método leva-nos para os estudos de casos e não lida com critérios catalogados que permitam uma comparação sistematizada das diferentes culturas conforme preconizado nos primeiros métodos».*

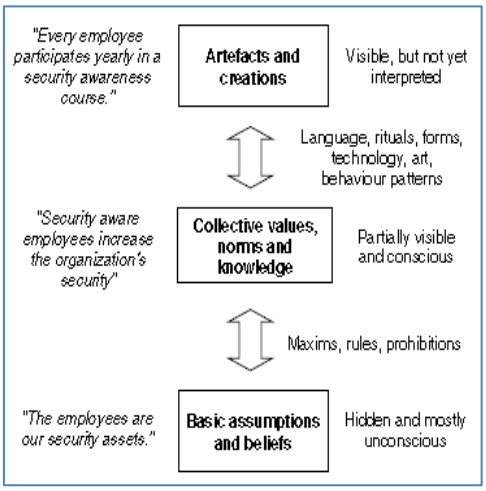


Figura 3.11 – Modelo de Schein – os três níveis da cultura de segurança

- *«o terceiro método, a metodologia Etno, propõe o assim chamado paradigma interpretativo. Os dados relacionados com a cultura organizacional podem ser agregados de maneira diferente conforme propostos pelos métodos anteriores. Um observador externo interpreta os artefactos observados tendo em conta a perspectiva da organização, como o proposto pelo segundo método. É também necessário definir os tipos culturais como propostos por Deal/Kennedy para possibilitar a sistematização. A diferença de pensamento recai na análise dos dados: enquanto os dois primeiros métodos propõem uma análise não empírica com diferenças conceptuais, o terceiro método usa o método empírico com recurso a análise estatística multivariável».*

Em relação à forma como os dados referentes à avaliação da cultura de segurança da informação podem ser recolhidos, os mesmos autores referem o seguinte:

- *«Para medir indicadores observáveis, os métodos geralmente propostos são: análise documental, observação física dos indicadores e entrevistas com membros da organização;*
- *Para a medição de normas, valores e crenças, são propostos os seguintes métodos: entrevistas narrativas, observação participativa e sessões de grupo».*

Contudo, Okere, Irene et al. [98] patrocinam que as metodologias para a avaliação da cultura em segurança da informação nas organizações, devem seguir as seguintes linhas de orientação:

- *«avaliar os diferentes níveis da cultura de segurança da informação*
- *Incluir métodos para avaliar cada nível da cultura da segurança da informação*
- *Usar uma abordagem integradora para avaliar cada nível da cultura …»*

Todavia, no mesmo artigo, as autoras referem os quatro níveis da cultura de segurança da informação, propostos no modelo de Niekerk, Van et al. [99] que «*adaptado do modelo de Schein contempla um quarto nível 'Conhecimento da segurança da informação`, o qual suporta os outros três níveis: Artefactos, Valores Expostos, Suposições tácitas partilhadas*». Assim, continuando a citar os mesmos autores, Okere, Irene et al. [100] apontam oito etapas que compõem o processo de mudança de cultura organizacional, a saber: *«1- Compromisso e suporte da gestão de topo; 2- Definição específica do problema do ´negócio´; 3-Desenvolver um Plano de Acção Estratégica; 4- Criar um ajuste cultural; 5- Desenvolver e escolher uma equipe líder da mudança; 6- Criar pequenas vitórias; 7- Identificar métricas, medidas e metas; 8- Retorno e Revisão»*, mencionando, ainda, as seguintes razões para realizar a avaliação da cultura em segurança da informação:

- *«Permite identificar o estado actual, comparando-o com os objectivos que se pretende atingir, possibilitando a identificação e a priorização do que é necessário realizar.*
- *Ajuda a organização a compreender o comportamento dos seus funcionários nas questões de segurança da informação e identifica as questões chave para a implementação e integração da cultura de segurança da informação na organização.*
- *Permite implementar soluções e endereçar outras que surgem na sequência de outras avaliações, possibilitando uma evolução na cultura da segurança da informação.*
- *Ajuda a reforçar as recomendações que foram implementadas na sequência de avaliações prévias.*
- *Por último, pode ainda servir como um ´wake-up´ para a forma como a gestão olha para estas questões ligadas à segurança da informação.»*

3.6 – O Sector da Água e Saneamento

«*A vida e todos os sectores da economia dependem da água*». Jonch-Clausen, Torkil et al.[101]

Grey, David et al. [102] indicam que «*Água Segura tem sido definida como um objectivo global onde* …» e citam a Global Water Partnership, 2000 «*…cada pessoa tem acesso à água potável suficiente a um custo acessível para levar uma vida limpa, saudável e produtiva, garantindo que o ambiente é protegido e melhorado*». A 28 de Julho de 2010, a Assembleia Geral das Nações Unidas [103] declara, na sua Resolução n.º 64/292 «*A água e o saneamento como direitos humanos*».

Todavia, ainda segundo Grey, David et al. [104] «*A escala do desafio sempre presente da sociedade de alcançar a sustentabilidade da segurança da água é determinada por muitos factores, entre os quais se destacam … o ambiente sócio-económico – a estrutura da economia e o comportamento dos seus actores – que reflectem legados naturais e culturais e escolhas políticas* …». Assim, Jonch-Clausen, Torkil et al. [105] defendem que «*a gestão integrada dos recursos hídricos contempla duas categorias básicas de integração. A primeira é o 'sistema natural' que é um factor determinante da disponibilidade e da qualidade dos recursos hídricos. O segundo é o 'sistema humano', a forma de utilização do recurso, a produção de resíduos e a poluição do recurso e o que define as prioridades de desenvolvimento. A integração deve ocorrer em ambas, dentro e entre aquelas categorias, tendo em conta a variação no tempo e espaço*». Neste contexto, os mesmos autores patrocinam também que «*a integração no ´sistema humano´ envolve…*» de entre outros «*a vinculação do planeamento dos recursos hídricos para o âmbito da ´segurança nacional e políticas comerciais´*».

Também, Tortajada, Cecilia [106] indica que «*Governação, e no caso específico da ´governação dos recursos hídricos´ engloba, além de normas, regulamentos e instituições, as questões de ´valores´, tais como responsabilidade, prestação de contas, transparência, equidade e justiça. Isso adiciona uma enorme complexidade aos desafios ainda por resolver num quadro cada vez mais complexo de implementação de políticas de água… Gestão da água, e a sua governação, está agora, portando sob uma pressão multidimensional*».

Por outro lado, a evolução dos sistemas e das tecnologias de informação têm contribuído para uma "dependência" cada vez maior das organizações públicas e privadas e da sociedade em geral, incluindo o sector das Águas, pelo que Jonch-Clausen, Torkil et al. [107] mencionam que «*A arte da gestão integrada dos recursos hídricos, está na selecção, ajustamento e aplicação da combinação certa de um conjunto de ferramentas (que ajudam os gestores da água a realizarem as suas funções) para cada situação. Cinco categorias devem ter especial atenção:*

avaliação dos recursos hídricos, compreendendo redes de recolha de dados, técnicas de avaliação de impacto ambiental e ferramentas de gestão de risco; comunicação e informação; Ferramentas de distribuição de água e resolução de conflitos; Instrumentos de regulação e Tecnologia».

Deste modo, segundo Biswas, Asit K. et al. [108] «*A revolução da informação e comunicação tem tido um impacto radical na Água*» indicando que «*Todavia, ao contrário das mudanças climáticas, o desenvolvimento tecnológico é muito mais propenso a trazer surpresas positivas em numerosos aspectos do desenvolvimento e gestão da água*».

De facto, a indústria dos computadores evidenciou um progresso espectacular em muito pouco tempo. O desenvolvimento e implementação dos equipamentos de controlo, dos sistemas de informação geográfica (SIG), dos sistemas de supervisão/controlo e aquisição de dados (SCADA), de controlo de processos, de teleleitura de contadores e outros como de modelação de sistemas, o controlo de perdas, de gestão de activos/infraestrutura, de indicadores de suporte à decisão … têm revolucionado a forma de "olhar" para a informação, por parte das organizações nos sectores dos chamados "serviços de utilidade pública", nomeadamente no sector da Água e Saneamento.

A normalização das plataformas tecnológicas para *standard* abertos como o TCP/IP, Ethernet, a utilização de sistemas operativos comuns (Windows, Linux) e sistemas aplicacionais suportados em bases de dados comuns (SQL Server) veio possibilitar uma maior flexibilidade e interoperabilidade entre equipamentos e sistemas, mas adiciona também um maior risco, uma vez que estão sujeitos a um maior número de vulnerabilidades, que se exploradas por atacantes poderão originar falhas e/ou perturbações graves no funcionamento dos sistemas, colocando em causa a segurança e/ou a prestação continuada do serviço público. Assim, de acordo com o Conselho da União Europeia [109] *«… a segurança é em si mesma, um direito básico.… A segurança converteu-se portanto num factor-chave para garantir uma elevada qualidade de vida na sociedade europeia e para proteger as nossas infra-estruturas críticas através da prevenção e da luta contra as ameaças comuns*».

Assim, segundo as Águas de Portugal et al. [110] na apresentação de uma sessão temática sobre 'Planos de Segurança da Água: Onde estamos, para onde vamos.' mencionam que «*Em 2004, na linha da sua aposta estratégica na melhoria dos princípios e práticas de controlo da qualidade para consumo humano, a OMS propõe, nas Guidelines for Drinking Water Quality, 3th Edition, um novo conceito de gestão do processo de produção e distribuição de água potável, através da implementação de 'Planos de Segurança da Água (PSA)'. Estes Planos incorporam uma nova abordagem de avaliação e gestão de riscos em todas as etapas do*

sistema de abastecimento de água para consumo humano, desde da captação de água até à torneira do consumidor, propondo a mudança de abordagem de um processo de monitorização de conformidade de 'fim-de-linha' para um processo de gestão de segurança, assegurando assim, a segurança sanitária da água abastecida. Esta nova metodologia considera que as ameaças que podem constituir potencial risco para a saúde pública podem ocorrer em qualquer ponto do sistema de abastecimento de água, incluindo a fonte de água bruta, o tratamento, a distribuição e as redes domiciliárias. Estamos, assim, perante mais um importante passo numa cadeia de evolução na gestão de sistemas de água, que tem sido da maior importância na defesa da saúde pública e na dignificação das condições de vida das populações, com enorme impacto na diminuição da mortalidade infantil, na redução da morbilidade e no aumento da esperança de vida. Nessa conformidade, em 2004, a International Water Association, através de uma declaração conhecida como Bonn Charter for Safe Drinking, manifestou total adesão às propostas da OMS relativas aos PSA. A nível nacional merecem referência, além da posição da Entidade Reguladora dos Serviços de Águas e Resíduos, o Despacho n.º 2339/2007 do Ministério do Ambiente, do Ordenamento do Território e do Desenvolvimento Regional, que aprovou o Plano Estratégico de Abastecimento de Águas Residuais para o período de 2007-2013. Nesse despacho é conferida prioridade às actividades de I&D que apoiem a gestão de riscos em todo o ciclo urbano da água, a complementar por esquemas de contingência para assegurar elevados índices de confiança do público. Por outro lado, as informações disponíveis indicam que a Comissão Europeia virá a incorporar os Planos de Segurança da Água na próxima revisão da Directiva da Qualidade da Água para Consumo Humano».

Os 'Planos de Segurança da Água' (PSA) encontram-se actualmente integrados no âmbito do 'Plano de Exploração das Águas de Abastecimento', os quais deverão fazer parte da governação corporativa das Entidades Gestoras de Água e Saneamento em Portugal que são reguladas pela ERSAR.

Actualmente as organizações do sector das Águas e Saneamento em Portugal incluem, conforme se ilustra na figura (Figura 6.27) seguinte, na sua acção de governação os três domínios: 'Água', 'Segurança' e 'Informação'. Contudo, verifica-se a necessidade de 'olhar' para estes domínios, não apenas de uma forma 'interligada' ('*Onde Estamos*') mas, também de uma forma integrada ('*Para onde ir'*).

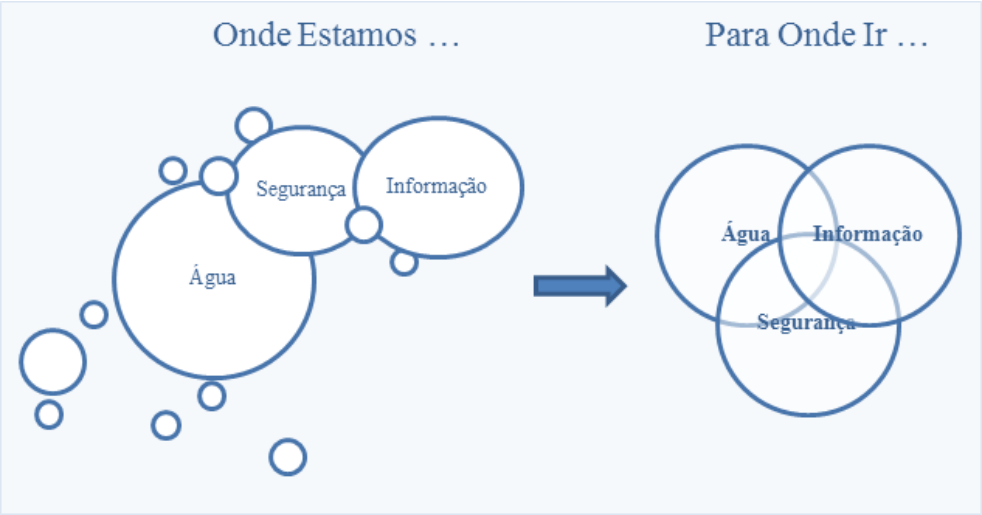


Figura 3.12- A mudança de paradigma no sector das Águas e Saneamento em Portugal

Deste modo, a governação da segurança da informação – assegurando a protecção de activos e possibilitando a criação de valor, pode bem ser o *driver* para alavancar a mudança de paradigma nestas organizações, contributo vital para a melhoria do pilar da estratégia para a Água Segura, resultando em ganhos na qualidade do serviço prestado.

De facto, a utilização da informação e sistemas de informação necessitam de ser considerados activos importantes destas organizações, pelo que se impõe a atenção relacionada com estas temáticas da governação da segurança da informação e da cultura em segurança da informação, integrando-as no Plano de Segurança da Água, cuja implementação se traduz numa gestão de risco com a criação de valor, permitindo a optimização do desempenho e da produtividade por parte das entidades gestoras, tirando o melhor partido dos recursos disponíveis.

Citando Dodds, Rupert [111] a «*Segurança do sistema de informação integrada na estrutura de governação do sistema de informação possibilita o seu alinhamento aos objectivos estratégicos do negócio e simultaneamente à protecção dos activos. Segurança gere riscos e o alinhamento à gestão de risco organizacional fornece uma estrutura para avaliar o investimento em segurança; cobre as pessoas, os processos e os aspectos tecnológicos; habilita os objectivos do negócio e protege os activos*».

Neste contexto, torna-se cada vez mais evidente a necessidade da utilização da "informação" como um recurso estratégico nas organizações em geral e deste sector, em particular, bem como a imprescindibilidade de abordar a "gestão eficaz e eficiente dos recursos hídricos" de uma forma holística, tendo por base a "gestão da segurança" através de uma abordagem de avaliação de risco, onde o recurso "informação" deverá ser considerado, em paralelo com o recurso "água", como factor de alinhamento à estratégia da organização, de forma a contribuir para a

resolução de problemas, criação de valor e garantia da continuidade dos serviços em situação de contingência.

Desta forma, o “factor humano” é indubitavelmente um ponto-chave, pelo que “criar uma cultura de segurança” nas organizações torna-se num desafio para as mesmas e, como anteriormente referido, deverá ser um foco da atenção da governação corporativa, bem como um objectivo prioritário da governação da segurança da informação nas organizações.

4. DESCRIÇÃO DO TRABALHO

Neste capítulo apresenta-se o racional utilizado, os objectivos e as motivações, bem como a abordagem utilizada (o que se usou e como se fez) na realização deste trabalho.

4.1 – Racional, Objectivos e Motivações

No decurso do capítulo anterior mostrou-se, através de revisão bibliográfica, a Informação como um recurso vital e «*instrumento de compreensão do mundo e de acção sobre ele*» Varajão, João Eduardo Quintela [112]. Daí, a relevância da utilização de tal meio, por parte das organizações. De facto, a informação ao «*proporcionar orientação, instrução e conhecimento pode habilitar, aquelas, para o desenvolvimento da sua actividade e consequente tomada de decisão*» Varajão, João Eduardo Quintela [113].

Contudo, se por um lado a evolução tecnológica incita à passagem do mundo do papel para o mundo electrónico, também é certo que a mesma, associada à globalização, faz aumentar a probabilidade de ataques capazes de pôr em causa a continuidade da actividade das organizações.

Neste contexto, torna-se necessário que as organizações desenvolvam mecanismos de protecção da informação, de forma a assegurar a continuidade do "negócio", a minimização dos riscos e a maximização do retorno do investimento e oportunidades de "negócio".

Assim, conforme anteriormente apresentado, vários são os autores que defendem que a governação da segurança da informação através da implementação dum Sistema ou Plano/Programa para a Gestão da Segurança da Informação, suportada na gestão do risco e partilhada/integrada na governação corporativa das organizações pode alavancar, não somente a protecção dos activos, como também possibilitar a criação de valor e a formação de vantagens competitivas.

Também se mostrou que a cultura organizacional e consequentemente a cultura da segurança da informação constituem pilares-chave na implementação da segurança da informação nas organizações. De facto, verifica-se que o "factor humano" é o elo mais fraco na cadeia de segurança, pelo que actuar preventivamente sobre este componente, facilita a criação sustentada de uma cultura de segurança da informação, proporcionando a entrega de valor e a resiliência organizacional.

Na figura seguinte (Figura 4.1) representa-se o modelo do racional teórico desenvolvido na realização do presente trabalho.

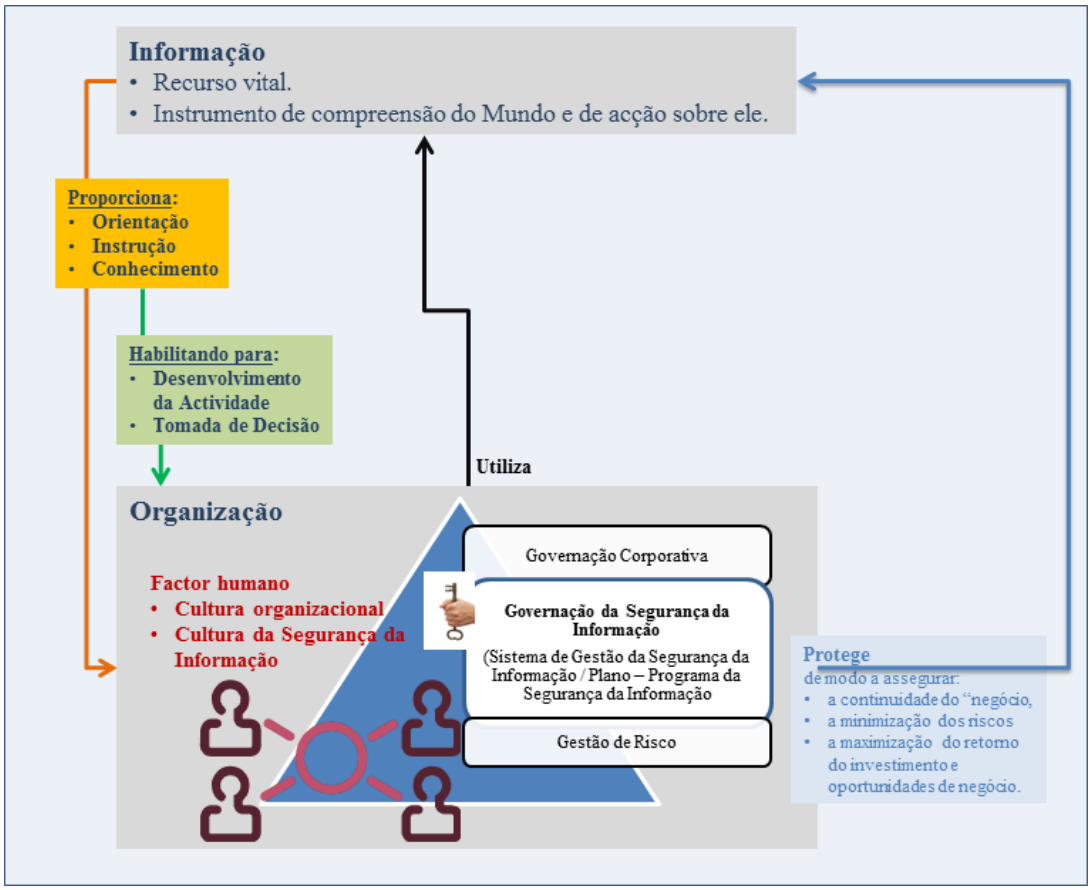


Figura 4.1- Modelo do Racional Teórico Desenvolvido

Porém, de acordo com as pesquisas efectuadas e anteriormente mencionadas, a implementação dum Sistema ou Plano/Programa de Gestão da Segurança da Informação tem sido um desafio para as organizações e muitas são as que ainda não aceitaram ou interiorizaram a importância e a mais-valia da aplicabilidade daqueles nas estruturas organizacionais.

Todavia, paralelamente também se verifica que esta não-aceitação por parte das organizações não se deve à falta de referenciais e/ou *guidelines*, uma vez que existe uma panóplia de modelos, *frameworks*, *standards* e normas disponíveis, embora se constate que a maioria proporciona "o que fazer" mas é "vago" na explicitação de "como fazer".

Assim, seguindo a linha de orientação dos autores que defendem que um passo importante na promoção de uma cultura de segurança da informação é a avaliação do seu estado, podendo trazer benefícios à organização, nomeadamente na forma como a mesma encara a governação da segurança da informação e acompanhando o pensamento de Okere, Irene et al. [114] que apontam, de entre outras, como razão para realizar a avaliação da cultura em segurança da informação, o facto de *«a mesma poder ainda servir como um ´wake-up´ para a forma como a gestão olha para estas questões ligadas à segurança da informação»* pretende-se, no âmbito da temática da segurança da informação, caracterizá-la no sector empresarial das Águas e

Saneamento em Portugal, segundo um dos pilar que é considerado de enorme relevância nas organizações – "o factor humano".

Assim, tendo por base as questões de apoio "Q1-Quais as crenças individuais dos profissionais na cultura da segurança da informação?" e "Q2 – Qual o impacto das crenças individuais na cultura de Segurança da Informação?" este estudo, de carácter exploratório e descritivo, tem como objectivos:

a) Investigar quais os Factores Motivadores (FM), Inibidores (FI), Críticos de Sucesso (FCS) e de Boas Práticas (FBP) que dão suporte à adopção/implementação de um Sistema de Gestão de Segurança da Informação (SGSI) nas organizações do sector de Águas e Saneamento em Portugal, tendo em conta a perspectiva do próprio (PP) e a perspectiva do próprio face à organização (PPO).

b) Comparar as duas perspectivas por meio do cálculo do nível médio de importância para cada elemento dos factores acima referidos.

c) Analisar os efeitos obtidos através do cruzamento do nível médio de importância dos elementos dos diferentes factores (FM, FI, FCS, FBP) com o mapeamento segundo a orientação do ISACA [115] que indica que «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*».

Assim, exclui-se do objecto do presente trabalho a realização da análise sobre a avaliação da cultura de segurança da informação, num quadro específico de utilização da mesma no âmbito dum processo de mudança cultural no sector seleccionado, dado o mesmo carecer de condução de dimensão estratégica adequada. Do mesmo modo que não se incluiu a observação directa de documentos e/ou de indicadores culturais, por ser temporalmente e funcionalmente inexequível.

Porém, apesar de âmbito redutor por apenas se diagnosticar, através de resposta a questionário, que Factores Motivadores, Inibidores, Críticos de Sucesso e/ou de Boas Práticas é que contribuem para a adopção/implementação de Sistema de Gestão da Segurança da Informação no sector das Água e Saneamento em Portugal, este estudo contempla:

- A envolvência de funcionários de diferentes tipos de categorias profissionais permitindo a análise comparativa por tipo de função e por cada factor.
- A perspectiva do próprio relativamente ao nível de importância que atribuem aos elementos seleccionados para cada factor, mas também a apreciação do seu ponto de

vista quando este se refere à organização, possibilitando a comparação das duas perspectivas, descobrindo-se a existência ou não de desvios.

Desta forma, apesar de reduzido o campo de acção da pesquisa, realça-se como principais pontos fortes os seguintes:

- Inovação do tema no sector seleccionado.
- Caracterização dos principais Factores Motivadores, Inibidores, Críticos de Sucesso e de Boas Práticas para a adopção/implementação de Sistema de Gestão da Segurança da Informação – na perspectiva do próprio e na perspectiva do próprio face à organização, bem como por tipo de função, ajudando o sector a compreender o estado actual do comportamento dos seus actores, abrindo para novos horizontes e possibilitando o endereçamento e encontro de outras soluções.
- Enquadramento dos itens que caracterizam cada um dos factores (motivadores, inibidores, críticos de sucesso e de boas práticas) mapeando-os, conforme o ISACA [116] refere que «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*», possibilitando a aferição da preocupação do sector para esta temática.
- Contribuição para a evolução da cultura da segurança da informação no sector, através do envolvimento dos respondentes ao questionário e da divulgação dos resultados do estudo, *«… servindo como um acordar para a forma como a gestão olha para estas questões ligadas à segurança da informação»*, Okere, Irene et al. [117].

Por último, de referir que foi seleccionado o sector da Água e Saneamento em Portugal, por representar uma área de interesse a nível nacional, onde actualmente a signatária exerce funções. De facto, cada vez mais este é um sector que utiliza os sistemas e tecnologias de informação.

Para além dos sistemas de informação de apoio às áreas de suporte organizacional, realçam-se os de suporte às áreas de "negócio" destas organizações, nomeadamente: sistemas de informação geográfica (SIG), dos sistemas de supervisão/controlo e aquisição de dados (SCADA), de controlo de processos, de teleleitura de contadores e outros como os que permitem a modelação de sistemas, o controlo de perdas de água, a gestão de activos/infraestrutura, a videovigilância, de indicadores de suporte à decisão …

Num estudo realizado, em Portugal, por Santos, Luís [118] sobre "Factores de Sucesso na Gestão de Segurança da Informação nas Empresas Portuguesas" concluiu-se que «*o factor ´Responsabilidades em Segurança da Informação´ foi o factor mais importante no sucesso da Gestão da Segurança da Informação e o factor ´Aconselhamento Externo de Serviços em Segurança da Informação´ foi o de menor importância comparados com os outros cinco factores: ´Suporte da Gestão de Topo´, ´Politica de Segurança da Informação´, ´Motivação dos Funcionários´, ´Programas de Sensibilização e Formação´ e ´Conformidade com Normas Internacionais de Segurança´*».

A mesma pesquisa indica, ainda, que as «*empresas portuguesas demonstram possuírem menor maturidade na classificação dos factores essenciais ao sucesso da Gestão da Segurança da Informação do que as empresas da Finlândia e da Jordânia*».

Além disto, o referido estudo, infere que «*na generalidade as empresas portuguesas encontram-se numa maturidade inicial ou em desenvolvimento de uma cultura de Segurança da Informação e fortemente associada a processos tecnológicos, verificando, no entanto, alguma maturidade nas empresas dos sectores financeiros e de telecomunicações*».

Acentua, também, que «*é sentida a necessidade de desenvolver uma consciencialização em Segurança da Informação, através de políticas governamentais, de carácter obrigatório para os organismos públicos e recomendada para o sector privado de forma a sensibilizar a gestão das empresas portuguesas nesta matéria*».

Assim, partindo deste conhecimento, pretendeu-se encontrar respostas no sector das Águas e Saneamento em Portugal, desbravando resistências, abrindo horizontes para a formação de uma cultura de segurança da informação que possibilitem a melhoria do planeamento estratégico dos investimentos e contribuam para uma gestão eficaz e eficiente dos recursos, capaz criar valor, resiliência e excelência nas organizações.

Seguidamente apresentam-se as actividades realizadas na execução deste trabalho.

4.2 - Abordagem

O que se utilizou

Conforme já referido, optou-se pela elaboração de um questionário (Anexo A) a enviar, por e-mail, à gestão de topo das organizações, solicitando a resposta ao mesmo, bem como a sua divulgação interna na organização, no sentido de envolver todos os funcionários nas organizações.

Como se fez

Neste estudo, de caracter exploratório e descritivo, foi utilizada uma abordagem qualitativa e quantitativa, onde se destacam as seguintes actividades:

- Elaboração de Questionário com base em estudos teóricos e empíricos, que faz parte do Anexo A deste documento. Para tal, procedeu-se à identificação dos tipos de factores e para cada um deles, quais os elementos que concorriam para caracterização do factor na escala respectiva. Assim, foram identificados quatro tipos de factores relacionados com a cultura organizacional na segurança da informação: motivadores, inibidores, críticos de sucesso e de boas práticas. De modo a aferir o nível de importância atribuído, pelos profissionais, foram identificados, para cada tipo de factor, elementos que possibilitassem aquela avaliação. Porém, cada elemento em cada tipo de factor foi classificado numa escala de 1 (Não é importante) a 4 (Muito importante), sendo 2 (Pouco importante) e 3 (Importante). Estes factores foram analisados tendo em conta duas perspectivas: a do próprio sobre a matéria e a do próprio face à organização de que fazia parte. Todas as questões foram consideradas de resposta obrigatória. A figura (Figura 4.2) retrata o modelo de questionário realizado.

Figura 4.2 - Modelo do Questionário Realizado

- Elaboração de folheto explicativo enviado, em anexo, na divulgação do Questionário, fazendo, também, parte do Anexo A deste documento.
- Divulgação do questionário *on-line* através de envio de e-mail aos Conselhos de Administração das Entidades Gestoras de Água e/ou Saneamento de Sistemas Municipais e Plurimunicipais, à Entidade Reguladora – ERSAR, a três Associações

(PPA, APDA e AMEGA) e a 6 empresas com actividade de prestação de serviços neste sector.

- Caracterização da amostra (ver ponto 4.3 deste capítulo) segundo os parâmetros estabelecidos para o respondente: função, área de formação, nível de formação, anos de experiência profissional, número de funcionários na organização, género e grupo etário.

- Elaboração do mapeamento de cada elemento de cada Factor (Motivador / Inibidor / Crítico de Sucesso / Boas Práticas) segundo a orientação do ISACA [119] que refere: «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*». Deste modo que factores, então, poderão ser considerados como motivadores, possibilitando a alavancagem na aplicação da governação da segurança da informação nas organizações? Tendo em conta o já referido pode considerar-se o indicado na tabela seguinte (Tabela 4.1).

Factores Motivadores	
Alinhamento Estratégico	"Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização"
Gestão de Risco	"Evitar perdas financeiras" "Ocorrência de incidente anterior" "Emergência de novos riscos" "Alterações continuas na legislação/regulação"
Gestão de Recursos	"Garantir a disponibilidade, confidencialidade e integridade da informação"
Gestão de Desempenho	"Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança" "Obrigatoriedade de conformidade com standards internacionais ISSO/IEC 27001/2, etc."
Garantia da Integração de Processos	"Planear a segurança da informação antes da implementação das novas tecnologias"

Tabela 4.1- Factores Motivadores: Mapeamento dos elementos segundo orientação ISACA

Porém, verifica-se que os profissionais de segurança também se debatem com Factores Inibidores na implementação destas orientações nas suas organizações.

Ainda mencionando o ISACA [120] este refere que «*Para ser justo, os profissionais da segurança da informação têm realizado um trabalho louvável dado os poucos recursos disponíveis. Orçamentos baixos, recursos humanos limitados e acesso restrito à gestão de topo são obstáculos comuns que os profissionais da segurança da*

informação enfrentam enquanto tentam proteger os activos informacionais, minimizar o risco e proporcionar valor acrescentado ao negócio».

Assim, como elementos a mapear os Factores Inibidores podem destacar-se os mencionados na tabela (Tabela 4.2) seguinte.

Factores Inibidores	
Alinhamento Estratégico	"Acesso restrito à gestão de topo"
Gestão de Risco	"Alterações continuas na legislação/regulação" "Emergência de novos riscos"
Gestão de Recursos	"Valor do investimento"
Gestão de Desempenho	"Dificuldade em medir o custo/benefício"
Garantia da Integração de Processos	"Falta de conhecimento" "Cultura organizacional"

Tabela 4.2- Factores Inibidores - Mapeamento dos elementos segundo orientação ISACA

Neste contexto, pode considerar-se como elementos a mapear os Factores Críticos de Sucesso na implementação ou adopção do Sistema de Gestão de Segurança da Informação os mostrados na tabela (Tabela 4.3) que se segue.

Factores Críticos de Sucesso	
Alinhamento Estratégico	"Entendimento da Gestão de Topo para as questões da segurança da informação" "Suporte da Gestão de Topo" "Politica de Segurança da Informação" "Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)"
Gestão de Risco	"Programas para a conscientização, educação e formação em segurança da informação" "Conformidade com Normas Internacionais de Segurança"
Gestão de Recursos	"Utilização de tecnologias de suporte (COBIT, ITIL, etc.)"
Gestão de Desempenho	"Responsabilização pela Segurança da Informação" "Motivação dos funcionários"
Garantia da Integração de Processos	"Auditorias de Segurança da Informação"

Tabela 4.3- Factores Críticos de Sucesso - Mapeamento dos elementos segundo orientação ISACA

Para aferir que boas práticas são consideradas como mais ou menos importantes num Sistema de Gestão de Segurança da Informação, dentro do sector, efectuou-se o

mapeamento para as boas práticas, conforme se visualiza na tabela (Tabela 4.4) seguinte.

Factores de Boas Práticas	
Alinhamento Estratégico	"Deve existir uma Politica de Segurança da Informação" "Deve existir Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)"
Gestão de Risco	"A minha senha de acesso não a partilho com ninguém" "Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC" "Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções" "Devem existir programas para a conscientização, educação e formação em segurança da informação"
Gestão de Recursos	"Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)"
Gestão de Desempenho	"Deve existir conformidade com standards internacionais de segurança(ISO/IEC 27001/2, COBIT e ITIL etc.)"
Garantia da Integração de Processos	"Devem existir auditorias de Segurança da Informação"

Tabela 4.4- Factores de Boas Práticas - Mapeamento dos elementos segundo orientação ISACA

- Análise e tratamento dos dados, cuja apresentação dos resultados pode ser encontrada no Capítulo 5 deste documento, dos quais destacam-se:
    - Indicação dos elementos de cada factor que foram os mais e menos votados, pelos participantes, tendo em conta o tipo de função do respondente, bem como cada uma das perspectivas: a do próprio e a do próprio face à organização.
    - Realização para cada elemento de cada factor, do cálculo médio ponderado das respostas, de forma a atribuir, a cada um dos elementos de cada factor, um nível médio de importância (NMI).
    - Elaboração da análise comparativa entre as duas perspectiva evidenciadas pelo respondente: a do próprio e a do próprio face à organização/sector para o qual trabalhava, tendo em conta o nível médio de importância calculado para cada elemento de cada factor e por tipo de função.
    - Elaboração da análise resultante entre o cálculo do nível médio de importância obtido para cada elemento dos factores (tendo em conta as duas perspectivas evidenciadas pelo respondente) e o mapeamento dos elementos dos factores segundo orientação do ISACA [121] acima apresentado e por tipo de função.

4.3 – A Amostra

Para a realização deste estudo a recolha de dados foi efectuada através de um questionário *on-line* (ver Anexo A), que esteve disponível entre 20 de Janeiro e 24 de Fevereiro de 2013.

O convite para a participação foi enviado por e-mail aos Conselhos de Administração das Entidades Gestoras de Água e/ou Saneamento de Sistemas Municipais e Plurimunicipais, à Entidade Reguladora – ERSAR, a três Associações (PPA, APDA e AMEGA) e a 6 empresas com actividade na prestação de serviços a este sector. Nesse convite, solicitava-se a participação dos gestores de topo da organização, bem como a divulgação do questionário pela organização no sentido de outros gestores e/ou funcionários também participarem.

No Anexo A encontram-se discriminados os endereços de e-mail utilizados para o envio do convite à participação, bem como o corpo do texto remetido. Na tabela seguinte (Tabela 4.5) apresenta-se a indicação da distribuição realizada.

	N.º de organizações a quem foram enviados questionários
Entidades Gestoras de Água e/ou Saneamento - Sistemas Municipais	
Região Norte	77
Região LVT	44
Região Centro	63
Região Alentejo	42
Região Algarve	15
Açores	13
Madeira	6
Entidades Gestoras de Água e/ou Saneamento - Sistemas Plurimunicipais	24
Associação Portuguesa de Distribuição e Drenagem de Água (APDA)	1
Entidade Reguladora dos Serviços de Água e Resíduos (ERSAR)	1
Parceria Portuguesa para a Água (PPA)	1
Associação de Municipios de Estudos e Gestão de Água (AMEGA)	1
Consultores (empresas) com actividade no Sector Água/Saneamento	6
Total	294
Repostas recebidas entre 20-01 e 25-2-2013	121
% de respostas recebidas versus Total de Organizações enviadas	41,16

Tabela 4.5-Lista de Organizações a quem foram enviados os Questionários

Porém, a percentagem acima apresentada (41,16%) não significa que foram recebidas respostas referentes a 41,16% das entidades, pois pode ter-se várias respostas relativas à mesma entidade, o que não foi possível verificar dado o anonimato existente para o respondente.

Caracterização da amostra face aos parâmetros

Começa-se, então, pela exposição da caracterização da amostra – 121 respostas recebidas no período de 20 de Janeiro a 25 de Fevereiro de 2013 e tratadas - face aos parâmetros recolhidos. No Anexo B encontra-se o detalhe desta caracterização.

Em relação à função que os respondentes exercem, verifica-se que a maior parcela corresponde à função "Trabalhador" (42,15%), sendo a menor relativa à função "Gestor / Funcionário de Segurança" (2,48%). Seguem-se, por ordem decrescente, as funções "Gestor Intermédio" (21,49%), "Gestor das TI" (14,05%), Consultor das TI (11,57%) e "Gestor de Topo" (8,26%). O gráfico seguinte (Gráfico 4.1) mostra o acima mencionado.

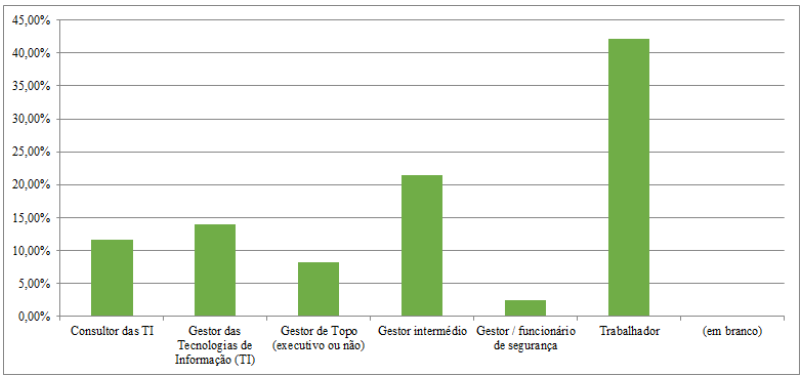


Gráfico 4.1- Caracterização da amostra face ao parâmetro: Distribuição por tipo de função

Relativamente à distribuição dos respondentes pela área de formação, verifica-se maior enfoque na área "Engenharia" (33,88%) e "Outra" (25,62%). As áreas "Informática / Ciências da Computação" e "Economia / Gestão" representam, respectivamente (20,66%) e (14,05%). As áreas "Direito" (4,96%) e a "Auditoria" (0,83%), conforme podemos visualizar no gráfico seguinte (Gráfico 4.2).

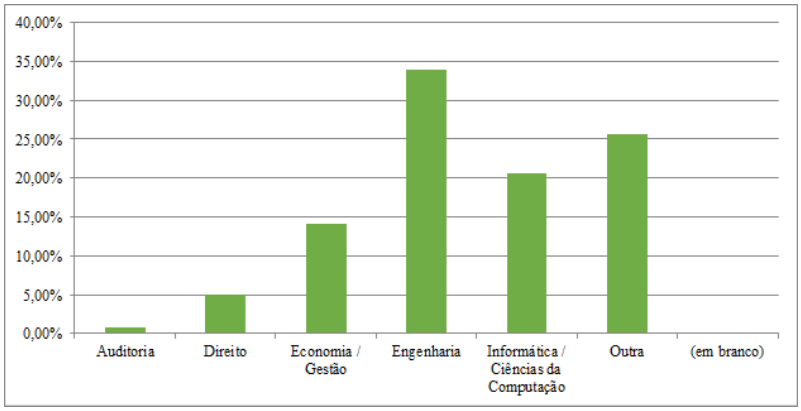


Gráfico 4.2- Caracterização da amostra face ao parâmetro: Distribuição por área de formação

Contudo, em relação ao "nível de formação" apresentado pelos respondentes poderemos verificar, no gráfico que se segue (Gráfico 4.3), que maioritariamente (76,03%) os respondentes apresentam um nível superior de formação, distribuído da seguinte forma: o nível "Bacharelato / Licenciatura" (42,15%) que é um valor bastante significativo face aos restantes, o nível "Especialização / Pós-graduação" (19,83%) e o nível "Mestrado" (14,05%). De referir ainda, que apenas (23,97%) da amostra apresenta formação de "Nível não superior".

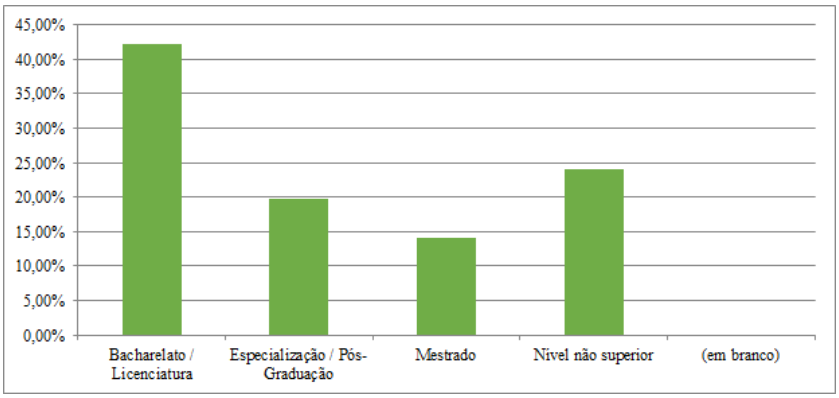


Gráfico 4.3- Caracterização da amostra face ao parâmetro: Distribuição por habilitações literárias

Com referência à distribuição por experiência profissional, o gráfico seguinte (Gráfico 4.4), mostra que maioritariamente, os respondentes apresentam "Entre 11 a 20 anos" de experiência profissional (36,36%). O grupo "Entre 21 e 30 anos" é o segundo mais populado (26,45%) seguido, por ordem decrescente, pelos grupos "Entre 6 e 10 anos" (15,70%) e "Mais de 30 anos" (13,22%). O grupo "Até 5 anos" (8,26%) é o menos populado.

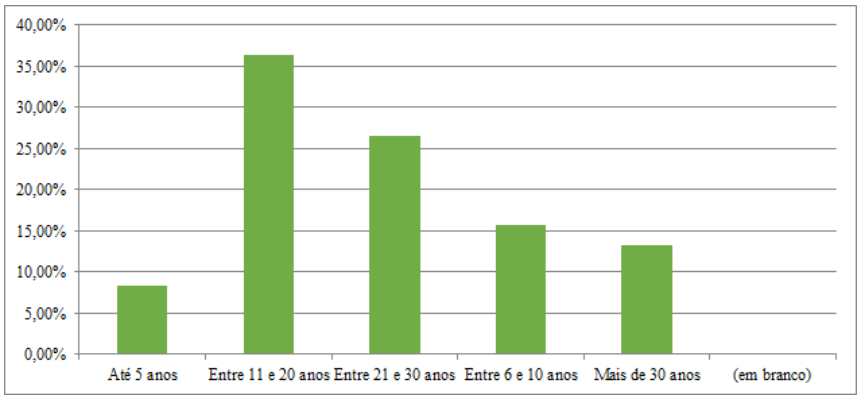


Gráfico 4.4- Caracterização da amostra face ao parâmetro: Distribuição por experiência profissional

Relativamente ao género, o gráfico seguinte (Gráfico 4.5) mostra-nos, que os respondentes são maioritariamente do sexo feminino (51,24%).

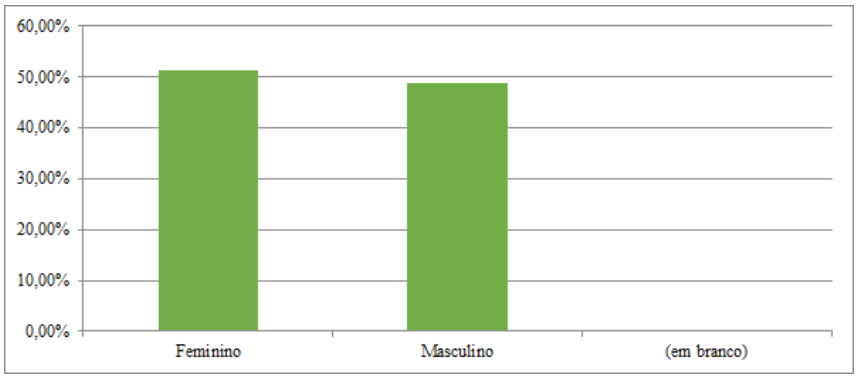


Gráfico 4.5- Caracterização da amostra face ao parâmetro: Distribuição por género

Em relação ao tipo de organização a que pertencem os respondentes, podemos visualizar no gráfico seguinte (Gráfico 4.6), que se destacam os organismos cujo número de trabalhadores se situam "Entre 501 a 1500 trabalhadores" (52,89%) e "Até 500 trabalhadores" (37,19%). O tipo de organização que apresenta "Entre 1501 a 2500 trabalhadores" é o terceiro grupo mais populado (7,44%), sendo que os outros dois grupos mostram valores residuais: "Entre 2501 e 3500 trabalhadores" (0,83%) e "Mais de 4500 trabalhadores" (1,65%).

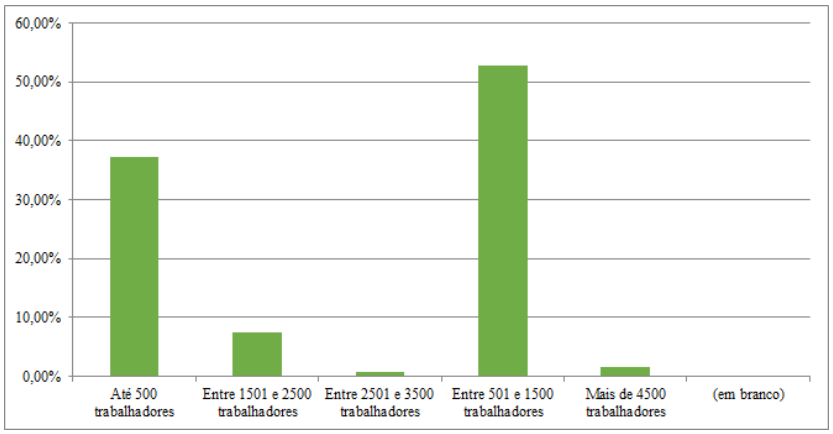


Gráfico 4.6- Caracterização da amostra face ao parâmetro: Distribuição por tipo de organização

Achou-se, ainda, interessante a caracterização da amostra tendo em conta o cruzamento da função com as outras variáveis de parâmetros, nomeadamente: área de formação, nível de formação, experiência profissional, tipo de organização, género e grupo etário. Os gráficos seguintes assinalam os valores percentuais encontrados.

Assim, pode verificar-se no gráfico seguinte (Gráfico 4.7) que as funções "Consultor das TI" e "Gestor das TI" são desempenhadas maioritariamente por trabalhadores com formação nas áreas "Engenharia" (CTI = 4,13%; GTI = 2,48%) e "Informática / Ciências da Computação" (CTI = 6,61%; GTI = 11,75%), sendo que a primeira função apresenta trabalhadores também formados na área "Economia / Gestão" (CTI = 0,83%).

A função “Gestor de Topo” apresenta uma maioria na área de formação “Engenharia” (5,79%) e valores residuais (0,83%) noutras áreas de formação.

A função “Gestor Intermédio” também apresenta uma maioria de representação na área de formação “Engenharia” (11,57%) e um valor significativo na área “Economia / Gestão” (5,79%), tendo as outras áreas menores valores (<=2,48%).

A função “Gestor / Funcionário de Segurança” mostra também maioria na área “Engenharia” (1,65%) e a função “Trabalhador” é a que apresenta maior diversidade de formação. No entanto, a maioria inclui-se no item “Outra” (21,49%). Porém, as áreas “Engenharia” e “Economia / Gestão” apresentam, respectivamente, os seguintes valores: (8,26%) e (6,61%).

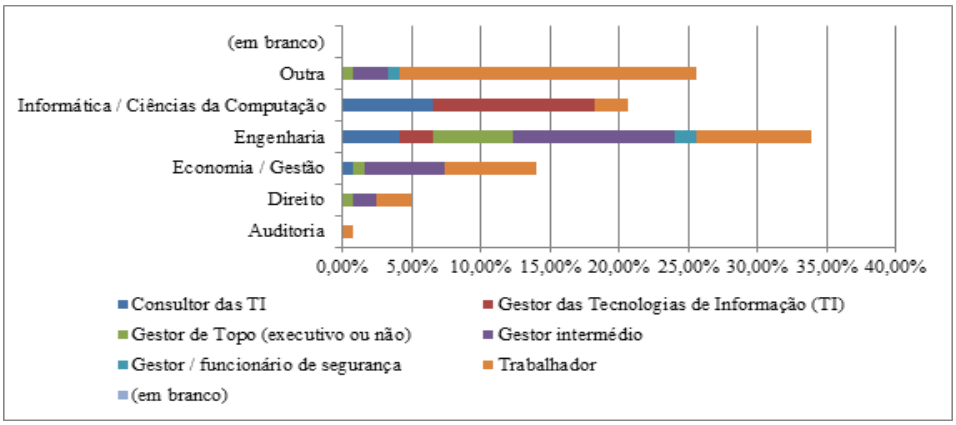


Gráfico 4.7- Caracterização da amostra face aos parâmetros: Tipo de função vs Área de formação

O cruzamento da variável “Função” com a variável “Nível de Formação” revela, no gráfico seguinte (Gráfico 4.8) que, maioritariamente, todas as funções são exercidas por recursos humanos com nível de formação qualificada, encontrando-se valores para o “Nível não superior” nas funções “Consultor das TI” (1,65%), “Gestor das Tecnologias de Informação” (4,13%) e “Trabalhador” (18,18%).

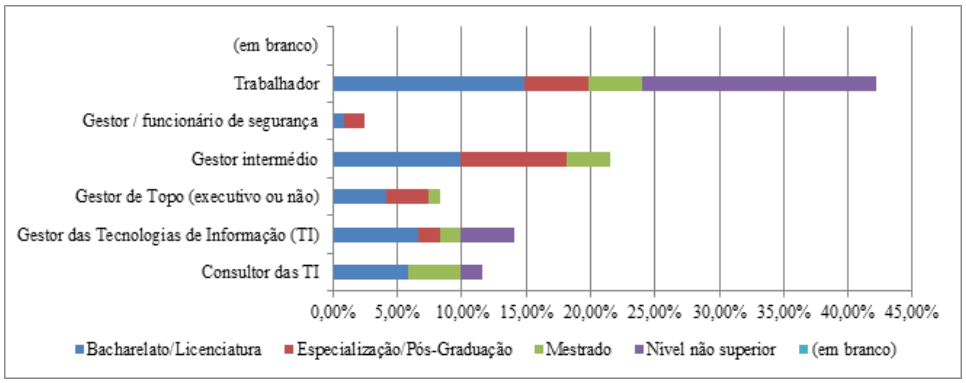


Gráfico 4.8-Caracterização da amostra face aos parâmetros: Tipo de função vs Habilitação literária

Através do gráfico seguinte (Gráfico 4.9) constata-se que na função "Consultor das TI" o grupo mais populado da variável "Experiência Profissional" é "Até 5 anos" (4,13%). Para a função "Gestor das TI" destaca-se o grupo "Entre 21 e 30 anos" (7,44%).

Para o "Gestor de Topo" existem dois grupos que obtêm o mesmo valor percentual (3,31%): "Entre 21 e 30 anos" e "Mais de 30 anos".

Nas funções "Gestor Intermédio" e "Trabalhador" o tempo de experiência profissional maioritário encontra-se no grupo "Entre 11 e 20 anos" obtendo, respectivamente, os valores (10,74%) e (16,53%).

Finalmente, para a função "Gestor / Funcionário da Segurança" surge o grupo maioritário "Entre 6 a 10 anos" (1,65%).

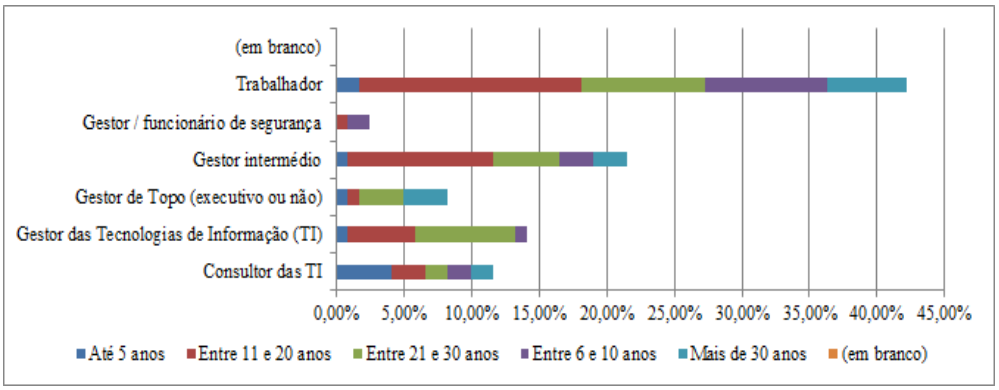


Gráfico 4.9- Caracterização da amostra face aos parâmetros: Tipo de função vs Experiência profissional

Pelo gráfico seguidamente apresentado (Gráfico 4.10) verifica-se que os respondentes da função "Consultor das TI" encontram-se representados em todos os tipos de organismo.

Para as funções "Gestor das TI" e "Gestor Intermédio" as respostas provêm de três tipos de organismos, a saber: "Até 500 trabalhadores", "Entre 501 e 1500 trabalhadores" e "Entre 1501 e 2500 trabalhadores".

Para as respostas referentes às funções "Gestor de Topo" e "Trabalhador" verifica-se a sua proveniência de dois tipos de organismos: "Até 500 trabalhadores" e "Entre 501 e 1500 trabalhadores".

Finalmente o grupo menos representativo "Gestor / Funcionário da Segurança" provêm apenas de um tipo de organismo: "Até 500 trabalhadores".

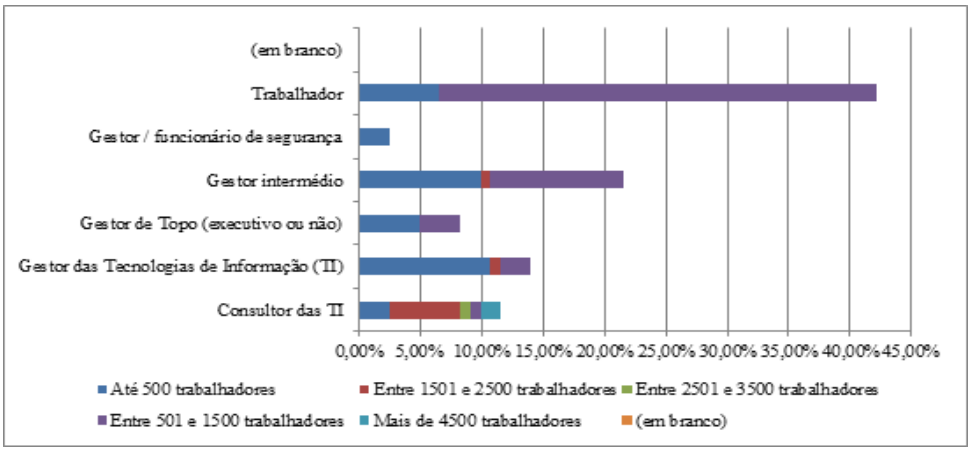


Gráfico 4.10 - Caracterização da amostra face aos parâmetros: Tipo de função vs Tipo organização

Finalmente, no gráfico (Gráfico 4.11) seguinte visualiza-se a distribuição da amostra por função, por grupo etário e por sexo.

Assim, constata-se que os respondentes, nas funções "Gestor de Topo" e "Gestor das TI" são maioritariamente do sexo masculino. A função "Gestor Intermédio" revela enfoque no grupo etário "Entre 36 e 45 anos". Já a função "Consultor das TI" mostra uma incidência masculina e no grupo etário "Entre 26 e 35 anos".

Contudo, a função "Gestor / Funcionário de Segurança" evidência uma incidência totalmente masculina. Porém, a função "Trabalhador" apresenta uma predominância no sexo feminino e no grupo etário "Entre 36 e 45 anos".

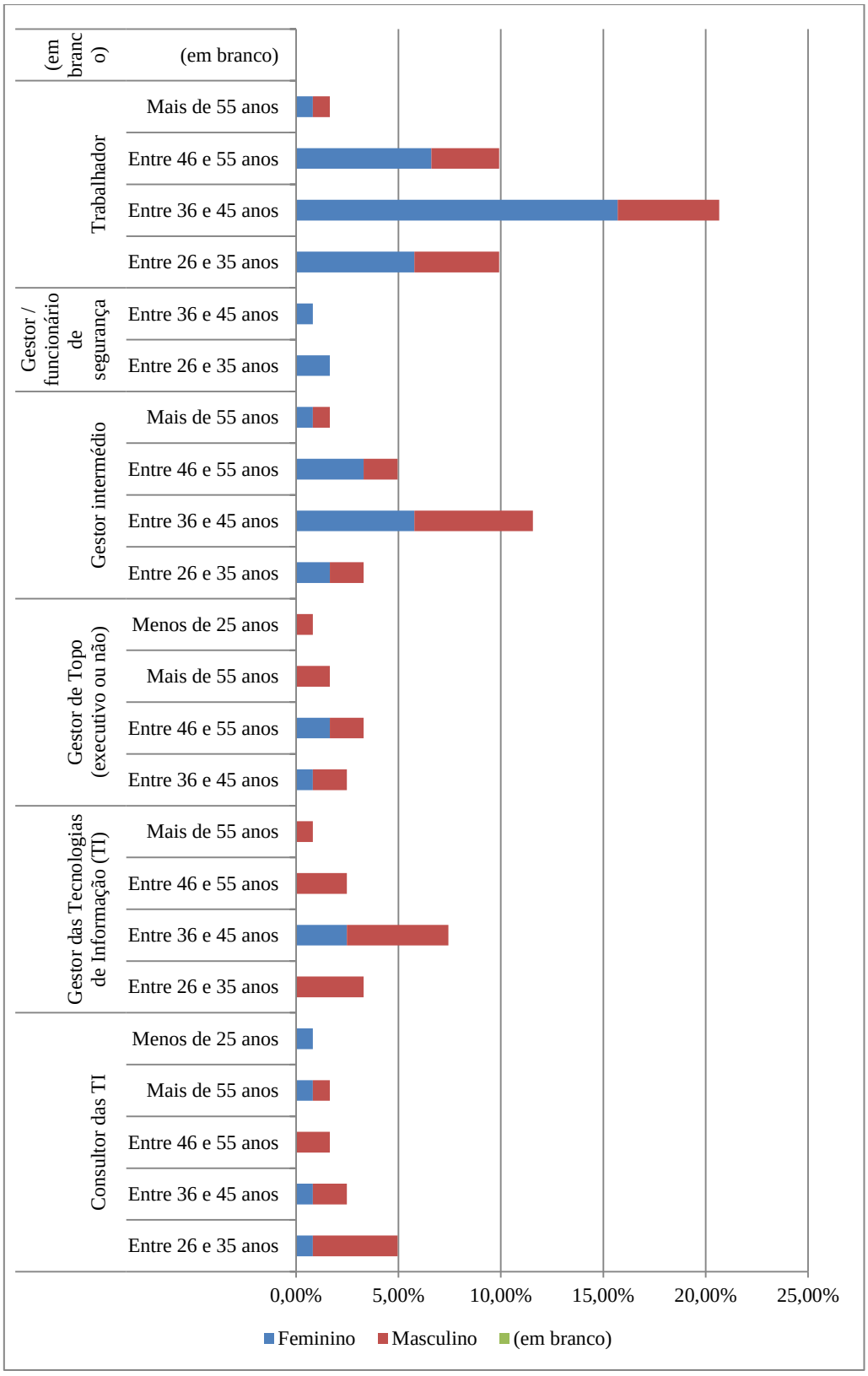


Gráfico 4.11- Caracterização da amostra face aos parâmetros: Tipo de função vs Grupo Etário vs Sexo

5. RESULTADOS OBTIDOS

Neste capítulo apresentam-se os principais resultados obtidos. Assim, primeiramente caracteriza-se a amostra tendo em conta as diferentes perspectivas expressas pelos respondentes, seguindo-se a análise comparativa entre as mesmas e, partindo-se dos valores dos níveis médios de importância encontrados para os elementos considerados na caracterização dos diferentes factores, prossegue-se para a análise resultante do mapeamento dos mesmos conforme orientação proposta pelo ISACA [122] e representada no ponto 4.2 deste documento. Na figura seguinte (Figura 5.1) encontra-se representado o raciocínio realizado para a análise e explanação daqueles.

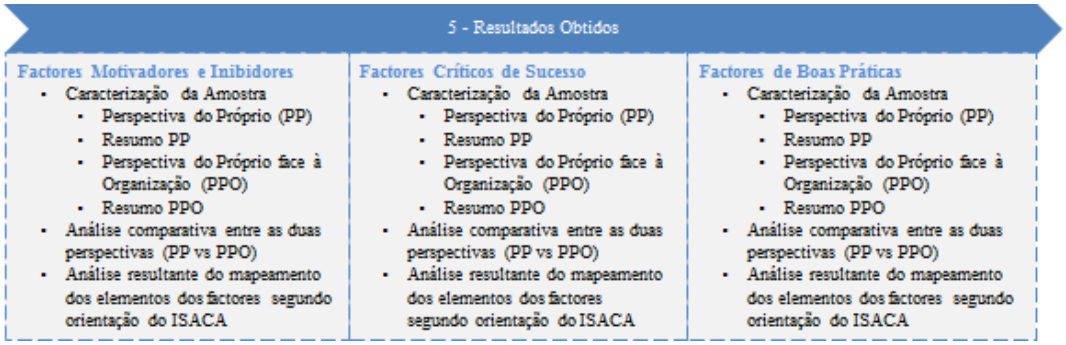


Figura 5.1 - Modelo dos Resultados Obtidos

Também no Anexo B podemos encontrar o tratamento mais detalhado dos dados, realizados em folhas de cálculo Excel.

5.1 - Factores Motivadores e Inibidores

5.1.1 - Caracterização da Amostra

Neste item expõem-se os resultados obtidos, recordando que foram expostos, aos respondentes, como Factores Motivadores para a adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização, os seguintes elementos:

a) Evitar perdas Financeiras

b) Ocorrência de Incidente Anterior

c) Garantir a disponibilidade, confidencialidade e integridade da informação

d) Planear a segurança antes da implementação de novas tecnologias

e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança

f) Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização

g) Emergência contínua de novos riscos

h) Alterações contínuas na legislação/regulação

i) Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)

e, como Factores Inibidores, os seguintes:

a) Valor do investimento

b) Falta de conhecimento

c) Cultura organizacional

d) Dificuldade em medir o custo/benefício

e) Acesso restrito à "Gestão de Topo"

f) Alterações contínuas na legislação/regulação

g) Emergência contínua de novos riscos

Assim, a análise de dados, para ambos os factores, teve em conta a classificação do grau de importância dada (percentagem) aos diferentes elementos, pelos respondentes, incluindo as duas perspectivas: a do próprio e a do próprio face à organização. De modo a aferir a existência ou não de desvios entre as duas vistas foi realizada a comparação entre as mesmas. Para tal, efectuou-se o cálculo do nível médio de importância para cada elemento destes factores.

5.1.2 - Perspectiva do Próprio

Neste sub-capítulo apontam-se os resultados obtidos para os Factores Motivadores e Inibidores referentes ao ponto de vista do próprio (Figura 5.2) e procedente, respectivamente, do tratamento dos dados efectuados às respostas obtidas à nona e à décima primeira questão do questionário elaborado (ver Anexo A).

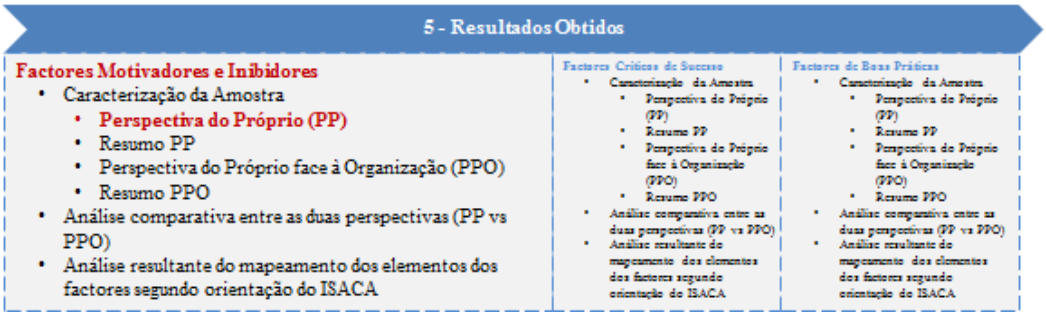


Figura 5.2- Modelo dos Resultados Obtidos: FM e FI / PP

Desta forma, numa primeira fase analisou-se a totalidade das respostas, verificando-se que, quer para os nove elementos dos Factores Motivadores, quer para os sete elementos dos Factores Inibidores acima identificados, os mesmos, de uma forma global, são classificados nas categorias "Muito importante" ou "Importante", com predominância das preferências nesta última categoria.

Contudo, os Factores Motivadores mais votados na categoria "Muito importante" na implementação/adopção dum Sistema de Gestão da Segurança da Informação (SGSI) são: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (80,17%), seguido do elemento "*Evitar perdas financeiras*" (62,81%). Os menos votados nesta categoria são: "*Alterações contínuas na legislação/regulação*" (23,97%), "*Ocorrência de Incidente Anterior*" (30,58%) e "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*" (32,23%).

Estes três últimos elementos são também os únicos apontados na categoria "Não é importante", respectivamente com as seguintes percentagens: (0,83%), (1,65%) e (0,83%).

Apesar disso, os dois primeiros elementos surgem com uma percentagem elevada na categoria "Importante": "*Alterações contínuas na legislação/regulação*" (59,50%) – sendo o elemento mais votado nesta categoria. O segundo elemento preferido é "*Ocorrência de Incidente Anterior*" (57,85%) e o elemento "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*" aparece na terceira posição (52,07%).

De salientar que o elemento "*Garantir a disponibilidade, confidencialidade e integridade da informação*" agrupa a totalidade (100,00%) das preferências, quando somados os valores percentuais nas categorias "Muito importante" e "Importante".

Na categoria "Pouco Importante", o elemento "*Alterações contínuas na legislação/regulação*" revela-se como o mais seleccionado pelos respondentes (15,70%).

Ainda, nesta categoria o segundo e terceiro elementos mais votados são, respectivamente: "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*"

(14,88%) e "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*" (10,74%).

No gráfico (Gráfico 5.1) seguinte pode encontrar-se o detalhe do atrás indicado.

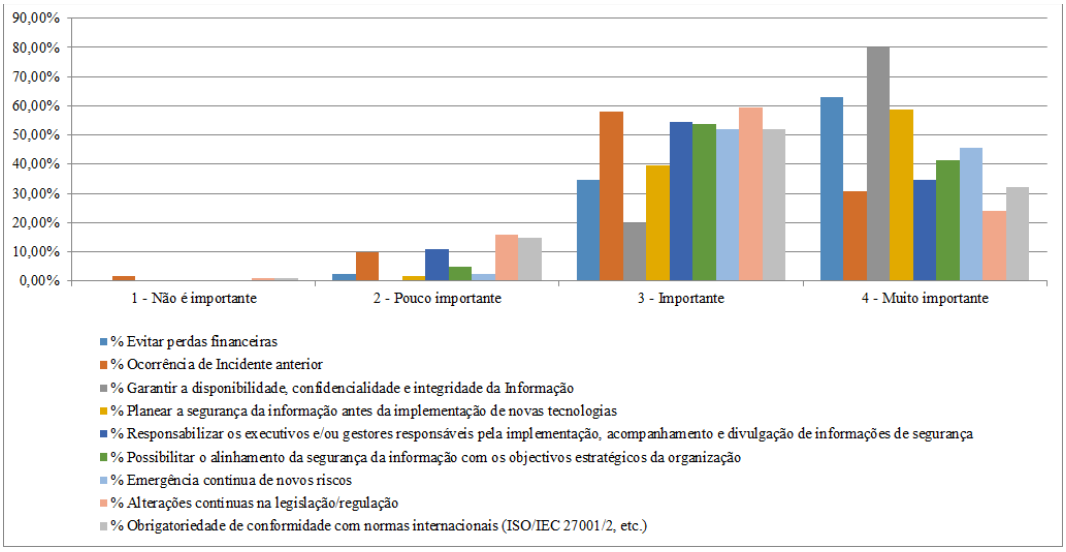


Gráfico 5.1 - Factores Motivadores - PP (Global)

Por outro lado, nos Factores Inibidores verifica-se que, na categoria "Importante", todos os elementos atingem valores percentuais cerca da metade ou superiores a esta (maiores que 45,00%), sendo os mais votados: "*Valor do investimento*" (62,81%) e "*Acesso restrito à gestão de topo*" (55,37%).

Porém, os Factores Inibidores mais seleccionados na categoria "Muito importante" na implementação/adopção dum Sistema de Gestão da Segurança da Informação (SGSI) são: "*Falta de conhecimento*" (44,63%) e a "*Cultura organizacional*" (43,80%).

Na categoria "Pouco Importante", o elemento "*Alterações contínuas na legislação/regulação*" também surge como o mais preferido pelos respondentes (31,40%). Nesta categoria o segundo e terceiro elemento mais escolhidos são, respectivamente: "*Acesso restrito à gestão de topo*" (24,79%) e "*Emergência contínua de novos riscos*" (23,14%).

Na categoria "Não é importante" são mencionados quatros dos sete elementos com valores percentuais pouco significativos (inferiores a 5,00%). No gráfico (Gráfico 5.2) seguinte pode encontrar-se detalhadamente o anteriormente indicado.

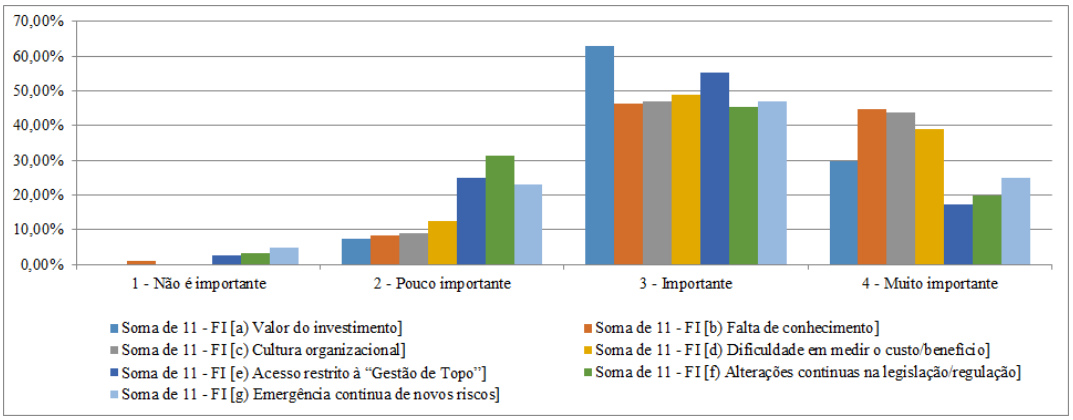


Gráfico 5.2- Factores Inibidores - PP (Global)

Numa segunda fase, analisou-se as respostas dos participantes tendo em conta a sua função, uma vez que, nelas, poder-se-ia encontrar mais algumas vistas para estes factores, isto é, que elementos são considerados como motivadores e/ou inibidores na implementação/adopção de um SGSI para um Gestor de Topo? E para um Gestor Intermédio? E para um Gestor das TI? E para um Consultor das TI? E para um Gestor / Funcionário da Segurança? E para um Trabalhador? Procurou-se e obteve-se os seguintes resultados.

Do ponto de vista do Gestor de Topo - conforme gráfico (Gráfico 5.3) seguinte, verifica-se que os três elementos mais votados como Factores Motivadores na categoria "Muito Importante" são: "*Evitar perdas financeiras*" (90,00%), "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (80,00%) e "*Planear a segurança da informação antes da implementação de novas tecnologias*" (70,00%).

Todos os elementos são considerados como Factores Motivadores e classificados com percentagens acima da metade percentual (50,00%), quando somados os valores nas categorias "Muito importante" ou "Importante", com excepção do elemento "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*", em que metade (50,00%) dos gestores de topo seleccionam as categorias "Não é importante" (10,00%) e "Pouco importante" (40,00%) e a restante pontuação (50,00%) surge nas categorias "Importante" (30,00%) e "Muito importante" (20,00%).

Na categoria "Importante", existem quatro elementos que atingem uma pontuação maioritária (60,00%), a saber: "*Ocorrência de incidente anterior*", "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*", "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" e "*Alterações contínuas na legislação/regulação*".

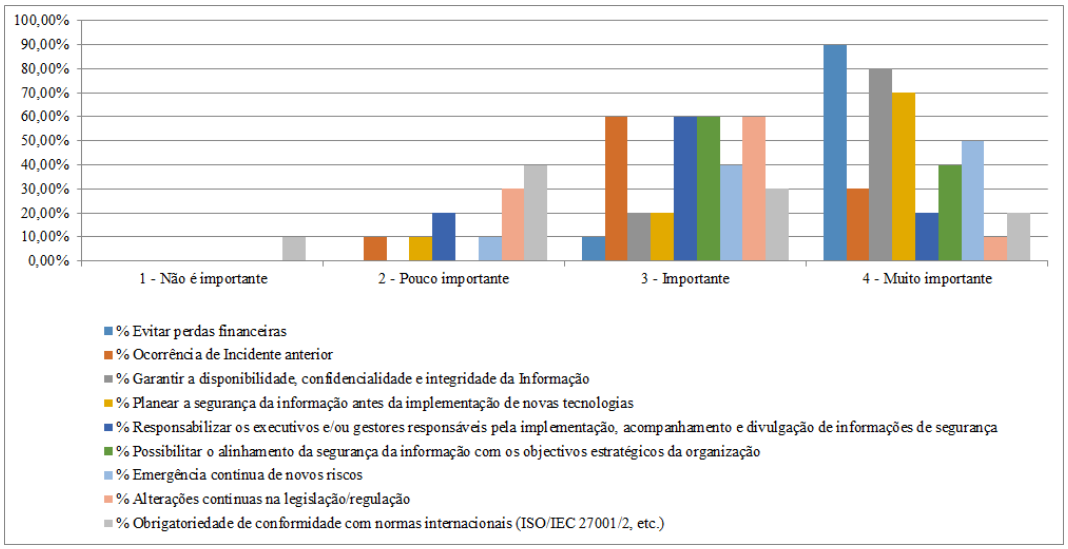


Gráfico 5.3 - Factores Motivadores - PP (Gestor de Topo)

Todavia, para o Gestor de Topo e conforme gráfico (Gráfico 5.4) seguinte, verifica-se que todos os elementos são considerados como Factores Inibidores e classificados com percentagens acima da metade percentual (50,00%) nas categorias "Muito importante" ou "Importante, situando-se o enfoque da votação na categoria "Importante".

Contudo, os elementos "*Valor do Investimento*", "*Falta de conhecimento*" e "*Dificuldade de medir o custo/benefício*" atingem a totalidade da votação (100,00%), quando somados os resultados percentuais nas categorias "Muito importante" e "Importante".

Por outro lado, os dois elementos mais votados como Factores Inibidores na categoria "Muito Importante" são: "*Valor do investimento*" e "*Emergência contínua de novos riscos*", ambos com a mesma pontuação (40,00%).

Para este grupo profissional nenhum dos elementos considerados é classificado na categoria "Não é importante", porém os elementos "*Cultura organizacional*" e "*Alterações contínuas na legislação/regulação*" são ambos apontados na categoria "Pouco importante" (40,00%).

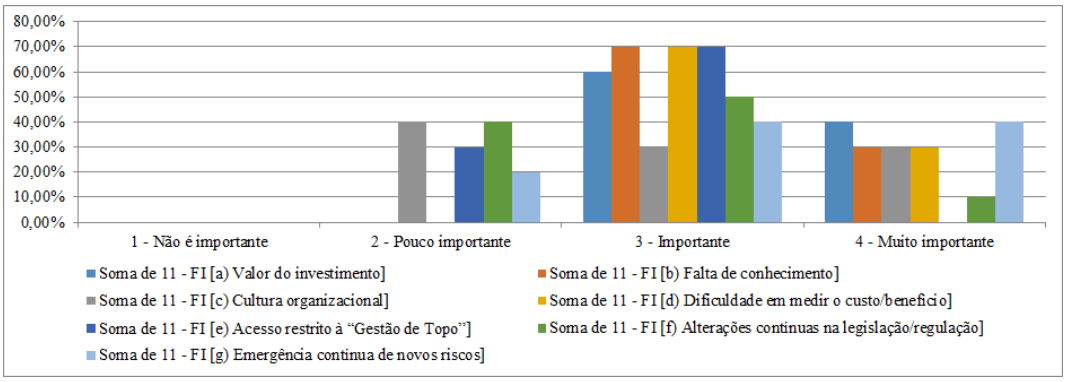


Gráfico 5.4- Factores Inibidores - PP (Gestor de Topo)

Do ponto de vista do Gestor Intermédio – para este gestor, conforme gráfico (Gráfico 5.5) abaixo, verifica-se que os três elementos mais votados como Factores Motivadores na categoria "Muito Importante" são: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (80,77%), "*Evitar perdas financeiras*" (69,23%) e "*Emergência contínua de novos riscos*" (57,69%), passando o elemento "*Planear a segurança da informação antes da implementação de novas tecnologias*" para o quarto lugar (57,69%).

No entanto, todos os elementos continuam a ser considerados como Factores Motivadores e classificados com percentagens acima da metade percentual (50,00%), quando somados os valores nas categorias "Muito importante" ou "Importante".

Mas, verifica-se que (11,54%) dos gestores intermédios consideram como "Pouco importante" o elemento motivador "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" e (7,69%) considera também "Pouco importante" o elemento motivador "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*".

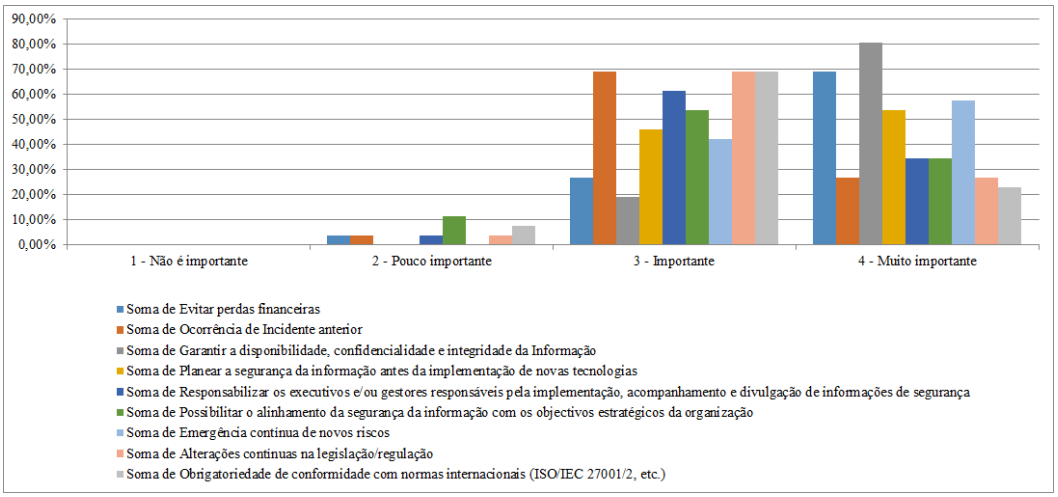


Gráfico 5.5- Factores Motivadores - PP (Gestor Intermédio)

Relativamente aos Factores Inibidores e conforme gráfico (Gráfico 5.6) abaixo, comprova-se que, para o gestor intermédio, existem dois elementos com metade da votação (50,00%) na categoria "Muito importante", que são: "*Falta de conhecimento*" e "*Dificuldade em medir o custo/benefício*". Em relação ao primeiro elemento inibidor "*Falta de conhecimento*" constata-se que a votação atinge a unanimidade (100,00%) no somatório dos valores indicados nas categorias "Muito importante" e "Importante".

Todavia, todos os elementos continuam a ser considerados como Factores Inibidores e classificados com percentagens significativas (acima dos 50,00%) nas categorias "Muito importante" ou "Importante", permanecendo o maior enfoque na categoria "Importante".

Verifica-se, ainda, que estes gestores consideram como "Pouco importante" o elemento inibidor "*Alterações contínuas na legislação/regulação*" (26,92%), bem como o elemento "*Acesso restrito à Gestão de Topo*", embora este apresente um valor mais reduzido (3,85%).

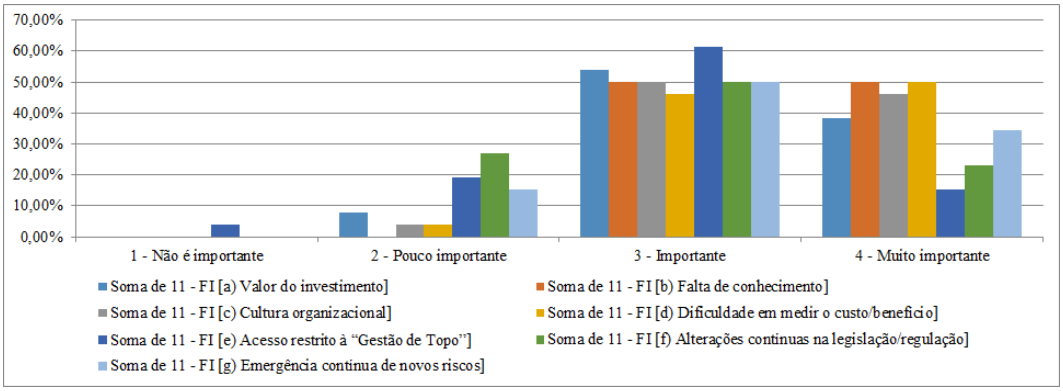


Gráfico 5.6- Factores Inibidores - PP (Gestor Intermédio)

Do ponto de vista do Gestor das TI – para este gestor e conforme gráfico (Gráfico 5.7) seguinte, constata-se que todos os elementos continuam a ser considerados como Factores Motivadores e

classificados com percentagens acima da metade percentual (50,00%), quando somados os valores nas categorias "Muito importante" e "Importante", notando-se que as preferências da votação recaem sobre a categoria "Importante".

De realçar que os elementos motivadores "*Evitar perdas financeiras*", "*Garantir a disponibilidade, confidencialidade e integridade da informação*" e "*Planear a segurança da informação antes da implementação de novas tecnologias*" agrupam a totalidade da votação (100,00%) das preferências no somatório dos valores apresentados nas categorias "Muito importante" e "Importante".

Contudo, os dois elementos motivadores mais populados na categoria "Muito importante" são, respectivamente: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (94,12%) e "*Planear a segurança da informação antes da implementação de novas tecnologias*" (64,71%). Em quarto lugar desta categoria surge o elemento "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" (52,94%).

Porém, o elemento motivador "*Evitar perdas financeiras*" (58,82%) revela-se classificado na terceira posição na categoria "Muito importante" e é o único elemento referido na categoria "Não é importante".

Os elementos motivadores "*Alterações contínuas na legislação/regulação*" (17,65%) e "*Emergência de novos riscos*" (11,75%) são assinalados pelos respondentes como "Pouco importante".

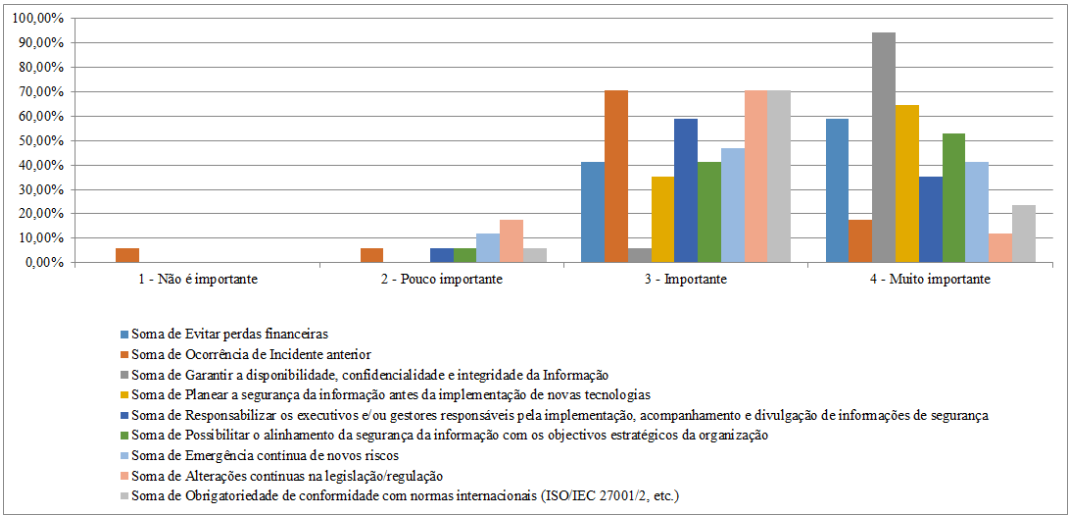


Gráfico 5.7- Factores Motivadores - PP (Gestor das TI)

Em relação aos Factores Inibidores, para o gestor das TI e conforme gráfico (Gráfico 5.8) a seguir, verifica-se que os elementos "*Dificuldade em medir o custo/benefício*" e "*Alterações contínuas na legislação/regulação*" são os mais votados (70,59%) e encontram-se classificados na categoria "Importante".

Também neste grupo profissional, os elementos considerados como Factores Inibidores revelam-se sempre maioritariamente populados nas categorias "Muito importante" ou "Importante", notando-se um enfoque na categoria "Importante".

Na categoria "Muito importante" o elemento inibidor mais populado é "*Cultura organizacional*" (41,18%). Já na categoria "Pouco Importante" encontram-se, com a mesma percentagem, os elementos inibidores "*Acesso restrito à gestão de topo*" e "*Alterações contínuas na legislação/regulação*" (29,41%), embora o elemento "*Emergência contínua de novos riscos*" (23,53%) seja o único elemento inibidor assinalado na categoria "Não é importante" com valor percentual pouco significativo (5,88%).

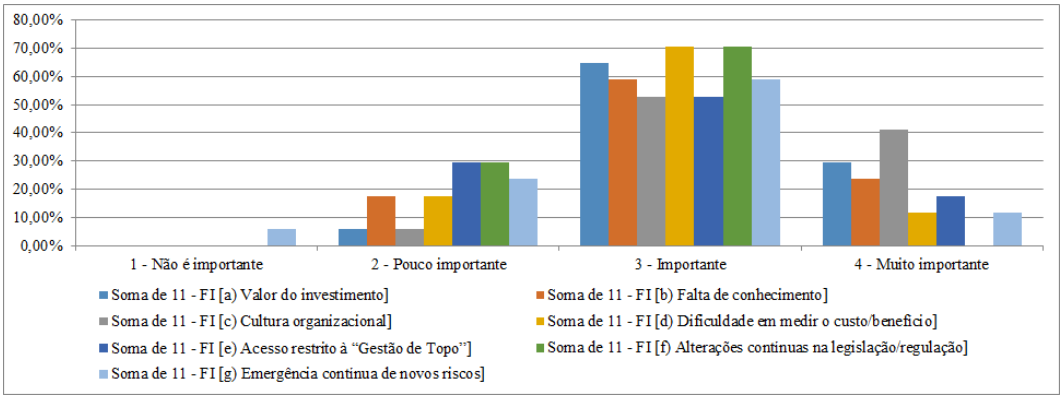


Gráfico 5.8- Factores Inibidores - PP (Gestor das TI)

Do ponto de vista do Consultor das TI – nesta perspectiva encontra-se algum paralelismo com a visão do Gestor Intermédio, pois na categoria "Muito importante" verifica-se que os dois elementos motivadores mais seleccionados (embora com menores valores percentuais) são os mesmos: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (71,43%) e "*Evitar perdas financeiras*" (57,14%). O terceiro elemento motivador mais votado difere, mas "*Planear a segurança da informação antes da implementação de novas tecnologias*" obtém quase metade das preferências (42,86%), sendo o escolhido pelo Consultor das TI, enquanto o Gestor Intermédio seleccionou na terceira posição da categoria "Muito importante" o elemento motivador "*Emergência contínua de novos riscos*" (57,69%). Ainda, na perspectiva do Consultor das TI, comprova-se que os elementos motivadores considerados apresentam valores percentuais maioritários (superiores a 50,00%), quando somados os valores

nas categorias “Importante” e “Muito importante”, notando-se uma predominância das preferências na categoria “Importante”.

Porém, o elemento motivador “*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*” é apontado como “Pouco importante” por mais de um quarto dos respondentes (28,57%). O gráfico (Gráfico 5.9) seguinte expõe o atrás referido.

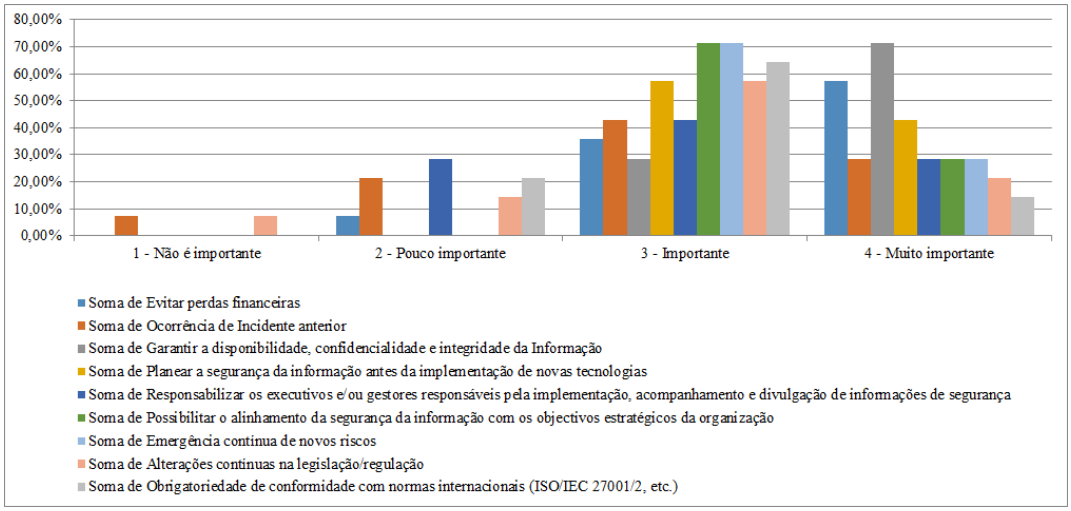


Gráfico 5.9- Factores Motivadores - PP (Consultor das TI)

Nesta visão do Consultor das TI e relativamente aos Factores Inibidores verifica-se que quatro dos sete elementos considerados agrupam, maioritariamente, as preferências de votação na categoria “Importante”, a saber: “*Valor do investimento*” (64,29%), “*Cultura organizacional*” (50,00%), “*Falta de conhecimento*” e “*Dificuldade em medir o custo/benefício*”, apresentando, estes últimos, a mesma percentagem (42,86%).

Em relação ao elemento inibidor “*Acesso restrito à gestão de topo*” verifica-se que a opinião está igualmente repartida pelas categorias “Muito importante” e “Importante” somando metade (50,00%), estando a restante parte (50,00%) atribuída às categorias “Pouco importante” e “Não é importante”.

Relativamente aos outros dois elementos inibidores “*Alterações contínuas na legislação/regulação*” e “*Emergência contínua de novos riscos*” verifica-se que os mesmos agrupam a votação maioritariamente nas categorias “Pouco importante” e “Não é importante” com, respectivamente, (42,86%; 14,29%) e (35,71%; 21,43%). O gráfico (Gráfico 5.10) seguinte apresenta o detalhe do acima mencionado.

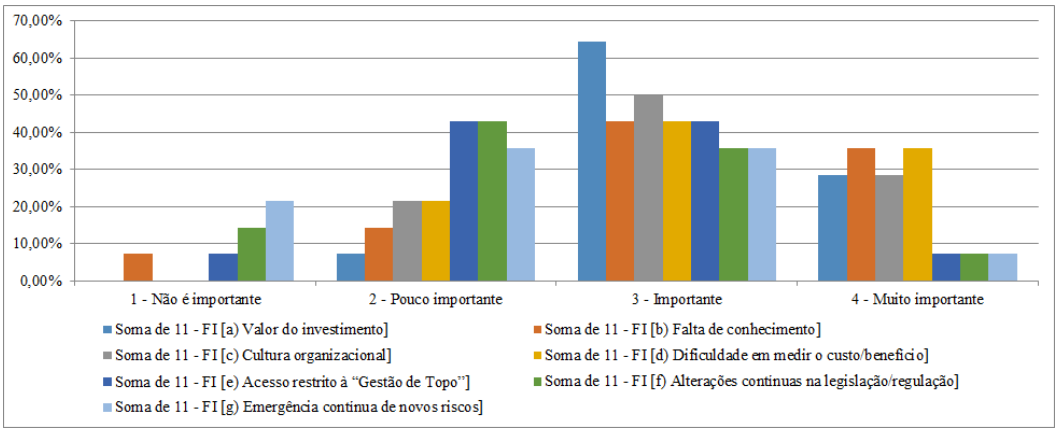


Gráfico 5.10- Factores Inibidores - PP (Consultor das TI)

Do ponto de vista do Gestor / Funcionário da Segurança – esta classe apresenta uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). Os elementos motivadores apresentam todos valores acima da metade percentual (50,00%) nas categorias "Importante" e "Muito importante", tendo o elemento "*Garantir a disponibilidade, confidencialidade e integridade da informação*" obtido a totalidade (100,00%) na categoria "Muito importante". Este grupo profissional aponta, ainda, como "Pouco importante" os elementos motivadores: "*Ocorrência de incidente anterior*" e "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*", ambos com a mesma pontuação (33,33%). No gráfico (Gráfico 5.11) seguinte visualiza-se o atrás referido.

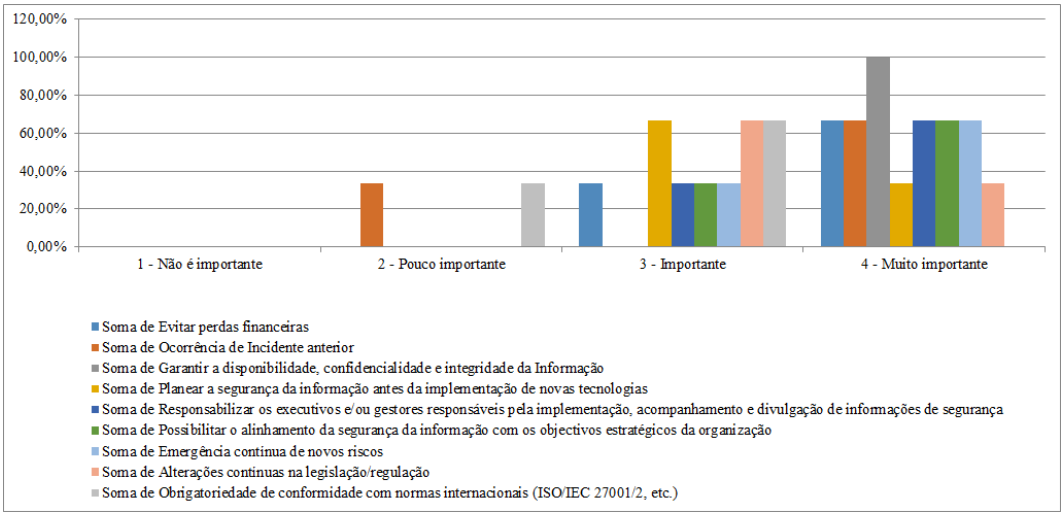


Gráfico 5.11- Factores Motivadores - PP (Gestor/Funcionário da Segurança)

Relativamente aos elementos representativos dos Factores Inibidores verifica-se, em todos eles, valores acima da metade percentual (50,00%), quando somados nas categorias "Muito importante" e "Importante", com prevalência nesta última.

O elemento inibidor "*Falta de conhecimento*" obtém a totalidade da votação (100,00%) na categoria "Importante".

Este grupo profissional aponta, ainda, como "Pouco importante" os elementos inibidores: "*Valor do investimento*", "*Cultura organizacional*" e "*Alterações contínuas na legislação/regulação*", todos com pontuação idêntica (33,33%). O gráfico (Gráfico 5.12) seguinte exibe o atrás exposto.

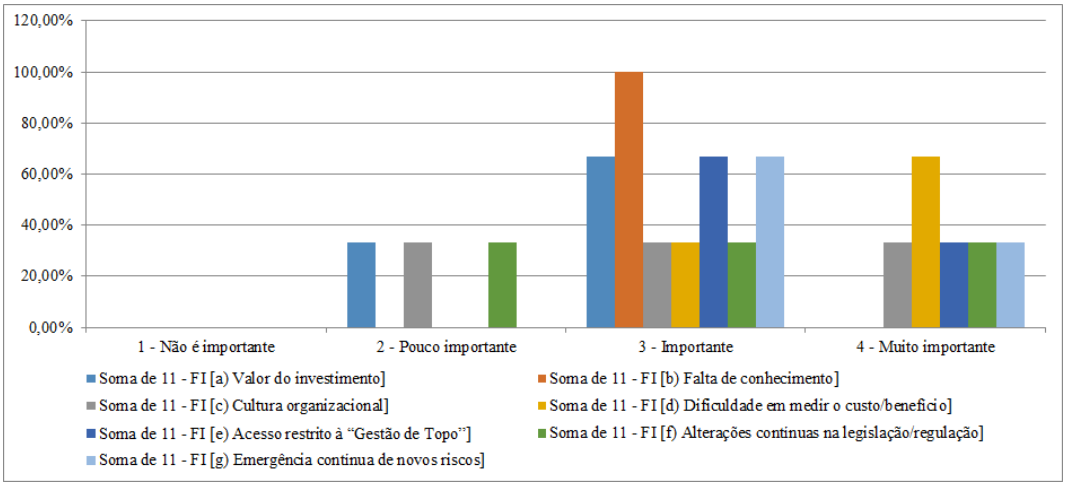


Gráfico 5.12- Factores Inibidores - PP (Gestor/Funcionário da Segurança)

Do ponto de vista do Trabalhador – também nesta perspectiva, todos os elementos considerados como Factores Motivadores apresentam valores acima da metade percentual (50,00%), quando somados os valores nas categorias "Muito importante" e "Importante", havendo preferência pela votação na última categoria. O elemento motivador mais seleccionado nesta categoria é "*Emergência contínua de novos riscos*" que junta um valor maioritário (56,86%) da votação dos respondentes.

Contudo, os três primeiros elementos motivadores preferidos pelos respondentes na categoria "Muito importante" são: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (76,47%), "*Planear a segurança da informação antes da implementação de novas tecnologias*" (62,75%) e "*Evitar perdas financeiras*" (56,86%).

O elemento motivador "*Alterações contínuas na legislação/regulação*" obtém a maior pontuação (19,61%) na categoria "Pouco importante", e o elemento "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*" alcança (13,73%) dos votos dos respondentes nesta categoria. Nenhum elemento é apontado na categoria "Não é importante". No gráfico (Gráfico 5.13) seguinte mostra-se o atrás referido.

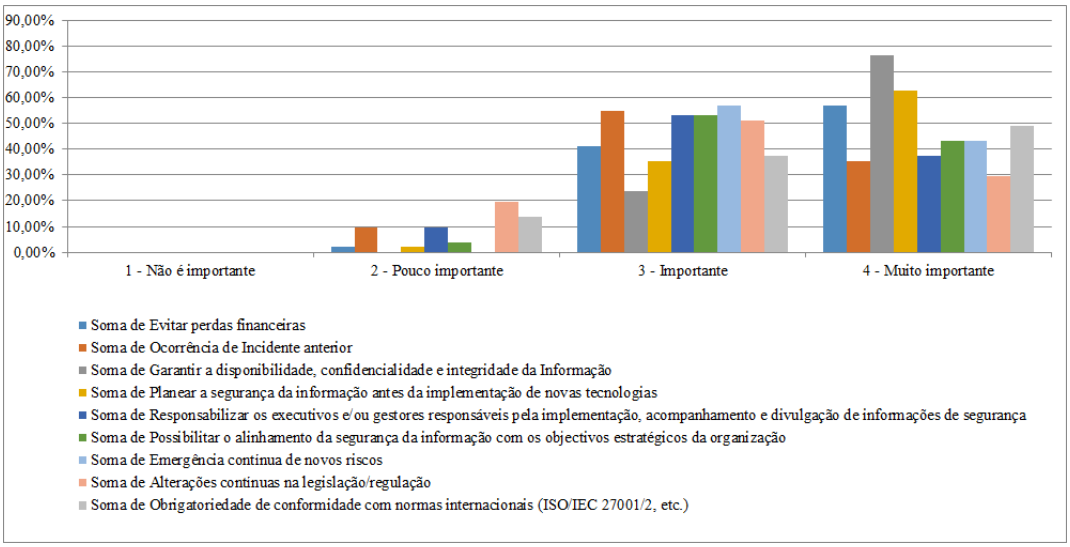


Gráfico 5.13- Factores Motivadores - PP (Trabalhador)

Ainda nesta perspectiva, todos os elementos considerados como Factores Inibidores apresentam também valores percentuais significativos (acima dos 50,00%), quando somados nas categorias "Importante" e "Muito importante".

O elemento inibidor mais votado na categoria "Importante" é "*Valor do investimento*" (66,67%), seguido do elemento "*Acesso restrito à Gestão de Topo*" (52,94%).

Por outro lado, na categoria "Muito importante" vence o elemento inibidor "*Falta de conhecimento*" (56,86%), seguido do elemento "*Cultura organizacional*" (50,98%).

Relativamente à categoria "Pouco importante" o elemento inibidor que agrupa maior pontuação é "*Alterações contínuas na legislação/regulação*" (29,41%), sendo seguido do elemento "*Emergência contínua de novos riscos*" (25,49%).

Na categoria "Não é importante" os elementos inibidores "*Acesso restrito à Gestão de Topo*", "*Alterações contínuas na legislação/regulação*" e "*Emergência contínua de novos riscos*" aparecem todos populados de forma pouco significativa (valores inferiores a 5,00%). O gráfico (Gráfico 5.14) seguinte revela o acima mencionado.

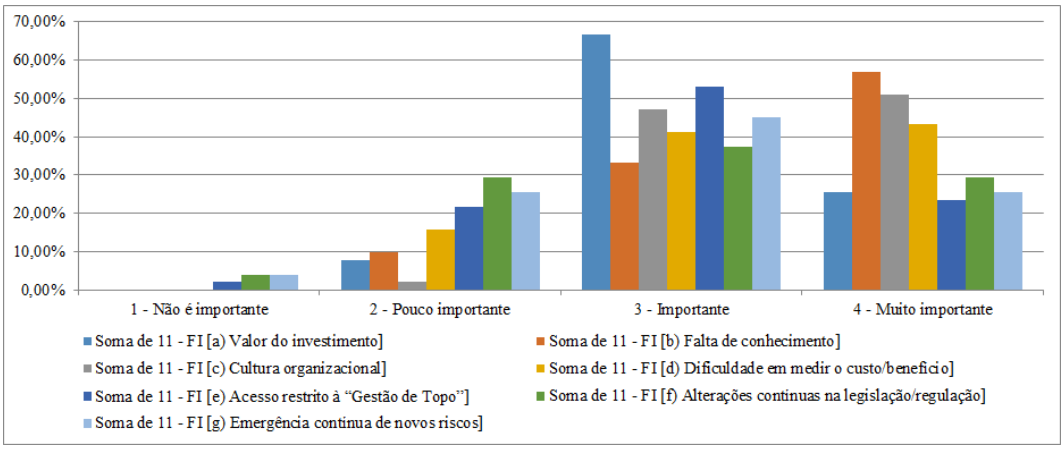


Gráfico 5.14- Factores Inibidores - PP (Trabalhador)

5.1.3 – Resumo da Perspectiva do Próprio

De seguida e conforme modelo mostrado na figura abaixo (Figura 5.3) decorre a compilação dos resultados obtidos, na perspectiva do próprio para os Factores Motivadores e Inibidores.

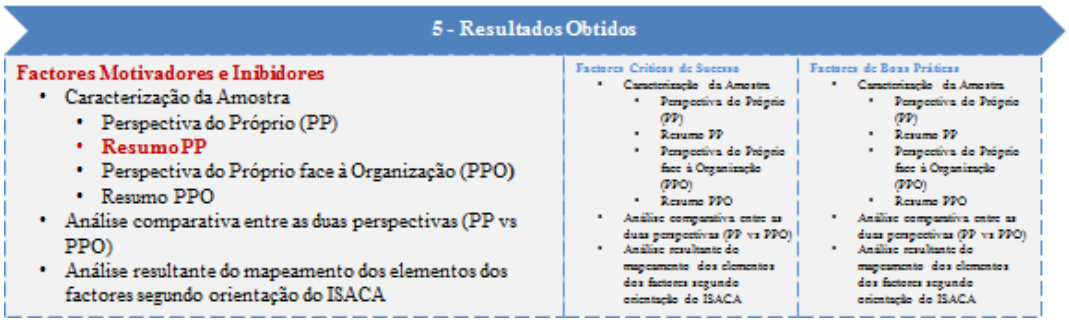


Figura 5.3- Modelo dos Resultados Obtidos: FM e FI / Resumo da PP

Em síntese, nas tabelas seguintes (Tabela 5.1 e Tabela 5.2), apresentam-se as ordenações pelas categorias "Muito importante" e "Não é importante" dos elementos considerados para o estudo como Factores Motivadores e Inibidores, segundo cada uma das vistas dadas pela função do respondente.

Assim, conforme se pode observar na tabela a seguir (Tabela 5.1) o elemento motivador "*Garantir a disponibilidade, confidencialidade e integridade da Informação*" é o mais referido em primeiro lugar na categoria "Muito importante". Só o Gestor de Topo é que o coloca em segundo lugar dando preferência ao elemento "*Evitar perdas financeiras*".

O elemento motivador "*Planear a segurança da informação antes da implementação de novas tecnologias*" é classificado em segundo lugar pelos "Gestor das TI" e "Trabalhador"; em terceiro pelos "Gestor de Topo", "Consultor das TI" e "Gestor/Funcionário da Segurança" e em quarto lugar pelo "Gestor intermédio".

Constata-se, ainda, que na categoria "Não é importante" são apontados os elementos motivadores "*Ocorrência de Incidente anterior*", "*Alterações contínuas na legislação/regulação*" e "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*".

Factores Motivadores - PP (- Elemento não é referido pelos respondentes)		09 - FM [a] Evitar perdas financeiras]	09 - FM [b] Ocorrência de Incidente anterior]	09 - FM [c] Garantir a disponibilidade, confidencialidade e integridade da Informação]	09 - FM [d] Planear a segurança da informação antes da implementação de novas tecnologias]	09 - FM [e] Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança]	09 - FM [f] Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização]	09 - FM [g] Emergência contínua de novos riscos]	09 - FM [h] Alterações contínuas na legislação/regulação]	09 - FM [i] Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)]
Gestor de Topo	Muito importante	1	6	2	3	7	5	4	8	7
	Não é importante	-	-	-	-	-	-	-	-	1
Gestor Intermédio	Muito importante	2	6	1	4	5	5	3	6	7
	Não é importante	-	-	-	-	-	-	-	-	-
Gestor das TI	Muito importante	3	8	1	2	6	4	5	9	7
	Não é importante	-	1	-	-	-	-	-	-	-
Consultor das TI	Muito importante	2	4	1	3	4	4	4	5	6
	Não é importante	-	1	-	-	-	-	-	1	-
Gestor / Funcionário da Segurança	Muito importante	2	2	1	3	2	2	2	3	-
	Não é importante	-	-	-	-	-	-	-	-	-
Trabalhador	Muito importante	3	7	1	2	6	5	5	8	4
	Não é importante	-	-	-	-	-	-	-	-	-
Global	**Muito importante**	**2**	**8**	**1**	**3**	**6**	**5**	**4**	**9**	**7**
	Não é importante	**-**	**1**	**-**	**-**	**-**	**-**	**-**	**2**	**2**

Tabela 5.1- Factores Motivadores - PP: Ordenação das preferências

Por outro lado, visualiza-se na tabela seguinte (Tabela 5.2) que o elemento inibidor "*Falta de conhecimento*" é o mais referido em primeiro lugar na categoria "Muito importante". O Gestor de Topo coloca-o em segundo lugar, dando preferência ao elemento inibidor "*Valor do investimento*".

Por outro lado, o Gestor das TI vota nesse elemento, em terceiro lugar, dando a sua preferência ao elemento "*Cultura organizacional*", o qual revela-se como o segundo elemento inibidor mais votado.

Verifica-se, ainda, que na categoria "Não é importante" são apontados três dos sete elementos: "*Emergência contínua de novos riscos*", "*Alterações contínuas na legislação/reg*ulação" e "*Acesso restrito à Gestão de Topo*".

Factores Inibidores - PP (- Elemento não é referido pelos respondentes)		11 - FI [a) Valor do investimento]	11 - FI [b) Falta de conhecimento]	11 - FI [c) Cultura organizacional]	11 - FI [d) Dificuldade em medir o custo/benefício]	11 - FI [e) Acesso restrito à "Gestão de Topo"]	11 - FI [f) Alterações contínuas na legislação/regulação]	11 - FI [g) Emergência contínua de novos riscos]
Gestor de Topo	Muito importante	1	2	2	2	-	3	1
	Não é importante	-	-	-	-	-	-	-
Gestor Intermédio	Muito importante	3	1	2	1	6	5	4
	Não é importante	-	-	-	-	1	-	-
Gestor das TI	Muito importante	2	3	1	5	4	-	5
	Não é importante	-	-	-	-	-	-	1
Consultor das TI	Muito importante	2	1	2	1	3	3	3
	Não é importante	-	3	-	-	3	2	1
Gestor / Funcionário da Segurança	Muito importante	-	-	2	1	2	2	2
	Não é importante	-	-	-	-	-	-	-
Trabalhador	Muito importante	5	1	2	3	6	4	5
	Não é importante	-	-	-	-	2	1	1
Global	**Muito importante**	**4**	**1**	**2**	**3**	**7**	**6**	**5**
	Não é importante	**-**	**-**	**-**	**-**	**3**	**2**	**1**

Tabela 5.2- Factores Inibidores - PP: Ordenação das preferências

5.1.4 – Perspectiva do Próprio face à Organização

Neste ponto, ao analisar os dados procurou-se saber quais os Factores Motivadores e Inibidores para a adopção/implementação dum Sistema de Gestão da Segurança da Informação que são considerados, mais ou menos importantes, pelas organizações do sector das Águas e Saneamento em Portugal, através das opiniões que os respondentes apontaram como sendo o seu ponto de vista no seu sector de actividade / organização. Assim, seguindo o raciocínio do modelo mostrado na figura abaixo (Figura 5.4) os resultados desta perspectiva resultam do tratamento dos dados efectuados às respostas obtidas à décima e à décima segunda questão do questionário elaborado (ver Anexo A).

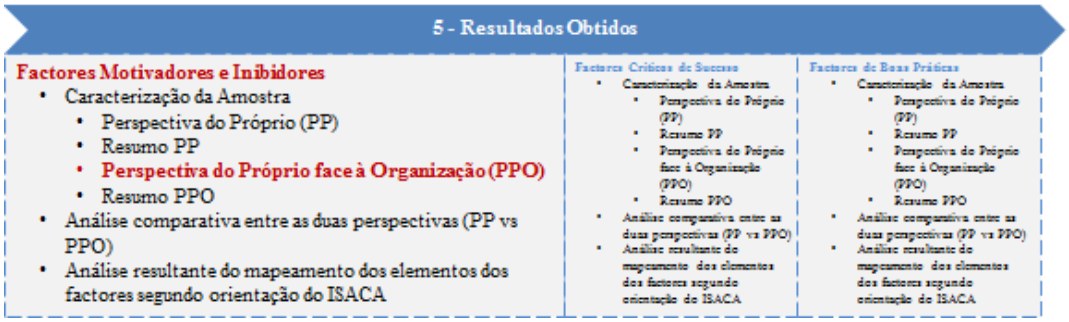


Figura 5.4- Modelo dos Resultados Obtidos: FM e FI / PPO

Como anteriormente já efectuado para a perspectiva do próprio, também nesta, começou por se considerar primeiramente, uma visão global das respostas para cada elemento dos Factores Motivadores e Inibidores e, de seguida, realizar-se o estudo segundo as vistas dos respondentes consoante a sua função.

Assim, de acordo com a perspectiva dos respondentes face à organização, os elementos indicados como Factores Motivadores e Inibidores são também globalmente classificados nas categorias "Muito importante" e "Importante".

Contudo, os Factores Motivadores mais votados na categoria "Muito importante" na implementação/adopção dum SGSI são os seguintes: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (73,55%), seguido do elemento "*Evitar perdas financeiras*" (57,02%). Os menos votados nesta categoria são: "*Alterações contínuas na legislação/regulação*" (29,75%) e "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*" (32,23%).

Na categoria "Importante" os elementos motivadores "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" e "*Alterações contínuas na legislação/regulação*" são os mais preferidos e agrupam a mesma pontuação (54,55%).

Porém, as categorias "Não é importante" ou "Pouco importante" encontram-se mais populadas do que quando é analisada a perspectiva do próprio.

Na categoria "Pouco Importante", o elemento motivador "*Alterações contínuas na legislação/regulação*" é o mais seleccionado pelos respondentes (14,05%). Nesta categoria, o segundo e terceiro elementos mais votados são, respectivamente: "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*" (12,40%) e "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*" (10,74%). No gráfico (Gráfico 5.15) seguinte encontra-se detalhadamente o anteriormente indicado.

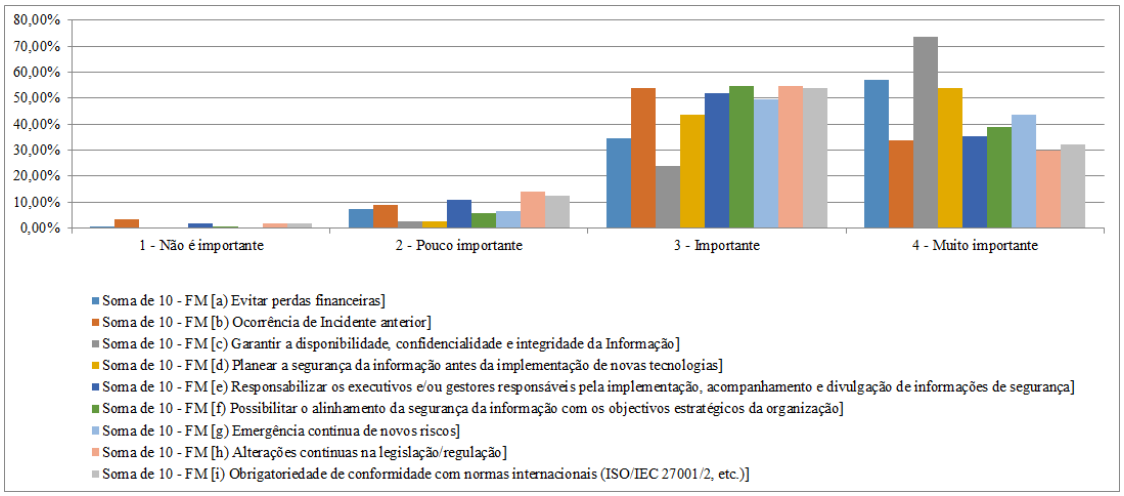


Gráfico 5.15- Factores Motivadores - PPO (Global)

Por outro lado, nos Factores Inibidores e, na categoria "Importante" todos os elementos atingem valores perto da metade percentual (superiores a 45,00%), sendo os mais votados: "*Acesso restrito à Gestão de Topo*" e "*Emergência contínua de novos riscos*", ambos com pontuação idêntica (51,24%).

Todavia, os Factores Inibidores mais seleccionados na categoria "Muito importante" na implementação/adopção dum SGSI são: "*Valor do investimento*" (42,98%) e "*Falta de conhecimento*" (39,67%).

Na categoria "Pouco Importante", o elemento inibidor "*Alterações contínuas na legislação/regulação*" surge como o mais escolhido pelos respondentes (28,93%). Nesta categoria, o segundo e terceiro elementos mais votados são, respectivamente: "*Acesso restrito à Gestão de Topo*" (25,62%) e "*Emergência contínua de novos riscos*" (21,49%).

Na categoria "Não é importante" são mencionados cinco dos sete elementos inibidores com valores percentuais pouco significativos (inferiores a 5,00%). No gráfico (Gráfico 5.16) seguinte encontra-se o pormenor do anteriormente indicado.

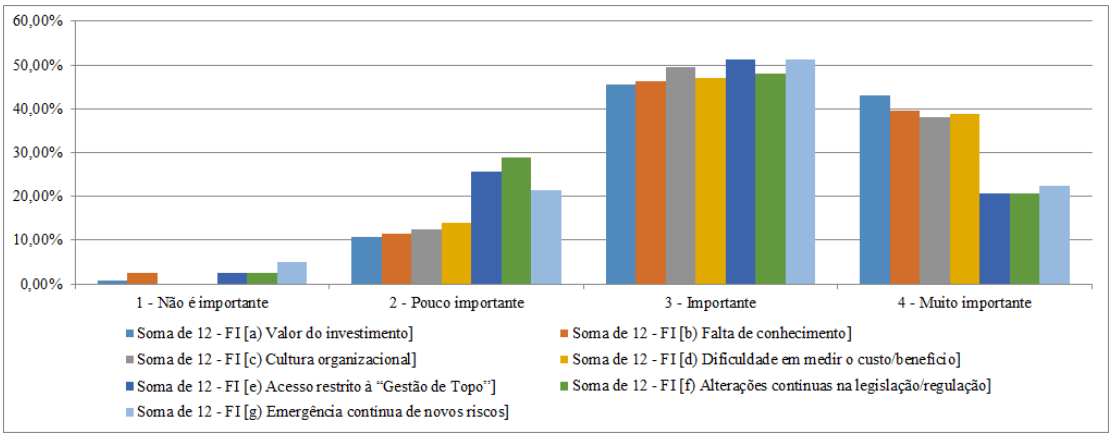


Gráfico 5.16- Factores Inibidores - PPO (Global)

Seguidamente, examinou-se os resultados obtidos desta PPO, tendo em conta a função do respondente na mesma, de modo a descobrir os elementos mais ou menos motivadores e inibidores na implementação/adopção de um SGSI para os Gestor de Topo, Gestor Intermédio, Gestor das TI, Consultor das TI, Gestor / Funcionário da Segurança e Trabalhador. Procurou-se e obteve-se os seguintes resultados.

Do ponto de vista do Gestor de Topo - conforme gráfico (Gráfico 5.17) a seguir, verifica-se que há dois elementos como Factores Motivadores em igualdade de votação (80,00%) na categoria "Muito Importante" e que são: "*Evitar perdas financeiras*" e "*Garantir a disponibilidade, confidencialidade e integridade da informação*". De seguida surge "*Planear a segurança da informação antes da implementação de novas tecnologias*" (70,00%).

Porém, todos os elementos são considerados como Factores Motivadores e classificados com percentagens significativas (acima dos 50,00%), quando somados os valores nas categorias "Muito importante" ou "Importante".

De realçar que o elemento motivador "*Garantir a disponibilidade, confidencialidade e integridade da informação*" atinge a unanimidade (100,00%) no somatório dos valores obtidos nestas duas categorias.

Os elementos motivadores "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*" e "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" revelam-se igualmente votados na categoria "Não é importante" (10,00%).

Os três elementos motivadores mais seleccionados na categoria "Pouco importante" são: "*Emergência contínua de novos riscos*", "*Alterações contínuas da legislação/regulação*" e "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*", mostrando-se todos igualmente pontuados (10,00%).

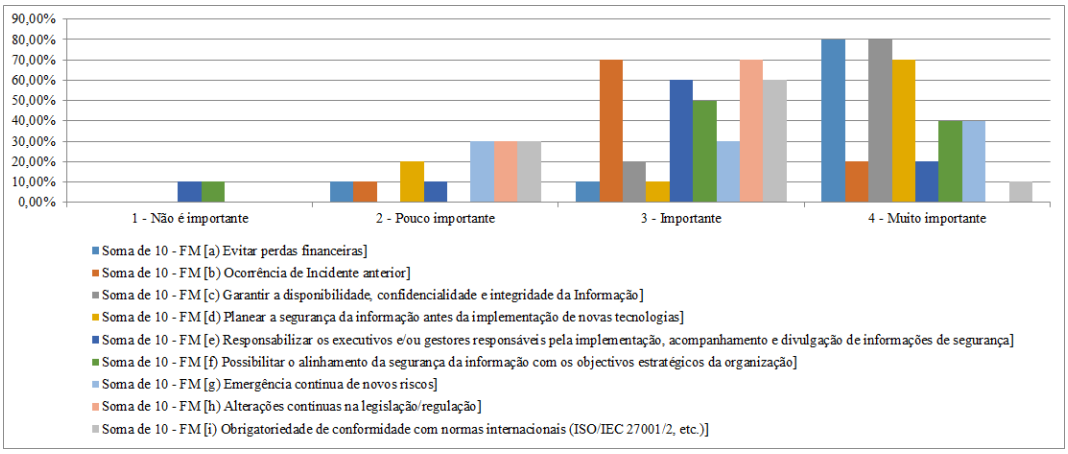


Gráfico 5.17- Factores Motivadores - PPO (Gestor de Topo)

Por outro lado, e conforme gráfico (Gráfico 5.18) abaixo, constata-se que todos os elementos são considerados como Factores Inibidores e classificados com percentagens significativas (acima dos 50,00%), quando somados os valores nas categorias "Muito importante" ou "Importante, situando-se o enfoque da votação na categoria "Importante".

Todavia, os elementos inibidores "*Valor do Investimento*", "*Falta de conhecimento*" atingem uma votação bastante significativa (90,00%) e os elementos "*Cultura organizacional*" e "*Dificuldade de medir o custo/benefício*" reúnem, também, uma votação maioritária (80,00%), quando somados os resultados percentuais nas categorias "Muito importante" e "Importante".

Porém, os dois elementos mais votados como Factores Inibidores na categoria "Muito Importante" são: "*Valor do investimento*" (70,00%) e "*Emergência contínua de novos riscos*" (40,00%).

Também para este grupo profissional – Gestor de Topo, o único elemento inibidor classificado na categoria "Não é importante" é "*Falta de conhecimento*" (10,00%). Todavia, o elemento "*Alterações contínuas na legislação/regulação*" realça-se na categoria "Pouco importante" (40,00%).

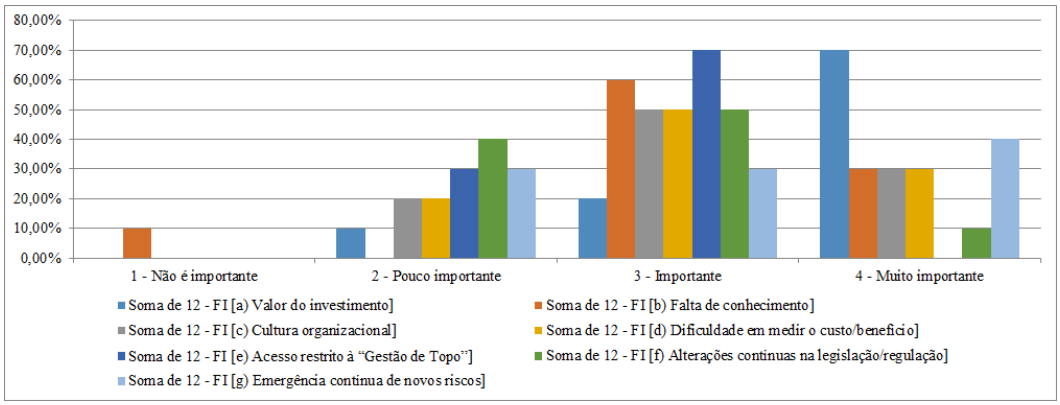


Gráfico 5.18- Factores Inibidores - PPO (Gestor de Topo)

Do ponto de vista do Gestor Intermédio – nesta perspectiva e conforme gráfico (Gráfico 5.19) abaixo, este gestor, distribui a sua votação pelas três categorias "Muito importante", "Importante" e "Pouco importante", não seleccionando nenhum elemento motivador na categoria "Não é importante".

Contudo, todos os elementos continuam a ser considerados como Factores Motivadores e classificados com percentagens significativas (acima dos 50,00%), quando somados os valores nas categorias "Muito importante" ou "Importante".

Assim, os dois elementos mais seleccionados como Factores Motivadores na categoria "Muito Importante" são: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (69,23%) e "*Evitar perdas financeiras*" (61,54%). Na terceira posição aparecem, com a mesma pontuação (50,00%), os elementos "*Emergência contínua de novos riscos*" e "*Planear a segurança da informação antes da implementação de novas tecnologias*".

No entanto, verifica-se que para a organização, os gestores intermédios (19,23%) consideram como "Pouco importante" o elemento motivador "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*". Como "Pouco importante" são, ainda, apontados (11,54%) os seguintes quatro elementos motivadores: "*Evitar perdas financeiras*", "*Ocorrência de incidente anterior*", "*Alterações contínuas na legislação/regulação*" e a "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*".

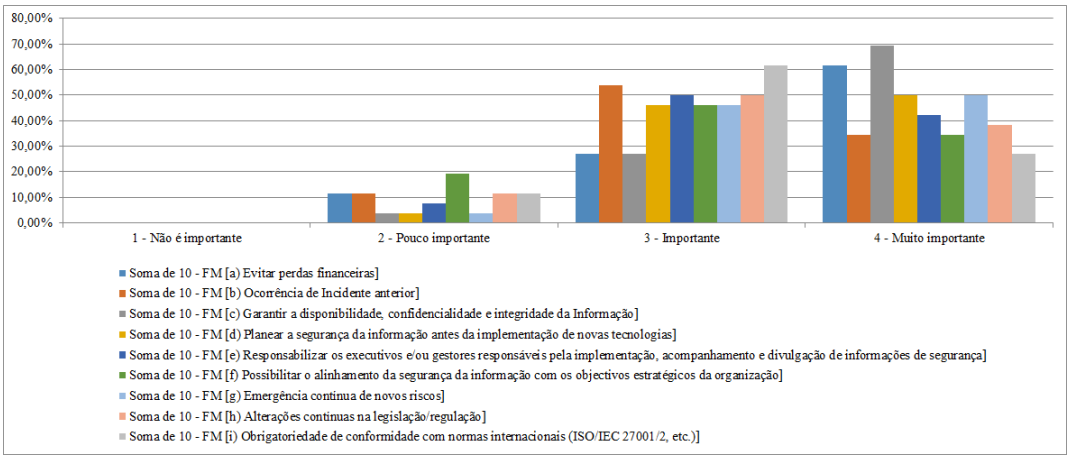


Gráfico 5.19- Factores Motivadores - PPO (Gestor Intermédio)

Por outro lado, e conforme gráfico (Gráfico 5.20) seguinte, verifica-se que, para o gestor intermédio e na categoria "Muito importante", revela-se o elemento inibidor "*Valor do investimento*" com a maior preferência (57,69%). O elemento inibidor "*Emergência contínua de novos riscos*" surge em primeiro lugar na categoria "Importante" (61,54%).

Contudo, todos os elementos continuam a ser considerados como Factores Inibidores e classificados com percentagens acima da metade (50,00%), quando somados os valores nas categorias "Muito importante" ou "Importante", continuando a constatar-se um enfoque maior na categoria "Importante".

No entanto, verifica-se que os gestores intermédios (19,23%) consideram como "Pouco importante" os elementos inibidores "*Alterações contínuas na legislação/regulação*" e "*Acesso restrito à Gestão de Topo*".

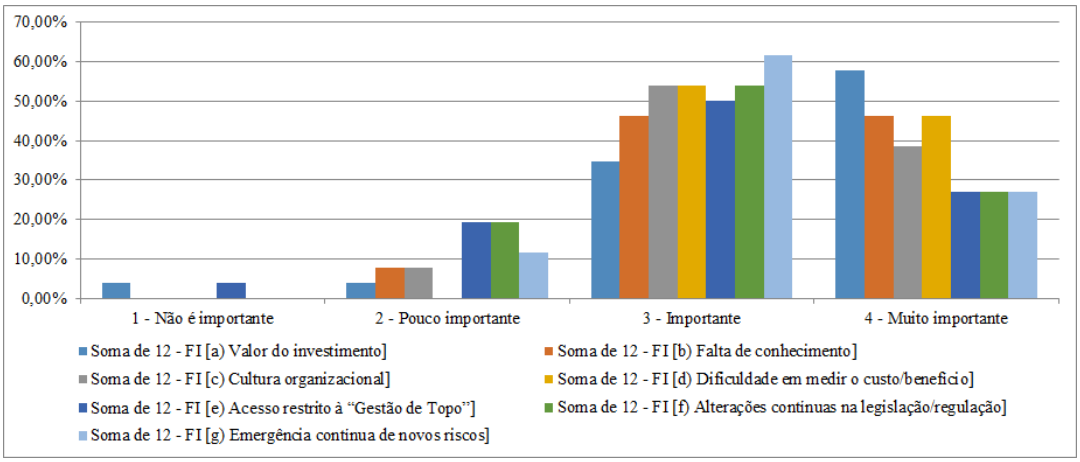


Gráfico 5.20- Factores Inibidores - PPO (Gestor Intermédio)

Do ponto de vista do Gestor das TI – para este gestor e, conforme gráfico (Gráfico 5.21) seguinte, comprova-se que o elemento motivador "*Garantir a disponibilidade,*

confidencialidade e integridade da informação" (70,59%) aparece em primeiro lugar na categoria "Muito importante". Nesta categoria, os elementos motivadores "*Evitar perdas financeiras*" e "*Planear a segurança da informação antes da implementação de novas tecnologias*" surgem classificados em segundo (64,71%) e terceiro lugar (52,94%). Em quarto lugar, daquela categoria, revela-se o elemento motivador "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" (47,06%).

De realçar ainda, que todos os elementos motivadores são considerados globalmente como "Muito importante" ou "Importante", atingindo pontuações superiores à metade percentual (50,00%), quando somados os valores nestas categorias.

O elemento motivador "*Emergência contínua de novos riscos*" (11,76%) é o principal na categoria "Pouco importante", sendo o elemento "*Ocorrência de incidente anterior*" (5,88%) o único a ser assinalado, na categoria "Não é importante".

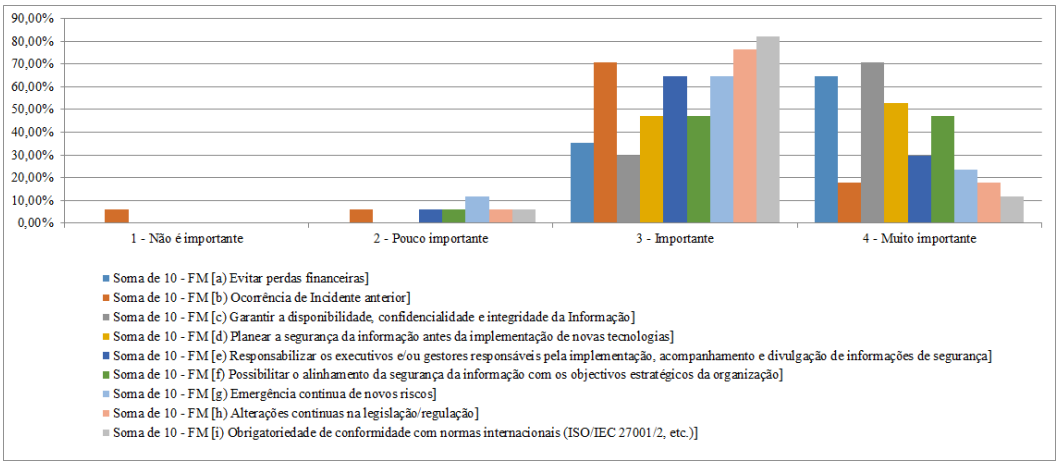


Gráfico 5.21- Factores Motivadores - PPO (Gestor das TI)

Por outro lado, e conforme o gráfico (Gráfico 5.22) abaixo, comprova-se que, para o gestor das TI, os elementos inibidores preferidos são: "*Alterações contínuas na legislação/regulação*" (82,53%) e "*Dificuldade em medir o custo/benefício*" (70,59%), encontrando-se os mesmos, classificados na categoria "Importante". Nesta categoria todos os elementos considerados como Factores Inibidores aparecem sempre maioritariamente populados (valores percentuais superiores a 50,00%).

O elemento inibidor "*Valor do investimento*" atinge a totalidade (100,00%), quando somados os valores percentuais nas categorias "Muito importante" e "Importante", sendo também o elemento inibidor mais votado na categoria "Muito importante".

Na categoria "Pouco Importante" encontram-se como elementos inibidores mais seleccionados "*Acesso restrito à Gestão de Topo*" e "*Emergência contínua de novos riscos*", ambos com

pontuação idêntica (23,53%). Seguidamente, também com igualdade de pontuação (17,65%), surgem os elementos: "*Alterações contínuas na legislação/regulação*" e "*Falta de conhecimento*".

A categoria "Não é importante" não recolhe votação por parte dos respondentes.

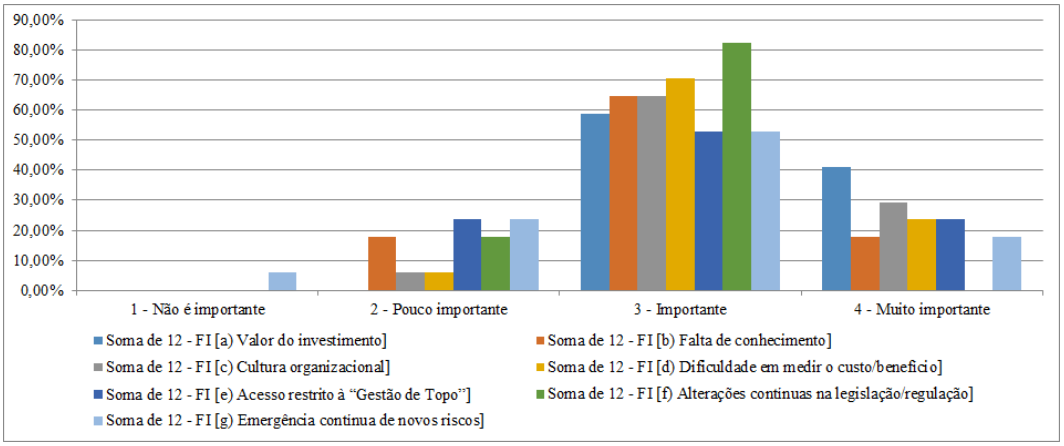


Gráfico 5.22- Factores Inibidores - PPO (Gestor das TI)

Do ponto de vista do Consultor das TI – nesta vista, na categoria "Muito importante" os dois elementos motivadores mais seleccionados são: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (71,43%) e "*Evitar perdas financeiras*" (64,29%). Na terceira posição, encontram-se, em igualdade de pontuação (35,71%), quatro elementos, a saber: "*Ocorrência de incidente anterior*", "*Planear a segurança da informação antes da implementação de novas tecnologias*", "*Emergência contínua de novos riscos*" e "*Alterações contínuas na legislação/regulação*".

Todavia, continua a comprovar-se, que todos os elementos motivadores considerados apresentam valores percentuais significativos (superiores a 50,00%), quando somados os valores nas categorias "Importante" e "Muito importante".

O elemento motivador mais apontado na categoria "Pouco importante" é "*Alterações contínuas na legislação/regulação*" (28,57%) e na categoria "Não é importante" surge o elemento "*Ocorrência de incidente anterior*" como o mais votado (14,29%). No gráfico (Gráfico 5.23) seguinte encontra-se detalhadamente o anteriormente indicado.

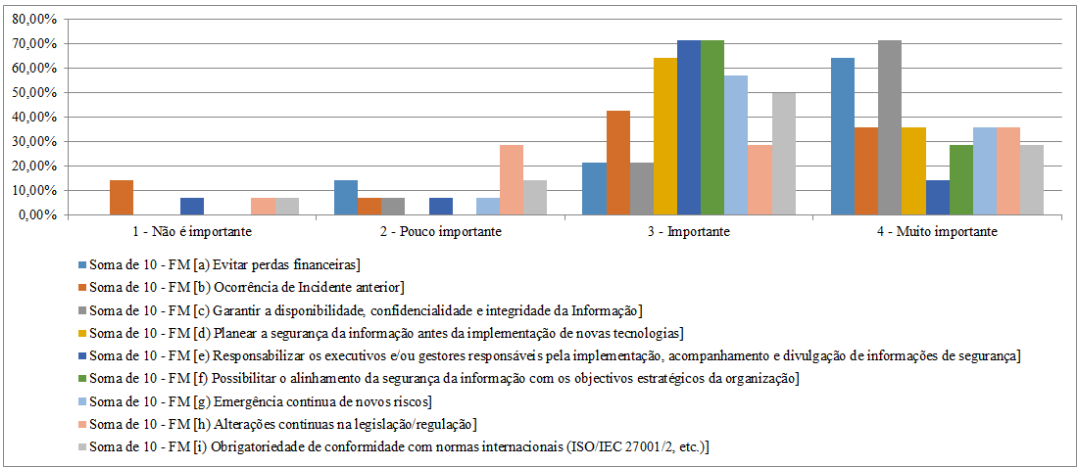


Gráfico 5.23- Factores Motivadores - PPO (Consultor das TI)

Por outro lado, o Consultor das TI tendo em conta o ponto de vista do próprio face à organização, considera que cinco dos sete elementos inibidores considerados agrupam, maioritariamente as preferências de votação nas categorias "Muito importante" e "Importante", embora o enfoque esteja, mais uma vez, na categoria "Importante". Os elementos inibidores são: "*Valor do investimento*" (28,57%; 64,29%), "*Cultura organizacional*" (28,57%; 42,86%), "*Falta de conhecimento*" (42,86%; 14,29%), "*Dificuldade em medir o custo/benefício*" (28,57%; 35,71%) e "*Acesso restrito à Gestão de Topo*" (7,14%; 50,00%).

Relativamente aos outros dois elementos inibidores "*Alterações contínuas na legislação/regulação*" e "*Emergência contínua de novos riscos*" agrupam a votação maioritariamente nas categorias "Pouco importante" e "Não é importante" com, respectivamente, (50,00%; 14,29%) e (35,71%; 21,43%). No gráfico (Gráfico 5.24) seguinte visualiza-se o acima mencionado.

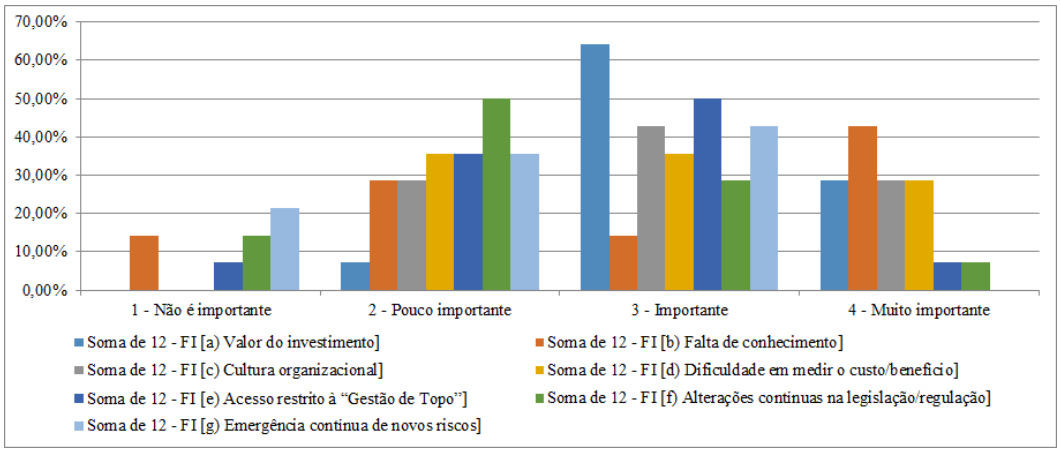


Gráfico 5.24- Factores Inibidores - PPO (Consultor das TI)

Do ponto de vista do Gestor / Funcionário da Segurança – esta classe apresenta uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). Os elementos

motivadores mostram todos valores acima da metade percentual (50,00%), quando somados os valores nas categorias "Importante" e "Muito importante", com excepção do elemento "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*" que obtém (66,67%) da pontuação na categoria "Pouco importante".

Os elementos motivadores "*Garantir a disponibilidade, confidencialidade e integridade da informação*" e "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*" obtêm a unanimidade (100,00%) na categoria "Muito importante".

Este grupo profissional aponta, ainda, como "Pouco importante" o elemento motivador: "*Ocorrência de incidente anterior*" (33,33%). No gráfico (Gráfico 5.25) seguinte visualiza-se o mencionado.

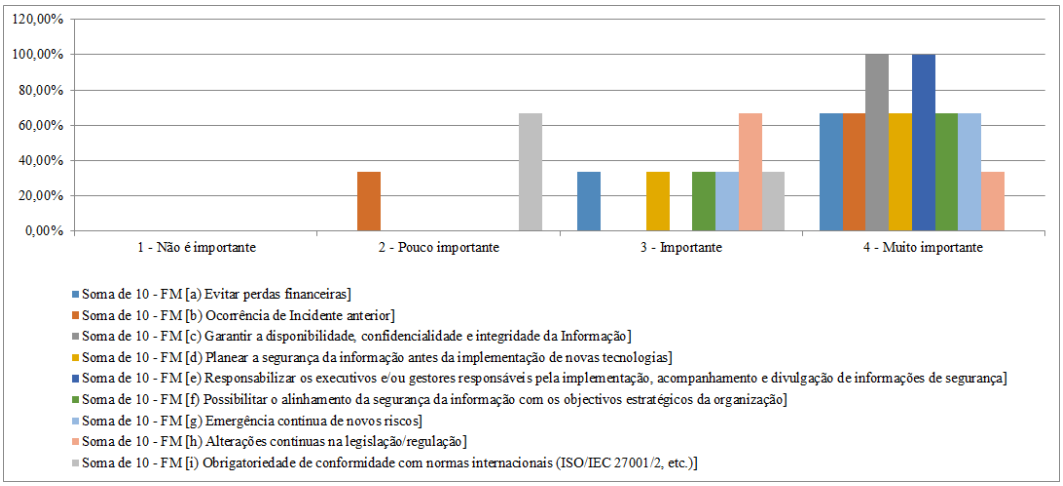


Gráfico 5.25- Factores Motivadores - PPO (Gestor/Funcionário da Segurança)

Contudo, nesta classe, verifica-se que os elementos inibidores apresentam todos valores percentuais acima da metade percentual (50,00%), quando somados os valores nas categorias "Muito importante" e "Importante", com prevalência nesta última.

Assim, os elementos inibidores "*Falta de conhecimento*", "*Dificuldade em medir o custo/benefício*", "*Acesso restrito à Gestão de Topo*" e "*Emergência contínua de novos riscos*" atingem a totalidade das preferências (100,00%), quando somados os valores nas categorias "Muito importante" e "Importante".

Na categoria "Importante" temos os seguintes elementos inibidores com igual votação (66,67%): "*Valor do investimento*", "*Falta de conhecimento*", "*Acesso restrito à gestão de topo*" e "*Emergência contínua de novos riscos*".

Na categoria "Muito importante" o elemento inibidor mais escolhido é "*Dificuldade em medir o custo/benefício*" (66,67%).

Este grupo profissional aponta ainda como "Pouco importante" os elementos inibidores: "*Valor do investimento*", "*Cultura organizacional*" e "*Alterações contínuas na legislação/regulação*", todos com a pontuação idêntica (33,33%). A categoria "Não é importante" não recolhe nenhuma votação. O gráfico (Gráfico 5.26) seguinte revela o acima exposto.

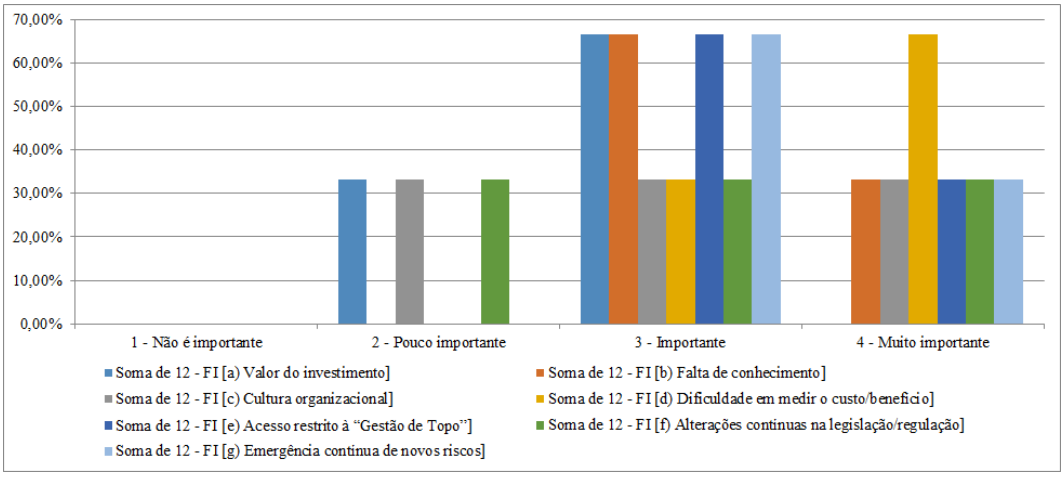


Gráfico 5.26- Factores Inibidores - PPO (Gestor/Funcionário da Segurança)

Do ponto de vista do Trabalhador – nesta vista também, todos os elementos considerados motivadores apresentam valores percentuais acima da metade (50,00%), quando somados nas categorias "Importante" e "Muito importante", notando-se a predominância das preferências na primeira categoria referida.

Porém, os dois primeiros elementos motivadores mais votados pelos respondentes na categoria "Muito importante" são: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (74,51%) e "*Planear a segurança da informação antes da implementação de novas tecnologias*" (56,86%). Todavia, este último elemento agrupa a totalidade percentual (100,00%), no somatório dos valores recolhidos para as categorias "Muito importante" e "Importante".

Na categoria "Importante" revela-se em primeiro lugar das preferências dos respondentes, o elemento motivador "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" (58,82%).

Porém, o elemento mais apontado, por este grupo profissional, na categoria "Pouco importante" para a organização como factor motivador é: "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*" (15,69%). No gráfico (Gráfico 5.27) seguinte visualiza-se o acima indicado.

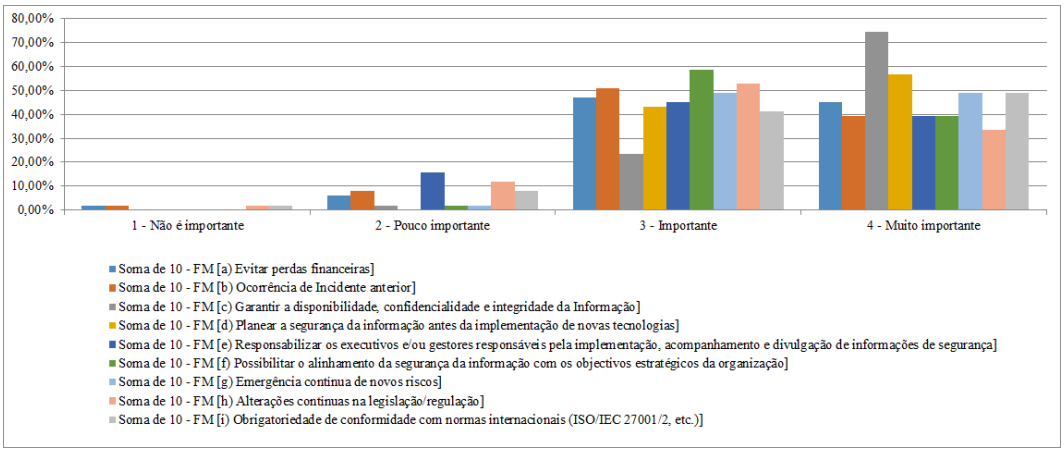


Gráfico 5.27- Factores Motivadores - PPO (Trabalhador)

Por outro lado, também nesta perspectiva do Trabalhador, todos os elementos inibidores considerados apresentam valores acima da metade percentual (50,00%), quando somados os valores nas categorias "Importante" e "Muito importante".

Assim, o elemento inibidor mais votado na categoria "Importante" é "*Emergência contínua de novos riscos*" (50,98%), seguido do elemento "*Acesso restrito à Gestão de Topo*" (47,06%).

Por outro lado, na categoria "Muito importante" vencem, com percentagem idêntica (45,10%), os elementos inibidores: "*Falta de conhecimento*" e "*Cultura organizacional*".

Relativamente à categoria "Pouco importante" agrupa maior pontuação o elemento inibidor "*Alterações contínuas na legislação/regulação*" (29,41%) seguido do elemento "*Emergência contínua de novos riscos*" (21,57%).

Na categoria "Não é importante" surgem os elementos inibidores "*Acesso restrito à Gestão de Topo*", "*Alterações contínuas na legislação/regulação*" e "*Emergência contínua de novos riscos*" todos populados com valores pouco significativos (inferiores a 5,00%). No gráfico (Gráfico 5.28) seguinte visualiza-se o acima referido.

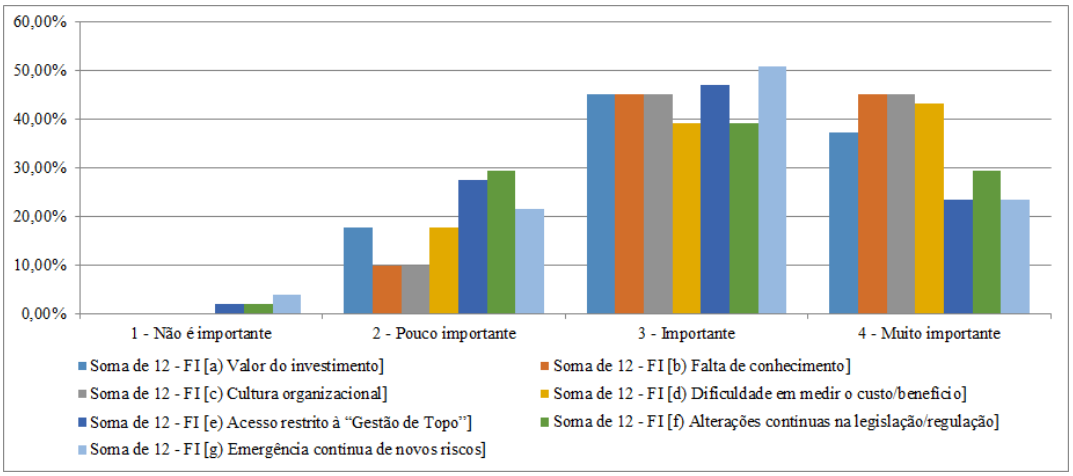


Gráfico 5.28- Factores Inibidores - PPO (Trabalhador)

5.1.5 – Resumo da Perspectiva do Próprio face à Organização

Neste item e conforme modelo mostrado na figura abaixo (Figura 5.5) sucede a reunião dos resultados obtidos, na perspectiva do próprio face à organização para os Factores Motivadores e Inibidores.

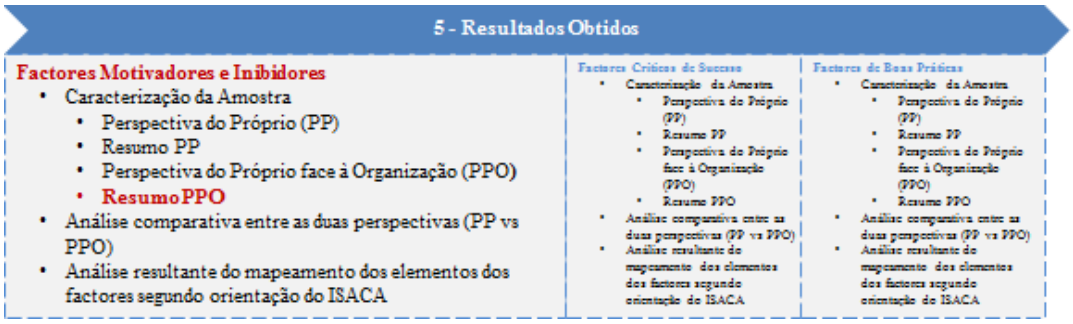


Figura 5.5- Modelo dos Resultados Obtidos: FM e FI / Resumo da PPO

Resumindo, na tabela (Tabela 5.3) seguinte apresenta-se a ordenação pela categoria "Muito importante" e "Não é importante" dos elementos considerados para o estudo como Factores Motivadores, segundo cada uma das vistas dadas pela função do respondente tendo em conta a perspectiva do mesmo face à organização.

Conforme se comprova, o elemento motivador "*Garantir a disponibilidade, confidencialidade e integridade da Informação*" surge como o mais referido, por todas as funções do respondente, na categoria "Muito importante". Em segundo lugar, nesta categoria, revela-se o elemento motivador "*Evitar perdas financeiras*".

De sublinhar que os elementos "*Planear a segurança da informação antes da implementação de novas tecnologias*" e "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" manifestam-se, respectivamente, na terceira e quinta

posição da votação dos respondente, quando estes indicam o seu ponto de vista face à organização.

Constata-se, ainda, que na categoria "Não é importante" são apontados seis dos nove elementos motivadores considerados para este factor, surgindo como elemento mais seleccionado "*Ocorrência de Incidente anterior*". Os elementos motivadores "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*", "*Alterações contínuas na legislação/regulação*" e "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*" mostram-se todos na segunda posição.

Factores Motivadores - PPO (- Elemento não é referido pelos respondentes)		10 - FM [a] Evitar perdas financeiras]	10 - FM [b] Ocorrência de Incidente anterior]	10 - FM [c] Garantir a disponibilidade, confidencialidade e integridade da Informação]	10 - FM [d] Planear a segurança da informação antes da implementação de novas tecnologias]	10- FM [e] Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança]	10- FM [f] Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização]	10 - FM [g] Emergência contínua de novos riscos]	10 - FM [h] Alterações contínuas na legislação/regulação]	10 - FM [i] Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)]
Gestor de Topo	Muito importante	1	4	1	2	4	3	3	-	5
	Não é importante	-	-	-	-	1	1	-	-	-
Gestor Intermédio	Muito importante	2	6	1	3	4	6	3	5	7
	Não é importante	-	-	-	-	-	-	-	-	-
Gestor das TI	Muito importante	2	7	1	3	5	4	6	7	8
	Não é importante	-	1	-	-	-	-	-	-	-
Consultor das TI	Muito importante	2	3	1	3	5	4	3	3	4
	Não é importante	-	1	-	-	2	-	-	2	2
Gestor / Funcionário da Segurança	Muito importante	2	2	1	2	1	2	2	3	-
	Não é importante	-	-	-	-	-	-	-	-	-
Trabalhador	Muito importante	4	5	1	2	5	5	3	6	3
	Não é importante	1	1	-	-	-	-	-	1	1
Global	**Muito importante**	**2**	**7**	**1**	**3**	**6**	**5**	**4**	**9**	**8**
	Não é importante	**3**	**1**	**-**	**-**	**2**	**3**	**-**	**2**	**2**

Tabela 5.3- Factores Motivadores - PPO: Ordenação das preferências

Por outro lado, na tabela (Tabela 5.4) seguinte apresenta-se a ordenação pela categoria "Muito importante" e "Não é importante" dos elementos considerados para o estudo como Factores Inibidores, segundo cada uma das vistas dadas pela função do respondente.

Desta forma, podemos visualizar, que o elemento inibidor "*Valor do investimento*" é o mais referido em primeiro lugar na categoria "Muito importante". O Consultor das TI coloca-o em segundo lugar dando preferência ao elemento inibidor "*Falta de conhecimento*".

No entanto, o Trabalhador vota naquele elemento inibidor, em terceiro lugar, dando também a sua preferência ao elemento "*Falta de conhecimento*", o qual revela-se como o segundo elemento inibidor mais votado.

Verifica-se, ainda, que na categoria "Não é importante" são apontados todos os elementos inibidores com excepção de dois, a saber: "*Cultura organizacional*" e "*Dificuldade em medir o custo/benefício*".

Factores Inibidores - PPO (- Elemento não é referido pelos respondentes)		12 - FI [a) Valor do investimento]	12 - FI [b) Falta de conhecimento]	12 - FI [c) Cultura organizacional]	12- FI [d) Dificuldade em medir o custo/benefício]	12 - FI [e) Acesso restrito à "Gestão de Topo"]	12 - FI [f) Alterações contínuas na legislação/regulação]	12 - FI [g) Emergência contínua de novos riscos]
Gestor de Topo	Muito importante	1	3	3	3	-	4	2
	Não é importante	-	1	-	-	-	-	-
Gestor Intermédio	Muito importante	1	2	3	2	4	4	4
	Não é importante	1	-	-	-	1	-	-
Gestor das TI	Muito importante	1	4	2	3	3	-	4
	Não é importante	-	-	-	-	-	-	-
Consultor das TI	Muito importante	2	1	2	2	3	3	-
	Não é importante	-	2	-	-	3	2	1
Gestor / Funcionário da Segurança	Muito importante	-	2	2	1	2	2	2
	Não é importante	-	-	-	-	-	-	-
Trabalhador	Muito importante	3	1	1	2	5	4	5
	Não é importante	-	-	-	-	2	2	1
Global	**Muito importante**	**1**	**2**	**4**	**3**	**6**	**6**	**5**
	Não é importante	**3**	**2**	**-**	**-**	**2**	**2**	**1**

Tabela 5.4- Factores Inibidores - PPO: Ordenação das preferências

5.1.6 – Análise Comparativa entre as duas Perspectivas (Próprio e Próprio face à Organização)

Neste ponto, apresentam-se os resultados comparativos das duas perspectivas dos respondentes (a do próprio e a do próprio face à organização/sector) relativamente aos Factores Motivadores e Inibidores considerados (Figura 5.6).

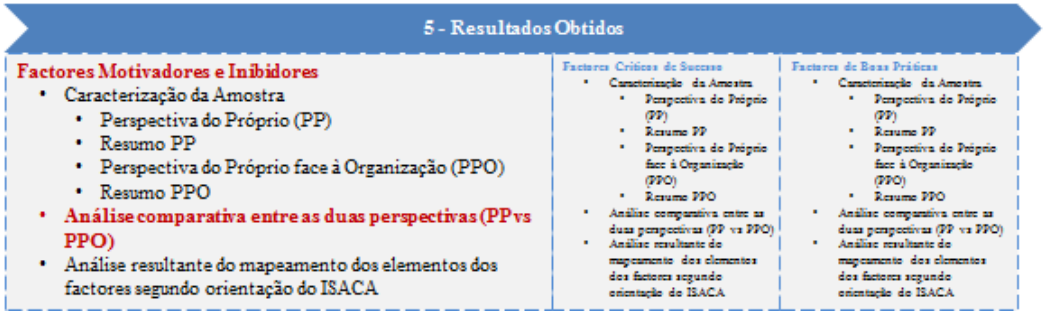


Figura 5.6- Modelo dos Resultados Obtidos: FM e FI / Análise Comparativa

Assim, primeiramente efectuou-se o cálculo do nível médio de importância para cada elemento destes factores, através da seguinte fórmula:

$$\text{Nível médio de importância} = \frac{\sum_{c=1}^{4}(nº\ de\ referências\ ao\ elemento * c)}{n.º\ de\ respondentes}$$

em que a variável "c" corresponde ao valor da categoria de classificação (1-Não é importante; 2-Pouco importante; 3-Importante e 4-Muito importante) seleccionado pelo respondente para o elemento em causa.

Deste modo, na tabela (Tabela 5.5) seguinte, mencionam-se os valores médios encontrados para todos os elementos considerados como Factores Motivadores, tendo em conta todas as respostas chegadas.

Factores Motivadores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Evitar perdas financeiras	3,6	3,5	0,1
Ocorrência de Incidente anterior	3,2	3,2	0,0
Garantir a disponibilidade, confidencialidade e integridade da Informação	3,8	3,7	0,1
Planear a segurança da informação antes da implementação de novas tecnologias	3,6	3,5	0,1
Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	3,2	3,2	0,0
Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização	3,4	3,3	0,1
Emergência contínua de novos riscos	3,4	3,4	0,0
Alterações contínuas na legislação/regulação	3,1	3,1	0,0
Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)	3,2	3,2	0,0

Tabela 5.5 - Factores Motivadores: valores Nível Médio de Importância (Global)

Da tabela anterior, verifica-se que, em quatro dos nove elementos considerados, os resultados mostram desvios na classificação dos mesmos como Factores Motivadores para a adopção/implementação de um SGSI numa organização do sector das Águas e Saneamento em Portugal.

Logo, constata-se que o nível médio de importância da perspectiva do próprio, referente aos elementos que se consideram como Factores Motivadores, difere do nível médio de importância da perspectiva do próprio face à organização, nomeadamente nos quatro seguintes elementos motivadores: "*Evitar perdas financeiras*", "*Garantir a disponibilidade, confidencialidade e integridade da Informação*", "*Planear a segurança da informação antes da implementação de novas tecnologias*" e "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*".

Estes desvios indicam que, para estes elementos motivadores, os respondentes assinalam um nível médio de importância maior, quando analisam os mesmos segundo a sua própria perspectiva do que quando indicam a sua perspectiva face à organização.

Para uma melhor visualização desses desvios apresenta-se, seguidamente, o gráfico (Gráfico 5.29) "radar".

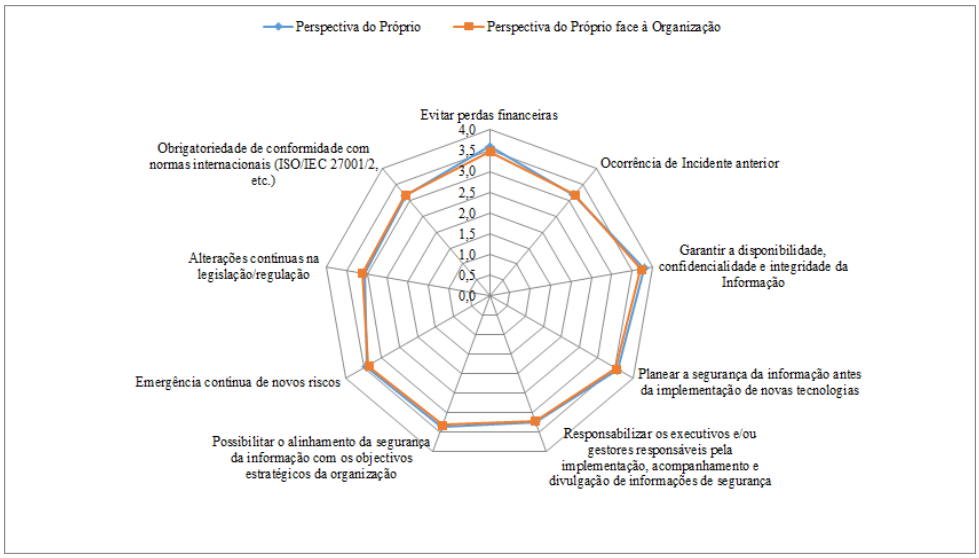


Gráfico 5.29- Factores Motivadores: Comparação entre PP e PPO (Global)

No entanto, na tabela (Tabela 5.6) seguinte encontram-se os valores médios apurados para todos os elementos considerados como Factores Inibidores tendo em conta todas as respostas chegadas, constatando-se que, em quatro dos sete elementos considerados como Factores Inibidores para a adopção/implementação de um SGSI numa organização do sector das Águas e Saneamento em Portugal, a perspectiva do próprio apresenta desvios na classificação dos mesmos relativamente à perspectiva do próprio face à organização.

Factores Inibidores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Valor do investimento	3,2	3,3	-0,1
Falta de conhecimento	3,3	3,2	0,1
Cultura organizacional	3,3	3,3	0,0
Dificuldade em medir o custo/benefício	3,3	3,2	0,1
Acesso restrito à "Gestão de Topo"	2,9	2,9	0,0
Alterações contínuas na legislação/regulação	2,8	2,9	-0,1
Emergência contínua de novos riscos	2,9	2,9	0,0

Tabela 5.6- Factores Inibidores: valores Nível Médio de Importância (Global)

Assim, verifica-se que o nível médio de importância - na perspectiva do próprio, é maior em dois dos elementos inibidores considerados, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, apresentando um valor de desvio igual (0,1) para os seguintes elementos:

- "*Falta de conhecimento*"
- "*Dificuldade em medir o custo/benefício*"

No entanto, existem outros dois elementos inibidores onde o nível médio de importância - na perspectiva do próprio é menor, perante o nível médio de importância – na perspectiva do próprio face à organização, apresentando um valor de desvio igual (-0,1) para esses elementos:

- "*Valor do investimento*"
- "*Alterações contínuas na legislação/regulação*".

Para uma melhor visualização desses desvios, apresenta-se, seguidamente, o gráfico (Gráfico 5.30) "radar".

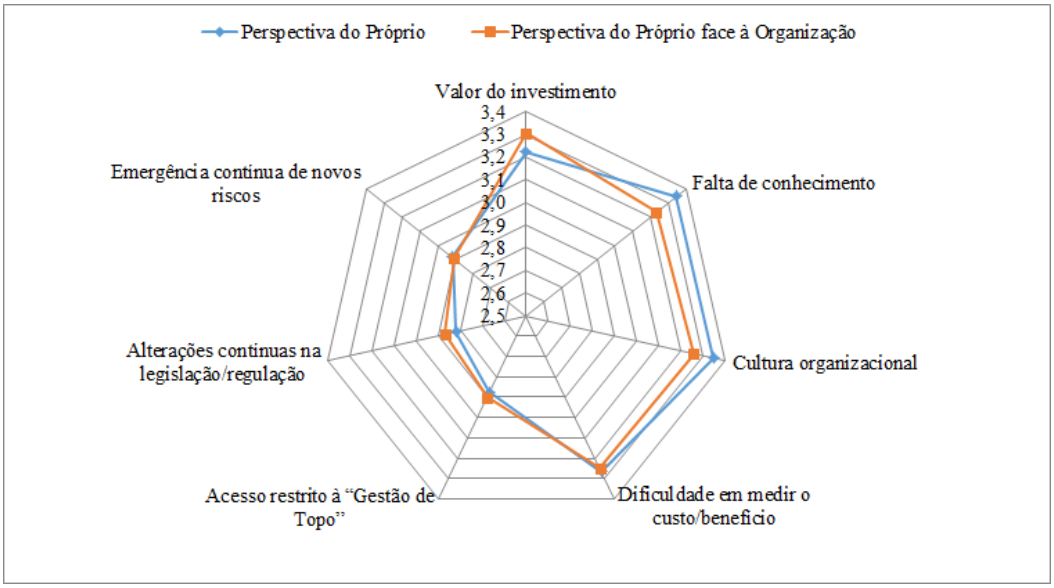


Gráfico 5.30- Factores Inibidores: Comparação entre PP e PPO (Global)

Para se compreender melhor a origem dos desvios, isto é, para aferir que tipo de respondentes contribuíram para a apresentação destes desvios, elaborou-se também o cálculo do nível médio de importância para cada elemento destes factores – motivadores e inibidores, acrescentando-se o tipo de função do respondente. Assim, chegou-se aos seguintes resultados:

Do ponto de vista do Gestor de Topo - a tabela (Tabela 5.7) seguinte, mostra que as opiniões dos gestores de topo, que somam (8,26%) dos respondentes, apresentam desvios em oito dos nove elementos motivadores considerados. Verifica-se, pois, que o nível médio de importância - na perspectiva do próprio, é maior em sete dos elementos motivadores considerados, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização. A excepção encontra-se no elemento motivador "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*" que apresenta menor valor, porque o gestor de topo atribui-lhe, em média, um nível de importância maior enquanto factor motivador, quando refere o seu ponto de vista face à organização.

Os desvios encontrados variam entre (0,1) e (0,3), verificando-se que o maior valor do desvio (0,3) corresponde ao elemento motivador "*Emergência contínua de novos riscos*". O valor do desvio igual a (0,2) aparece para os seguintes elementos motivadores: "*Evitar perdas financeiras*" e "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*", mostrando que o próprio atribui-lhes maior nível médio de importância do que quando emite a sua opinião face à organização.

Factores Motivadores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Evitar perdas financeiras	3,9	3,7	0,2
Ocorrência de Incidente anterior	3,2	3,1	0,1
Garantir a disponibilidade, confidencialidade e integridade da Informação	3,8	3,8	0,0
Planear a segurança da informação antes da implementação de novas tecnologias	3,6	3,5	0,1
Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	3,0	2,9	0,1
Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização	3,4	3,2	0,2
Emergência contínua de novos riscos	3,4	3,1	0,3
Alterações contínuas na legislação/regulação	2,8	2,7	0,1
Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)	2,6	2,8	-0,2

Tabela 5.7- Factores Motivadores: valores Nível Médio de Importância (Gestor de Topo)

O gráfico (Gráfico 5.31) radar abaixo mostra as diferenças acima expostas.

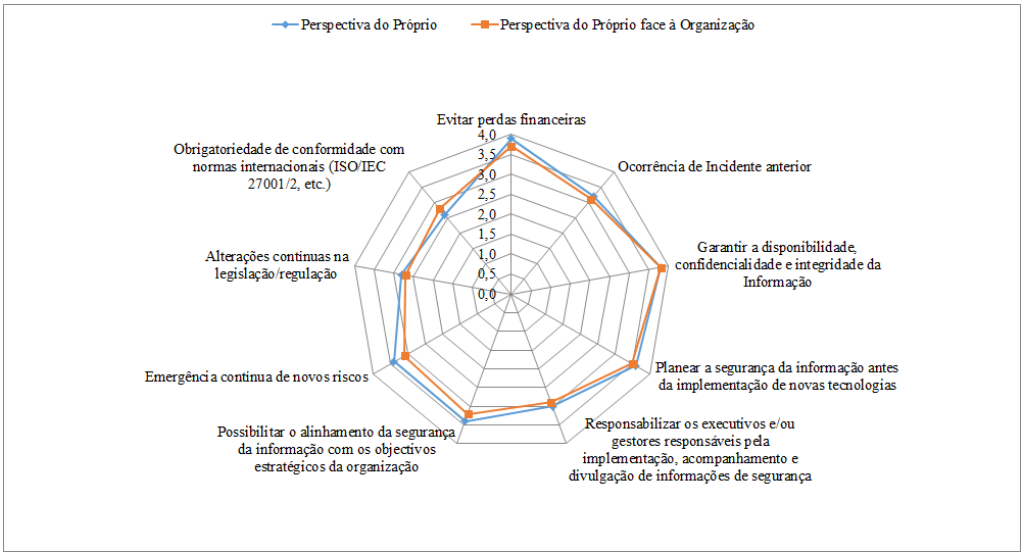


Gráfico 5.31- Factores Motivadores: Comparação entre PP e PPO (Gestor de Topo)

Também, a tabela (Tabela 5.8) seguinte, mostra que as opiniões dos gestores de topo apresentam desvios em cinco dos sete elementos inibidores considerados.

Assim, constata-se que o nível médio de importância - na perspectiva do próprio, é maior em três dos elementos inibidores considerados, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, a saber: "*Falta de conhecimento*" (3,3;3,1), "*Dificuldade em medir o custo/benefício*" (3,3; 3,1) e "*Emergência contínua de novos riscos*" (3,2;3,1). Isto é, o gestor de topo atribui-lhe, em média, um nível de importância maior como factor inibidor, quando refere o seu ponto de vista.

Contudo, nos elementos inibidores "*Valor do investimento*" (3,4;3,6) e "*Cultura organizacional*" (2,9;3,1) acontece o contrário. Ou seja, o gestor de topo agrupa, para estes elementos, um valor maior para o nível médio de importância como factor inibidor quando refere o seu ponto de vista face à organização. O valor, para o nível médio de importância, mantém-se igual nas duas perspectivas para os elementos "*Acesso restrito à gestão de topo*" e "*Alterações contínuas na legislação/regulação*".

Factores Inibidores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Valor do investimento	3,4	3,6	-0,2
Falta de conhecimento	3,3	3,1	0,2
Cultura organizacional	2,9	3,1	-0,2
Dificuldade em medir o custo/benefício	3,3	3,1	0,2
Acesso restrito à "Gestão de Topo"	2,7	2,7	0,0
Alterações contínuas na legislação/regulação	2,7	2,7	0,0
Emergência contínua de novos riscos	3,2	3,1	0,1

Tabela 5.8- Factores Inibidores: valores Nível Médio de Importância (Gestor de Topo)

O gráfico (Gráfico 5.32) radar abaixo mostra as diferenças acima expostas.

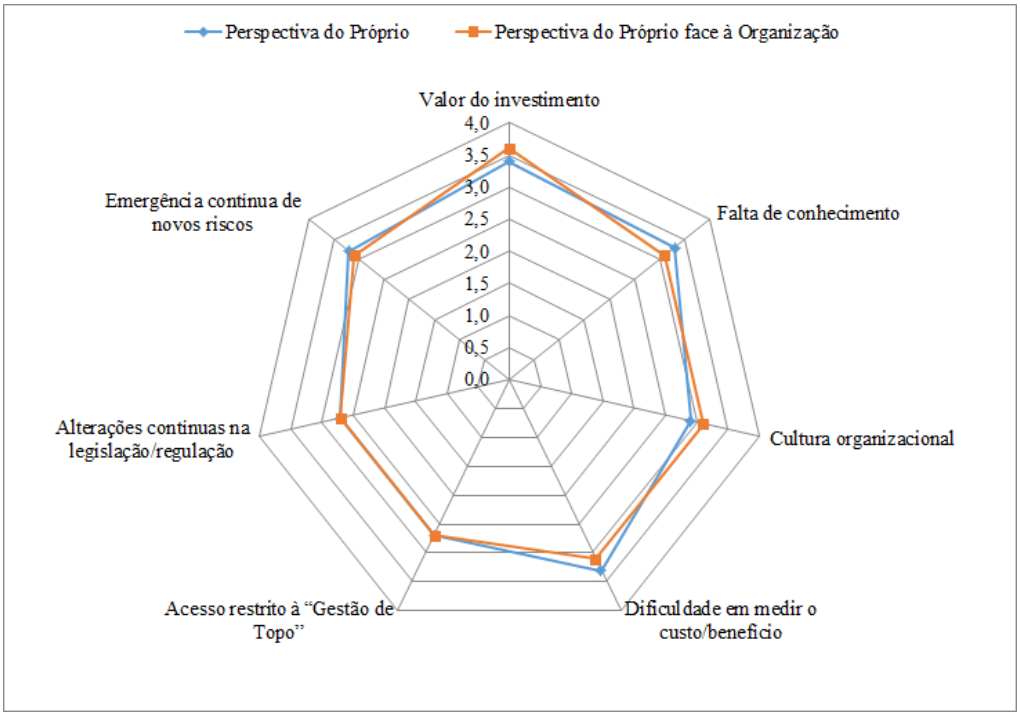


Gráfico 5.32- Factores Inibidores: Comparação entre PP e PPO (Gestor de Topo)

Do ponto de vista do Gestor Intermédio - a tabela (Tabela 5.9) seguinte, mostra que as opiniões dos gestores intermédios, que representam (21,49%) dos respondentes, apresentam desvios em relação a quatro elementos motivadores: "*Evitar perdas financeiras*", "*Garantir a disponibilidade, confidencialidade e integridade da Informação*", "*Emergência contínua de novos riscos*" e "*Alterações contínuas na legislação/regulação*". Nos três primeiros elementos,

este gestor indica maior pontuação no nível médio de importância quando apresenta a sua própria perspectiva. No entanto, caracteriza o quarto elemento motivador acima indicado – "*Alterações contínuas na legislação/regulação*" com um valor maior, para o nível médio de importância, quando aponta a sua perspectiva face à organização.

O elemento motivador que atinge maior desvio (0,2) é "*Evitar perdas financeiras*".

Factores Motivadores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Evitar perdas financeiras	3,7	3,5	0,2
Ocorrência de Incidente anterior	3,2	3,2	0,0
Garantir a disponibilidade, confidencialidade e integridade da Informação	3,8	3,7	0,1
Planear a segurança da informação antes da implementação de novas tecnologias	3,5	3,5	0,0
Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	3,3	3,3	0,0
Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização	3,2	3,2	0,0
Emergência contínua de novos riscos	3,6	3,5	0,1
Alterações contínuas na legislação/regulação	3,2	3,3	-0,1
Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)	3,2	3,2	0,0

Tabela 5.9- Factores Motivadores: valores Nível Médio de Importância (Gestor Intermédio)

O gráfico (Gráfico 5.33) radar abaixo mostra as diferenças acima indicadas.

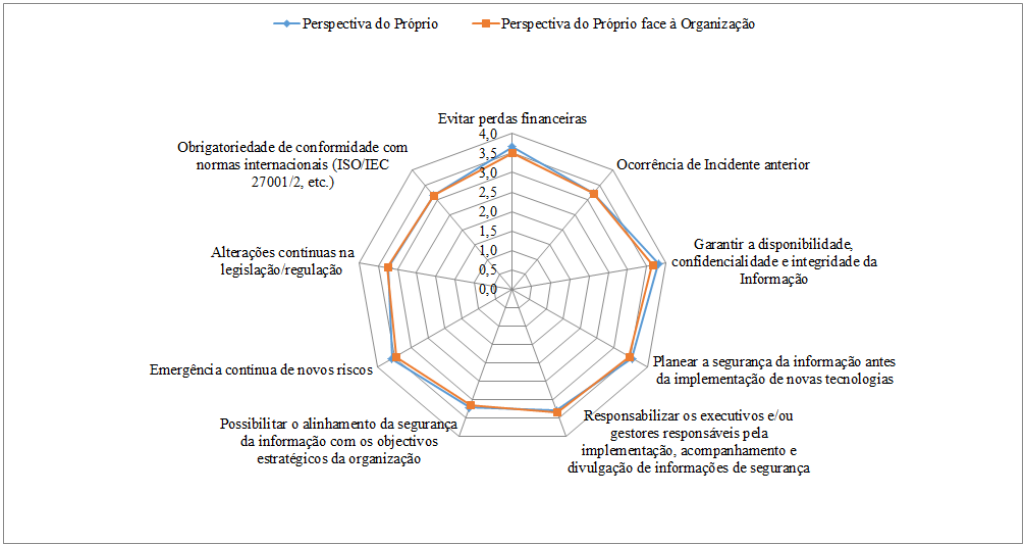


Gráfico 5.33- Factores Motivadores: Comparação entre PP e PPO (Gestor Intermédio)

Por outro lado, a tabela (Tabela 5.10) seguinte, mostra que as opiniões dos gestores intermédios, apresentam também desvios em cinco dos sete elementos inibidores considerados. São eles: "*Valor do investimento*", "*Acesso restrito à Gestão de Topo*", "*Alterações contínuas na legislação/regulação*", "*Falta de conhecimento*" e "*Cultura organizacional*". Para os três

primeiros elementos, este grupo profissional, indica uma maior pontuação no nível médio de importância, quando apresenta a sua perspectiva face à organização. No entanto, nos outros dois elementos inibidores, acontece o contrário: a pontuação do nível médio de importância é maior, quando apresenta a sua perspectiva.

O elemento inibidor "*Valor do investimento*" obtém o maior valor absoluto para o desvio (0,2) entre as perspectivas do respondente. Nos restantes elementos inibidores verificam-se valores absolutos de desvio idênticos (0,1).

Factores inibidores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Valor do investimento	3,3	3,5	-0,2
Falta de conhecimento	3,5	3,4	0,1
Cultura organizacional	3,4	3,3	0,1
Dificuldade em medir o custo/benefício	3,5	3,5	0,0
Acesso restrito à "Gestão de Topo"	2,9	3,0	-0,1
Alterações contínuas na legislação/regulação	3,0	3,1	-0,1
Emergência contínua de novos riscos	3,2	3,2	0,0

Tabela 5.10- Factores Inibidores: valores Nível Médio de Importância (Gestor Intermédio)

No gráfico (Gráfico 5.34) radar abaixo visualiza-se as diferenças atrás referidas.

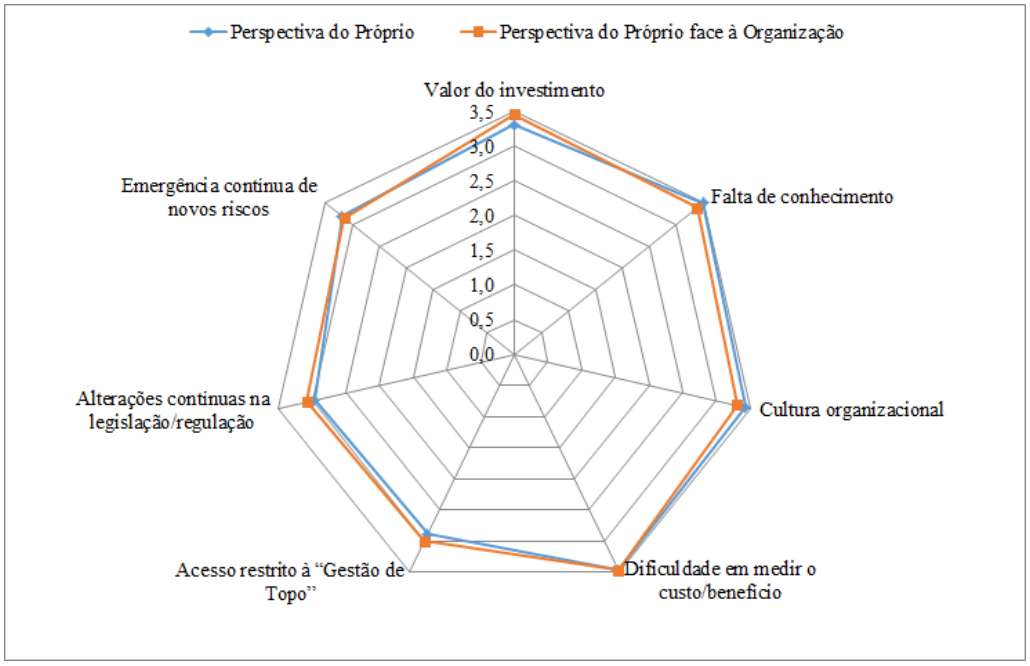


Gráfico 5.34- Factores Inibidores: Comparação entre PP e PPO (Gestor Intermédio)

Do ponto de vista do Gestor das TI - a tabela (Tabela 5.11) seguinte, mostra que as opiniões dos gestores das TI, que representam (14,05%) dos respondentes, não apresentam desvios para dois elementos motivadores: "*Evitar perdas financeiras*" e "*Ocorrência de Incidente anterior*".

Contudo, para todos os outros elementos motivadores, as classificações atribuídas ao nível médio de importância, tendo em conta a perspectiva do próprio, é sempre maior quando comparada com a perspectiva do próprio face à organização. Exceptua-se a este comportamento o elemento motivador "*Alterações contínuas na legislação/regulação*" que adquire maior valor de desvio (-0,2) na perspectiva do próprio face à organização.

Os dois elementos motivadores em que são verificados maiores desvios (0,2) são: "*Garantir a disponibilidade, confidencialidade e integridade da Informação*" e "*Emergência contínua de novos riscos*".

Factores Motivadores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Evitar perdas financeiras	3,6	3,6	0,0
Ocorrência de Incidente anterior	3,0	3,0	0,0
Garantir a disponibilidade, confidencialidade e integridade da Informação	3,9	3,7	0,2
Planear a segurança da informação antes da implementação de novas tecnologias	3,6	3,5	0,1
Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	3,3	3,2	0,1
Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização	3,5	3,4	0,1
Emergência contínua de novos riscos	3,3	3,1	0,2
Alterações contínuas na legislação/regulação	2,9	3,1	-0,2
Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)	3,2	3,1	0,1

Tabela 5.11- Factores Motivadores: valores Nível Médio de Importância (Gestor das TI)

O gráfico (Gráfico 5.35) radar abaixo mostra as diferenças acima mencionadas.

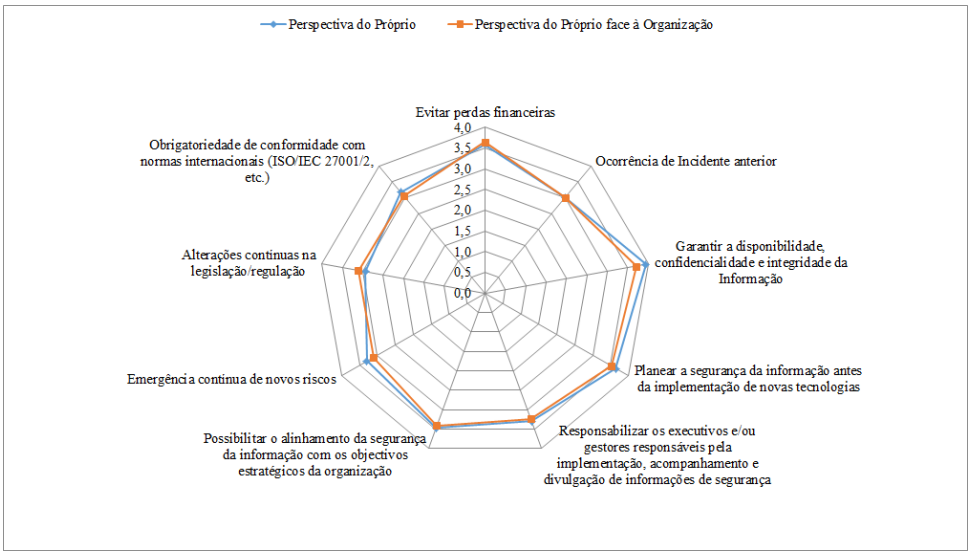


Gráfico 5.35- Factores Motivadores: Comparação entre PP e PPO (Gestor das TI)

Por outro lado, a tabela (Tabela 5.12) seguinte, mostra que as opiniões dos gestores das TI apresentam desvios para todos os elementos inibidores considerados com excepção do elemento "*Emergência contínua de novos riscos*".

Contudo, nos dois elementos inibidores "*Falta de conhecimento*" (3,1;3,0) e "*Cultura organizacional*" (3,4;3,2), a classificação atribuída ao nível médio de importância, tendo em conta a perspectiva do próprio, é maior quando comparada com a perspectiva do próprio face à organização.

Todavia, para os restantes elementos inibidores, comprova-se o contrário: a pontuação do nível médio de importância adquire um valor maior na perspectiva do próprio face à organização.

O elemento inibidor "*Dificuldade em medir o custo/benefício*" é o que obtém maior valor absoluto de desvio (0,3) seguido dos elementos "*Cultura organizacional*" e "*Valor do investimento*" que apresentam valores absolutos de desvio iguais (0,2).

Factores Inibidores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Valor do investimento	3,2	3,4	-0,2
Falta de conhecimento	3,1	3,0	0,1
Cultura organizacional	3,4	3,2	0,2
Dificuldade em medir o custo/benefício	2,9	3,2	-0,3
Acesso restrito à "Gestão de Topo"	2,9	3,0	-0,1
Alterações contínuas na legislação/regulação	2,7	2,8	-0,1
Emergência contínua de novos riscos	2,8	2,8	0,0

Tabela 5.12- Factores Inibidores: valores Nível Médio de Importância (Gestor das TI)

O gráfico radar abaixo (Gráfico 5.36) mostra as diferenças acima expostas.

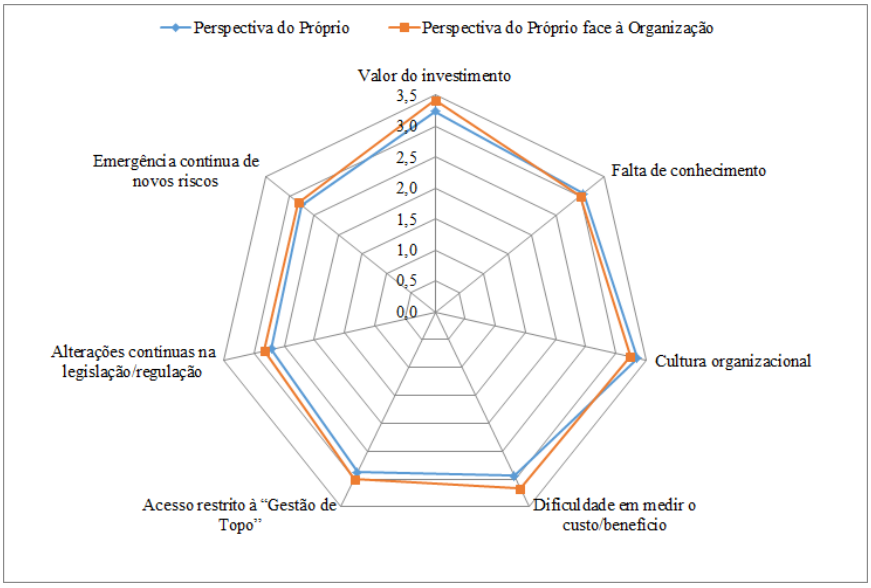


Gráfico 5.36- Factores Inibidores: Comparação entre PP e PPO (Gestor das TI)

Do ponto de vista do Consultor das TI - a tabela (Tabela 5.13) seguinte, mostra que as opiniões dos consultores das TI, que representam (11,57%) dos respondentes, apresentam desvios em quatro dos nove elementos motivadores considerados.

Assim, para os elementos motivadores "*Ocorrência de incidente anterior*" e "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*", este grupo profissional atribui, na perspectiva do próprio face à organização, um valor para o nível médio de importância superior ao apresentado para a perspectiva do próprio. Porém, para os elementos motivadores "*Garantir a disponibilidade, confidencialidade e integridade da Informação*" e "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*", os resultados indicam, que este grupo considera, que o nível médio de importância do ponto de vista do próprio é superior ao considerado na perspectiva do próprio face à organização.

Factores Motivadores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Evitar perdas financeiras	3,5	3,5	0,0
Ocorrência de Incidente anterior	2,9	3,0	-0,1
Garantir a disponibilidade, confidencialidade e integridade da Informação	3,7	3,6	0,1
Planear a segurança da informação antes da implementação de novas tecnologias	3,4	3,4	0,0
Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	3,0	2,9	0,1
Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização	3,3	3,3	0,0
Emergência contínua de novos riscos	3,3	3,3	0,0
Alterações contínuas na legislação/regulação	2,9	2,9	0,0
Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)	2,9	3,0	-0,1

Tabela 5.13- Factores Motivadores: valores Nível Médio de Importância (Consultor das TI)

O gráfico (Gráfico 5.37) radar abaixo mostra as diferenças acima expostas.

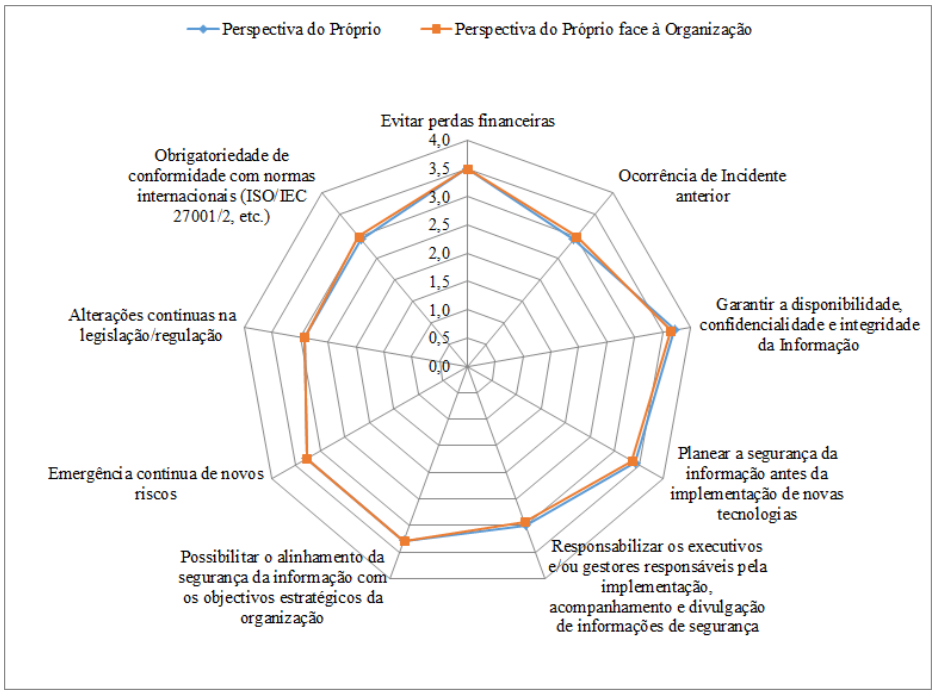


Gráfico 5.37- Factores Motivadores: Comparação entre PP e PPO (Consultor das TI)

Por sua vez, a tabela (Tabela 5.14) seguinte, mostra que as opiniões dos consultores das TI, apresentam desvios em todos os elementos inibidores com excepção do elemento "*Valor do investimento*" (3,2; 3,2) que surge com a mesma pontuação para o nível médio de importância em ambas as perspectivas.

Constata-se, ainda, que em cinco dos elementos inibidores - "*Falta de conhecimento*" (3,1; 2,9), "*Cultura organizacional*" (3,1; 3,0), "*Dificuldade em medir o custo/benefício*" (3,1; 2,9), "*Alterações contínuas na legislação/regulação*" (2,4; 2,3) e "*Emergência contínua de novos riscos*" (2,3; 2,2), este grupo profissional revela, na perspectiva do próprio face à organização, um valor para o nível médio de importância inferior ao apresentado para a perspectiva do próprio. Para o primeiro e terceiro elementos inibidores acima mencionados, encontra-se um desvio de valor absoluto idêntico (0,2) e para os outros elementos o valor absoluto do desvio também é igual (0,1).

Contudo para o elemento inibidor "*Acesso restrito à Gestão de Topo*" (2,5; 2,6) comprova-se o contrário. A pontuação é maior para o nível médio de importância na perspectiva do próprio face à organização, apresentando o valor absoluto (0,1) para o desvio.

Factores Inibidores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Valor do investimento	3,2	3,2	0,0
Falta de conhecimento	3,1	2,9	0,2
Cultura organizacional	3,1	3,0	0,1
Dificuldade em medir o custo/benefício	3,1	2,9	0,2
Acesso restrito à "Gestão de Topo"	2,5	2,6	-0,1
Alterações contínuas na legislação/regulação	2,4	2,3	0,1
Emergência contínua de novos riscos	2,3	2,2	0,1

Tabela 5.14- Factores Inibidores: valores Nível Médio de Importância (Consultor das TI)

O gráfico (Gráfico 5.38) radar abaixo mostra as diferenças acima referidas.

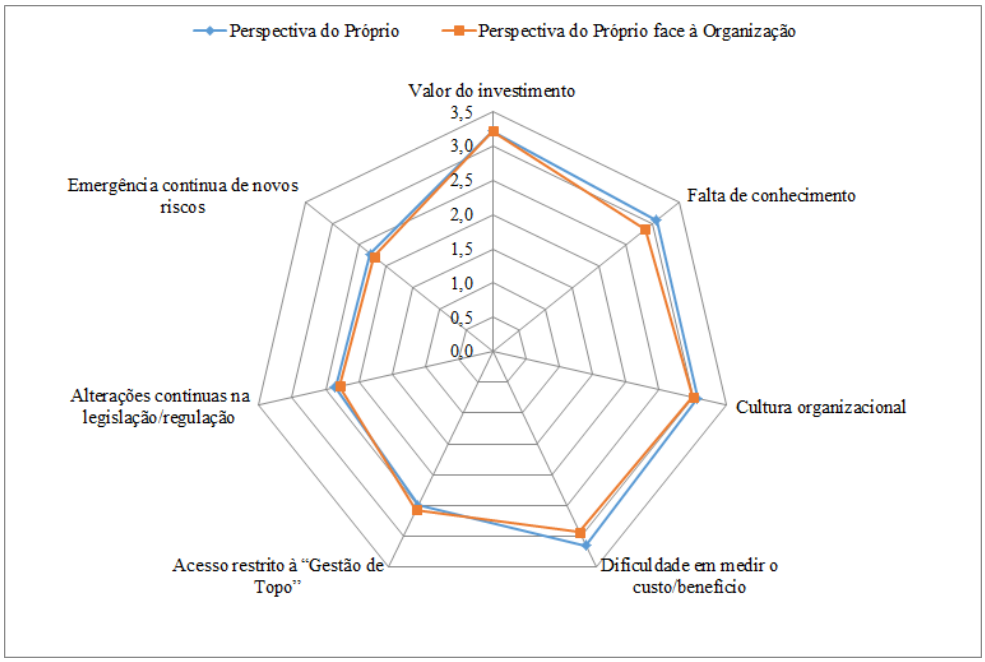


Gráfico 5.38- Factores Inibidores: Comparação entre PP e PPO (Consultor das TI)

Do ponto de vista do Gestor/Funcionário de Segurança – esta classe apresenta uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). No entanto, ainda assim e conforme tabela (Tabela 5.15) abaixo, refira-se os desvios apresentados para os três elementos motivadores: "*Planear a segurança da informação antes da implementação de novas tecnologias*", "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*" e "*Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)*" que apresentam, na perspectiva do próprio face à organização, valores para o nível médio de importância superiores aos encontrados para a perspectiva do próprio, verificando-se, respectivamente, valores de desvios iguais a (0,4), (0,3) e (0,4) .

Factores Motivadores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Evitar perdas financeiras	3,7	3,7	0,0
Ocorrência de Incidente anterior	3,3	3,3	0,0
Garantir a disponibilidade, confidencialidade e integridade da Informação	4,0	4,0	0,0
Planear a segurança da informação antes da implementação de novas tecnologias	3,3	3,7	-0,4
Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	3,7	4,0	-0,3
Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização	3,7	3,7	0,0
Emergência contínua de novos riscos	3,7	3,7	0,0
Alterações contínuas na legislação/regulação	3,3	3,3	0,0
Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)	2,7	2,3	0,4

Tabela 5.15- Factores Motivadores: valores Nível Médio de Importância (Gestor/Funcionário da Segurança)

O gráfico (Gráfico 5.39) radar abaixo visualiza-se as diferenças atrás indicadas.

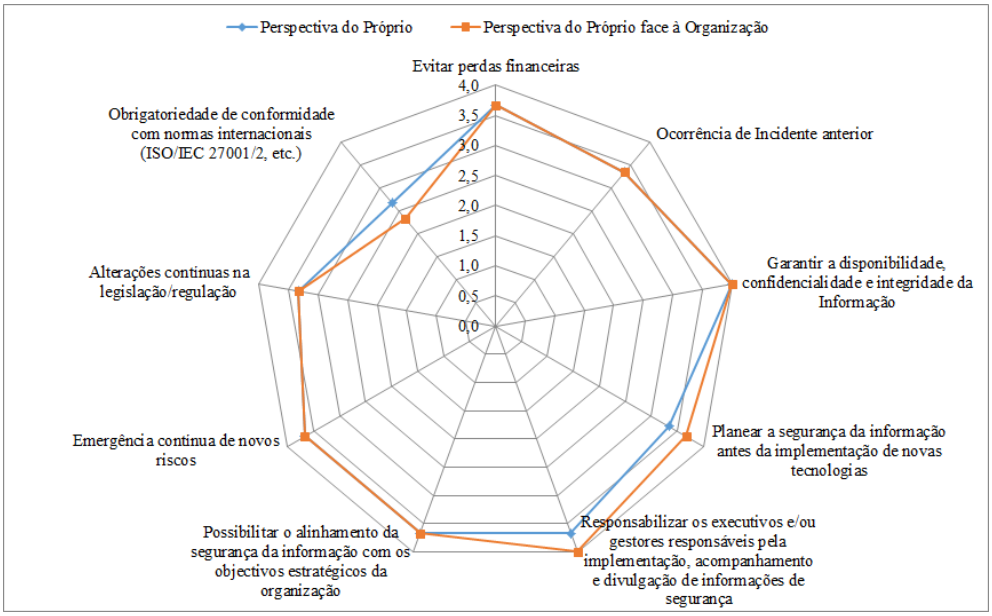


Gráfico 5.39- Factores Motivadores: Comparação entre PP e PPO (Gestor/Funcionário da Segurança)

No entanto, ainda assim, refira-se o desvio apresentado para o elemento inibidor: "*Falta de conhecimento*" que apresenta, na perspectiva do próprio face à organização, um valor para o nível médio de importância inferior ao encontrado para a perspectiva do próprio, obtendo-se o valor (0,3) para o desvio. A tabela (Tabela 5.16) seguinte revela o acima exposto.

Factores Inibidores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Valor do investimento	2,7	2,7	0,0
Falta de conhecimento	3,0	3,3	-0,3
Cultura organizacional	3,0	3,0	0,0
Dificuldade em medir o custo/benefício	3,7	3,7	0,0
Acesso restrito à "Gestão de Topo"	3,3	3,3	0,0
Alterações contínuas na legislação/regulação	3,0	3,0	0,0
Emergência contínua de novos riscos	3,3	3,3	0,0

Tabela 5.16- Factores Inibidores: valores Nível Médio de Importância (Gestor/Funcionário da Segurança)

O gráfico (Gráfico 5.40) radar abaixo mostra as diferenças acima mencionadas.

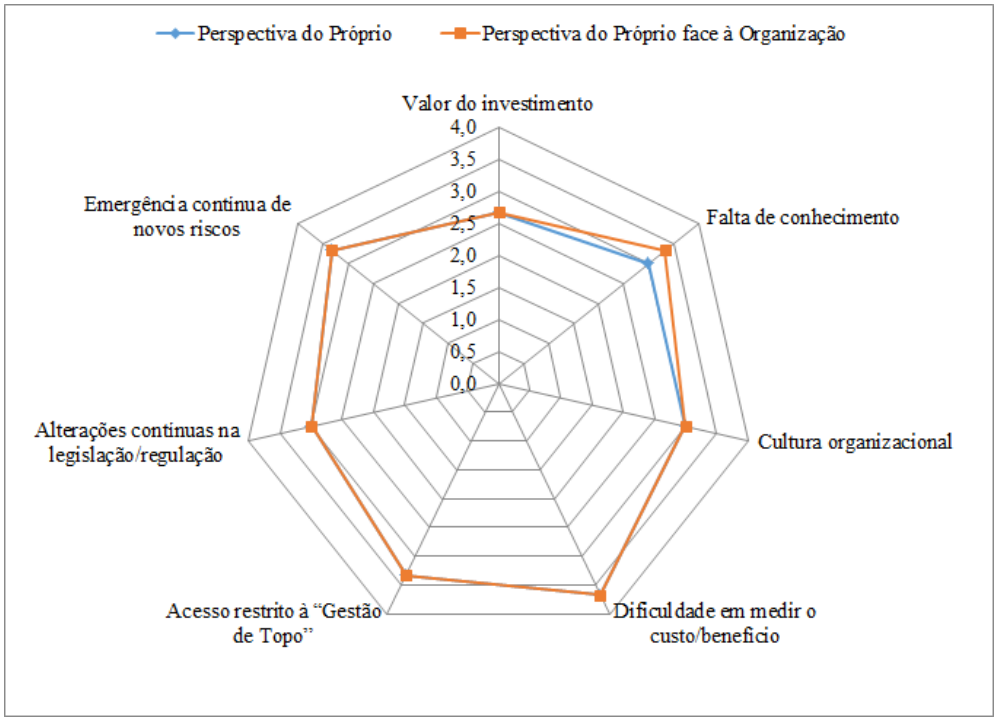


Gráfico 5.40- Factores Inibidores: Comparação entre PP e PPO (Gestor/Funcionário da Segurança)

Do ponto de vista do Trabalhador - a tabela (Tabela 5.17) seguinte, mostra que as opiniões dos trabalhadores, que representam (42,15%) dos respondentes, apresentam desvios em cinco dos nove elementos motivadores considerados.

Assim, nos elementos motivadores "*Evitar perdas financeiras*", "*Garantir a disponibilidade, confidencialidade e integridade da Informação*" e "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*", a perspectiva do próprio apresenta valores de nível médio de importância superiores aos encontrados para a perspectiva do próprio face à organização. Já para os outros dois elementos motivadores verifica-se o contrário. A perspectiva do próprio apresenta valores menores para o nível médio de importância do que na vertente da perspectiva do próprio face à organização.

Os desvios encontrados são todos iguais em valor absoluto (0,1).

Factores Motivadores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Evitar perdas financeiras	3,5	3,4	0,1
Ocorrência de Incidente anterior	3,3	3,3	0,0
Garantir a disponibilidade, confidencialidade e integridade da Informação	3,8	3,7	0,1
Planear a segurança da informação antes da implementação de novas tecnologias	3,6	3,6	0,0
Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	3,3	3,2	0,1
Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização	3,4	3,4	0,0
Emergência contínua de novos riscos	3,4	3,5	-0,1
Alterações contínuas na legislação/regulação	3,1	3,2	-0,1
Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)	3,4	3,4	0,0

Tabela 5.17- Factores Motivadores: valores Nível Médio de Importância (Trabalhador)

O gráfico (Gráfico 5.41) radar seguinte apresenta as diferenças acima expostas.

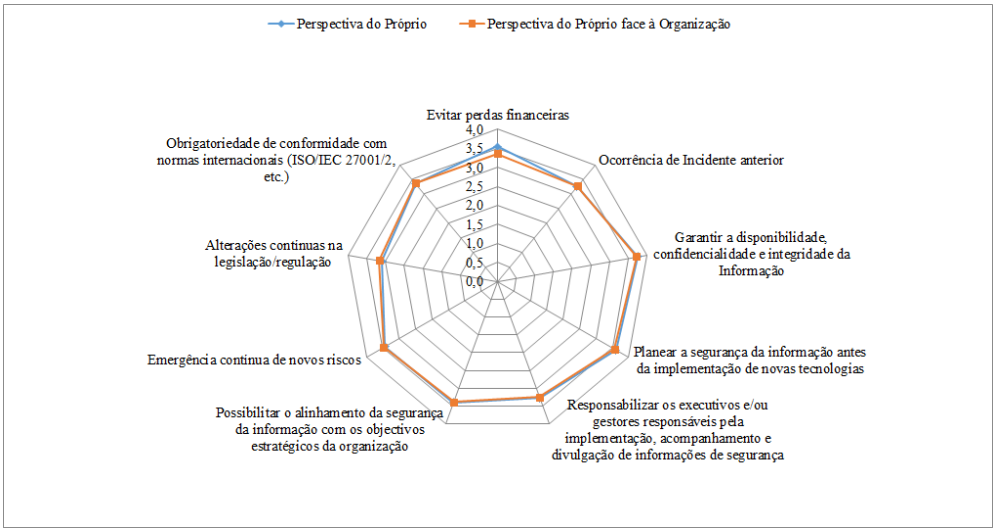


Gráfico 5.41- Factores Motivadores: Comparação entre PP e PPO (Trabalhador)

Por outro lado, no que respeita aos Factores Inibidores e conforme mostra a tabela (Tabela 5.18) seguinte, a opinião dos trabalhadores apresenta desvios em quatro dos sete elementos considerados. Assim, nos elementos inibidores "*Falta de conhecimento*", "*Cultura organizacional*" e "*Acesso restrito à Gestão de Topo*" a perspectiva do próprio apresenta valores de nível médio de importância superiores aos encontrados para a perspectiva do próprio face à organização. Já para o outro elemento "*Alterações contínuas na legislação/regulação*" comprova-se o contrário. A perspectiva do próprio apresenta um valor menor para o nível médio de importância do que na vertente da perspectiva do próprio face à organização.

Em todos os elementos encontrados com desvios, o valor absoluto deste é sempre igual a (0,1).

Factores Inibidores	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Valor do investimento	3,2	3,2	0,0
Falta de conhecimento	3,5	3,4	0,1
Cultura organizacional	3,5	3,4	0,1
Dificuldade em medir o custo/benefício	3,3	3,3	0,0
Acesso restrito à "Gestão de Topo"	3,0	2,9	0,1
Alterações contínuas na legislação/regulação	2,9	3,0	-0,1
Emergência contínua de novos riscos	2,9	2,9	0,0

Tabela 5.18- Factores Inibidores: valores Nível Médio de Importância (Trabalhador)

O gráfico (Gráfico 5.42) radar abaixo mostra as diferenças acima referidas.

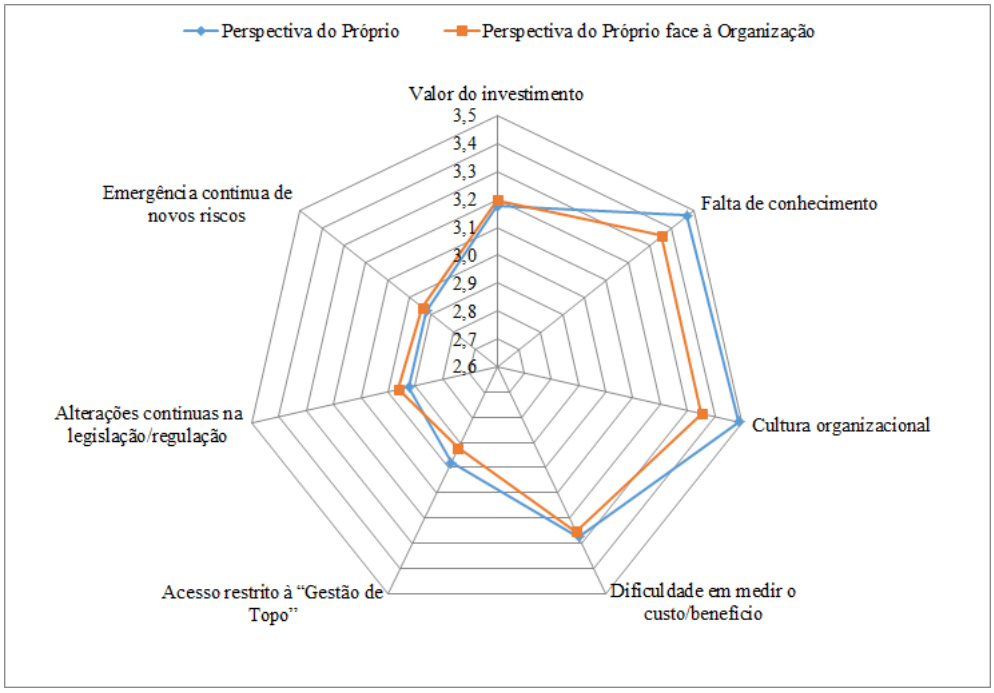


Gráfico 5.42 - Factores Inibidores: Comparação entre PP e PPO (Trabalhador)

5.1.7 – Análise resultante do mapeamento dos elementos do factor segundo a orientação - ISACA

Nesta parte, conforme indicado na figura seguinte (Figura 5.7), expõem-se os resultados da análise obtida para os elementos considerados na caracterização dos Factores Motivadores e Inibidores, enquadrando os mesmos conforme orientação proposta pelo ISACA [123] que refere: «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*» e representada no ponto 4.2 deste documento.

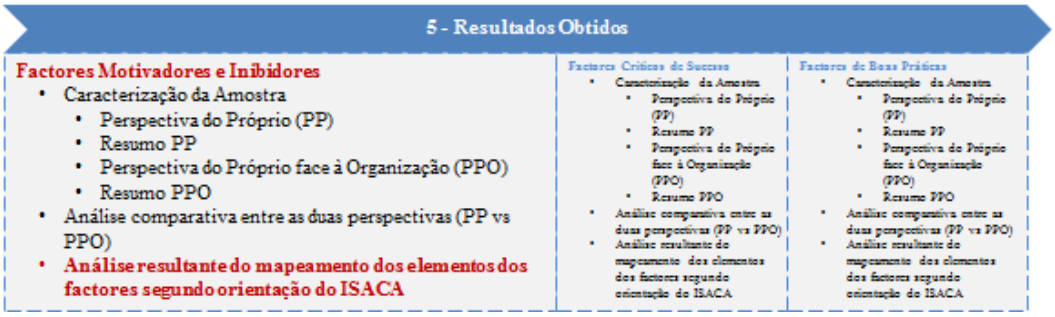


Figura 5.7- Modelo dos Resultados Obtidos: FM e FI / Análise – Mapeamento ISACA

Assim, a partir dos valores médios de importância encontrados para os elementos considerados na caracterização dos Factores Motivadores visualiza-se na tabela/gráfico abaixo (Gráfico 5.43) que, globalmente, os respondentes focam a sua preferência, como Factores Motivadores, em elementos relacionados com o pilar de resultados – "*Gestão de Recursos*", indiciando a existência de uma cultura de segurança da informação ainda focada na "protecção de activos". De facto, o pilar de resultados – "*Alinhamento Estratégico*" aparece na terceira posição apresentando-se com valores médios de importância de (3,4) – perspectiva do próprio (3,3) – perspectiva do próprio face à organização.

Factores Motivadores (Nivel médio de importância - Global)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Evitar perdas financeiras			3,6	3,5						
b) Ocorrência de incidente anterior			3,2	3,2						
c) Garantir a disponibilidade, confidencialidade e integridade da Informação					3,8	3,7				
d) Planear a segurança da informação antes da implementação das novas tecnologias									3,6	3,5
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança							3,2	3,2		
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	3,4	3,3								
g) Emergência contínua de novos riscos			3,4	3,4						
h) Alterações contínuas na legislação/regulação			3,1	3,1						
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.							3,2	3,2		
Total (valor médio)	3,4	3,3	3,3	3,3	3,8	3,7	3,2	3,2	3,6	3,5

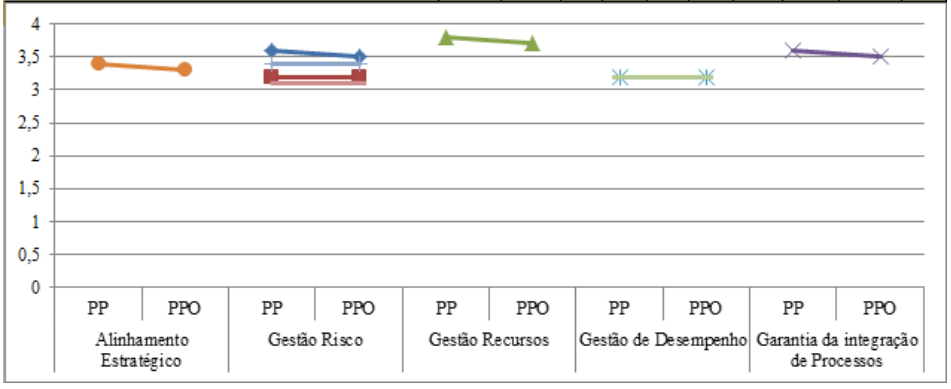


Gráfico 5.43- Factores Motivadores: Mapeamento ISACA (Global)

Por outro lado, o estudo revela que, globalmente, os elementos considerados inibidores para a adopção/implementação dum Sistema de Gestão da Segurança da Informação nas organizações centram-se nos pilares de resultados: "*Gestão de Recursos*" (3,2), "*Gestão de Desempenho*" e "*Garantia da Integração de Processos*" (3,3). De notar, ainda, que os itens "*Falta de conhecimento*" e "*Cultura Organizacional*", elementos relacionados com o ´factor humano´ revelam um nível médio de importância de dimensão paralela aos itens "*Valor do investimento*" e "*Dificuldade em medir o custo/benefício*". Neste contexto, pode-se aferir que o reconhecimento desta ´lacuna´ já é positivo para endereçar o caminho da mudança. A tabela/gráfico (Gráfico 5.44) seguinte mostra o acima referido.

Factores Inibidores (Nível médio de importância - Global)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Valor do investimento					3,2	3,3				
b) Falta de conhecimento									3,3	3,2
c) Cultura organizacional									3,3	3,3
d) Dificuldade em medir o custo/beneficio							3,3	3,2		
e) Acesso restrito à "Gestão de Topo"	2,9	2,9								
f) Alterações contínuas na legislação / regulação			2,8	2,9						
g) Emergência contínua de novos riscos			2,9	2,9						
Total (Valor médio)	2,9	2,9	2,9	2,9	3,2	3,3	3,3	3,2	3,3	3,25

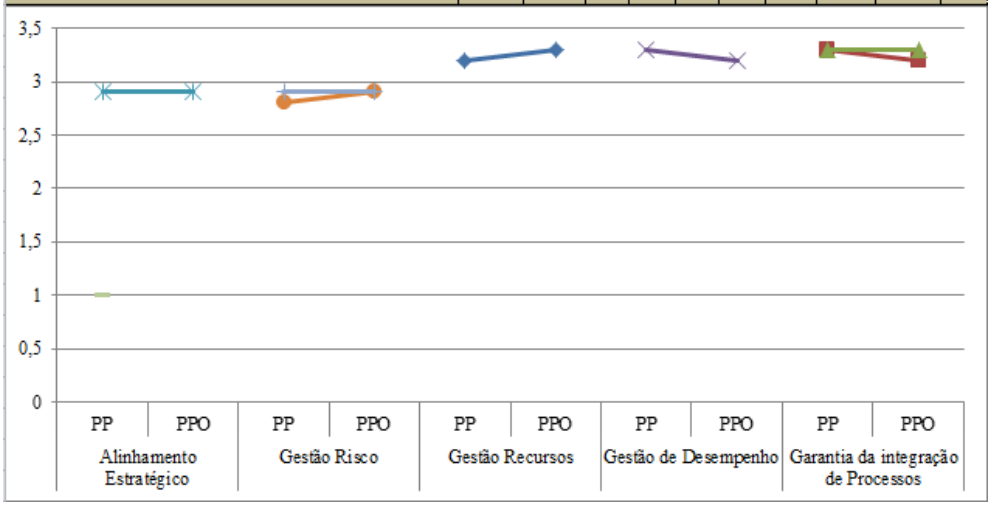


Gráfico 5.44 - Factores Inibidores: Mapeamento ISACA (Global)

Contudo, se se analisar os resultados tendo em conta a função do respondente, verifica-se que o enfoque do pilar de resultados muda com o grupo profissional.

Todavia, o Gestor de Topo mantém o enfoque da motivação no pilar de resultados – "*Gestão de Recursos*", embora na perspectiva do próprio realce o elemento motivador "*Evitar perdas financeiras*" pertencente ao pilar de resultados – "*Gestão de Risco*". Contudo, posiciona o pilar de resultados – "*Alinhamento Estratégico*" na terceira posição. A tabela/gráfico (Gráfico 5.45) seguinte ilustra o acima mencionado.

Factores Motivadores (Nível médio de importância - Gestor de Topo)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Evitar perdas financeiras			3,9	3,7						
b) Ocorrência de incidente anterior			3,2	3,1						
c) Garantir a disponibilidade, confidencialidade e integridade da Informação					3,8	3,8				
d) Planear a segurança da informação antes da implementação das novas tecnologias									3,6	3,5
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança							3	2,9		
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	3,4	3,2								
g) Emergência contínua de novos riscos			3,4	3,1						
h) Alterações contínuas na legislação/regulação			2,8	2,7						
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.							2,6	2,8		
Total (Valor Médio)	3,4	3,2	3,3	3,15	3,8	3,8	2,8	2,85	3,6	3,5

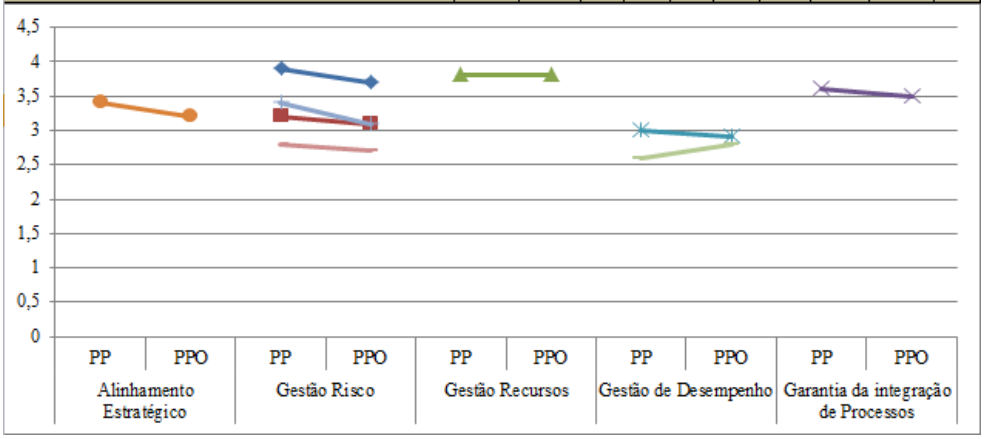


Gráfico 5.45- Factores Motivadores: Mapeamento ISACA (Gestor de Topo)

No entanto, para o Gestor de Topo o foco da inibição verifica-se nos elementos do pilar de resultados – "*Gestão de Recursos*", apresentando até (0,2) pontos de diferença entre a sua perspectiva e a sua perspectiva face à organização, isto é, do ponto de vista deste grupo profissional, a organização reflecte a inibição na adopção/implementação dum Sistema de Gestão da Segurança da Informação – apontando o elemento inibidor "*Valor do investimento*". A tabela/gráfico (Gráfico 5.46) seguinte mostra o acima referido.

Factores Inibidores (Nível médio de importância - Gestor de Topo)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Valor do investimento					3,4	3,6				
b) Falta de conhecimento									3,3	3,1
c) Cultura organizacional									2,9	3,1
d) Dificuldade em medir o custo/benefício							3,3	3,1		
e) Acesso restrito à "Gestão de Topo"	2,7	2,7								
f) Alterações contínuas na legislação / regulação			2,7	2,7						
g) Emergência contínua de novos riscos			3,2	3,1						
Total (Valor médio)	2,7	2,7	3	2,9	3,4	3,6	3,3	3,1	3,1	3,1

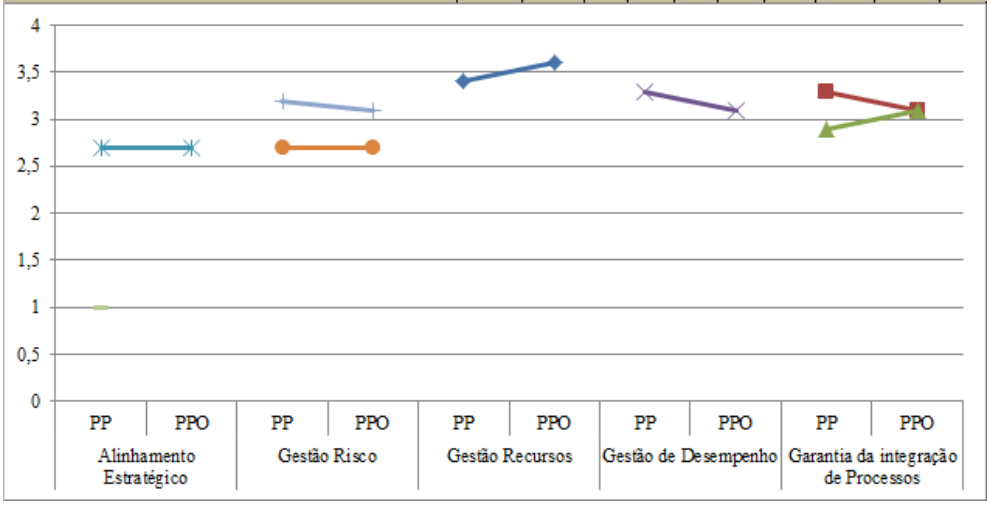


Gráfico 5.46- Factores Inibidores: Mapeamento ISACA (Gestor de Topo)

Já para o Gestor Intermédio verifica-se que o valor do nível médio de importância para o pilar de resultados – "*Alinhamento Estratégico*" desce para a quinta posição, mostrando um maior afastamento da visão da segurança da informação como um instrumento que permite a criação de mais-valias para a organização. Todavia, mantém-se na primeira posição o pilar de resultados – "*Gestão de Recursos*", indicando, também nesta categoria, uma motivação para a cultura de segurança da informação na perspectiva da protecção do activo. A tabela/gráfico (Gráfico 5.47) seguinte mostra o acima mencionado.

Factores Motivadores (Nível médio de importância - Gestor Intermédio)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Evitar perdas financeiras			3,7	3,5						
b) Ocorrência de incidente anterior			3,2	3,2						
c) Garantir a disponibilidade, confidencialidade e integridade da Informação					3,8	3,7				
d) Planear a segurança da informação antes da implementação das novas tecnologias									3,5	3,5
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança							3,3	3,3		
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	3,2	3,2								
g) Emergência contínua de novos riscos			3,6	3,5						
h) Alterações contínuas na legislação/regulação			3,2	3,3						
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.							3,2	3,2		
Total (Valor Médio)	3,2	3,2	3,4	3,4	3,8	3,7	3,25	3,25	3,5	3,5

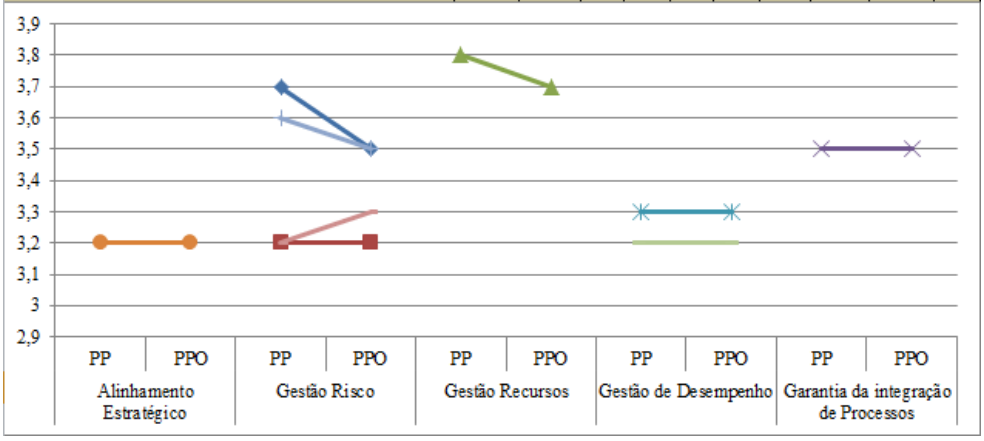


Gráfico 5.47- Factores Motivadores: Mapeamento ISACA (Gestor Intermédio)

Porém, relativamente aos Factores Inibidores, o Gestor Intermédio segue a tendência global e assinala três pilares de resultados: "*Gestão de Recursos*", "*Gestão de Desempenho*" e "*Garantia da integração de Processos*" como o centro da 'inibição´ na adopção/implementação dum Sistema de Gestão da Segurança da Informação, havendo contudo uma ligeira acentuação no elemento "*Dificuldade em medir o custo/benefício*", que colhe a mesma pontuação nas duas perspectivas. A tabela/gráfico (Gráfico 5.48) seguinte mostra o acima referido.

Factores Inibidores (Nível médio de importância - Gestor Intermédio)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Valor do investimento					3,3	3,5				
b) Falta de conhecimento									3,5	3,4
c) Cultura organizacional									3,4	3,3
d) Dificuldade em medir o custo/beneficio							3,5	3,5		
e) Acesso restrito à "Gestão de Topo"	2,9	3								
f) Alterações contínuas na legislação / regulação			3	3,1						
g) Emergência contínua de novos riscos			3,2	3,2						
Total (Valor médio)	2,9	3	3,1	3,15	3,3	3,5	3,5	3,5	3,45	3,35

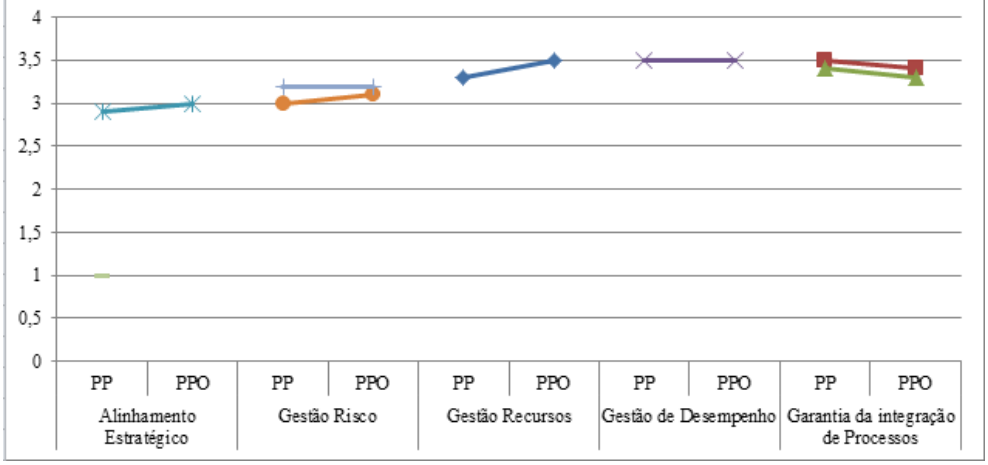


Gráfico 5.48- Factores Inibidores: Mapeamento ISACA (Gestor Intermédio)

Também os Gestores das TI apontam como principal motivação os elementos do pilar de resultados – "*Gestão de Recursos*", remetendo para terceira posição o pilar de resultados – "*Alinhamento Estratégico*". A tabela/gráfico (Gráfico 5.49) seguinte ilustra o mencionado.

Factores Motivadores (Nivel médio de importância - Gestor das TI)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Evitar perdas financeiras			3,6	3,6						
b) Ocorrência de incidente anterior			3	3						
c) Garantir a disponibilidade, confidencialidade e integridade da Informação					3,9	3,7				
d) Planear a segurança da informação antes da implementação das novas tecnologias									3,6	3,5
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança							3,3	3,2		
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	3,5	3,4								
g) Emergência contínua de novos riscos			3,3	3,1						
h) Alterações contínuas na legislação/regulação			2,9	3,1						
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.							3,2	3,1		
Total (Valor médio)	3,5	3,4	3,2	3,2	3,9	3,7	3,25	3,15	3,6	3,5

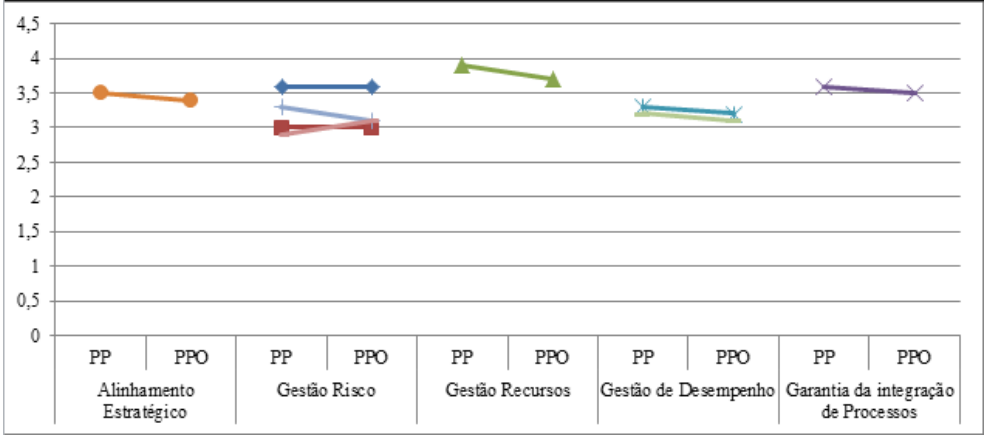


Gráfico 5.49- Factores Motivadores: Mapeamento ISACA (Gestor das TI)

Todavia, em relação aos Factores Inibidores, o Gestor das TI assiná-la um alinhamento com a posição do Gestor de Topo, dando realce ao pilar de resultados – "*Gestão de Recursos*" sobretudo quando refere a perspectiva do próprio face à organização, enfatizando o elemento inibidor "*Valor do investimento*". Contudo, quando refere a sua visão, realça o elemento inibidor "*Cultura organizacional*", colocando o enfoque no pilar de resultados – "*Garantia da integração de Processos*". A tabela/gráfico (Gráfico 5.50) seguinte mostra o acima referido.

Factores Inibidores (Nível médio de importância - Gestor TI)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Valor do investimento					3,2	3,4				
b) Falta de conhecimento									3,1	3
c) Cultura organizacional									3,4	3,2
d) Dificuldade em medir o custo/benefício							2,9	3,2		
e) Acesso restrito à "Gestão de Topo"	2,9	3								
f) Alterações contínuas na legislação / regulação			2,7	2,8						
g) Emergência contínua de novos riscos			2,8	2,8						
Total (Valor médio)	2,9	3	2,8	2,8	3,2	3,4	2,9	3,2	3,25	3,1

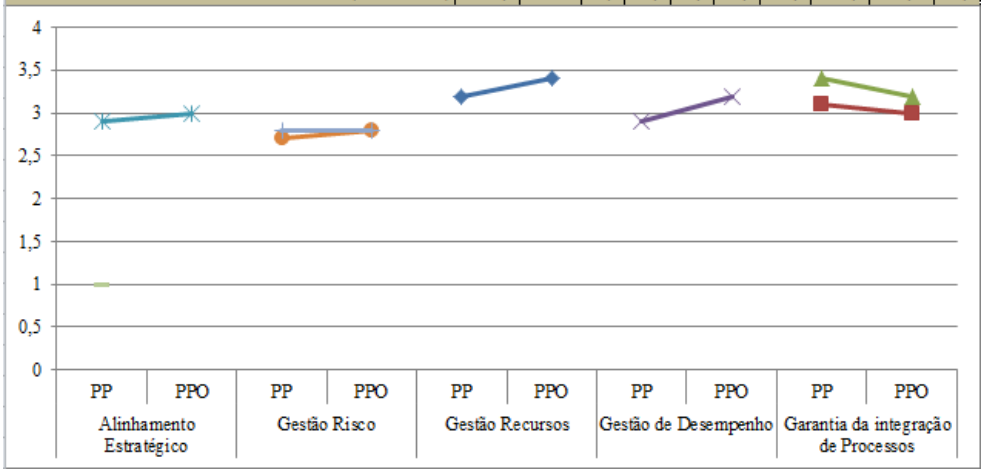


Gráfico 5.50- Factores Inibidores: Mapeamento ISACA (Gestor das TI)

O posicionamento dos Consultores das TI apresenta-se semelhante aos dos Gestores das TI, colocando o enfoque da motivação na adopção de Sistema de Gestão para a Segurança da Informação no pilar de resultados – "*Gestão de Recursos*", atribuindo também a terceira posição ao pilar de resultados – "*Alinhamento Estratégico*", o que denota, ainda, uma "não interiorização" do potencial da utilização deste "recurso" como basilar para o sector das Águas e Saneamento em Portugal. A tabela/gráfico (Gráfico 5.51) seguinte ilustra o acima mencionado.

Factores Motivadores (Nivel médio de importância - Consultor das TI)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Evitar perdas financeiras			3,5	3,5						
b) Ocorrência de incidente anterior			2,9	3						
c) Garantir a disponibilidade, confidencialidade e integridade da Informação					3,7	3,6				
d) Planear a segurança da informação antes da implementação das novas tecnologias									3,4	3,4
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança							3	2,9		
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	3,3	3,3								
g) Emergência contínua de novos riscos			3,3	3,3						
h) Alterações contínuas na legislação/regulação			2,9	2,9						
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.							2,9	3		
Total (Valor médio)	3,3	3,3	3,2	3,18	3,7	3,6	2,95	2,95	3,4	3,4

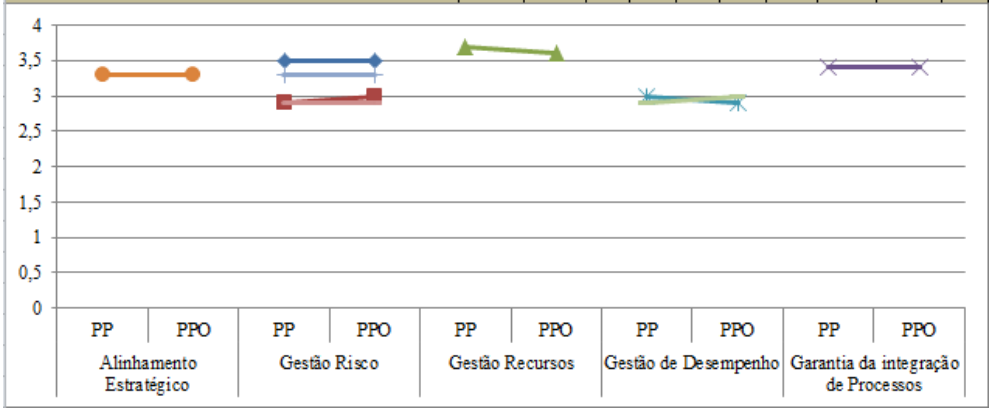


Gráfico 5.51- Factores Motivadores: Mapeamento ISACA (Consultor das TI)

Relativamente aos Factores Inibidores, verifica-se para esta classe - Consultor das TI, o realce no pilar de resultados – "*Gestão de Recursos*" com o enfoque no elemento inibidor "*Valor do Investimento*". A tabela/gráfico (Gráfico 5.52) seguinte mostra o acima referido.

Factores Inibidores (Nível médio de importância - Consultor das TI)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Valor do investimento					3,2	3,2				
b) Falta de conhecimento									3,1	2,9
c) Cultura organizacional									3,1	3
d) Dificuldade em medir o custo/benefício							3,1	2,9		
e) Acesso restrito à "Gestão de Topo"	2,5	2,6								
f) Alterações contínuas na legislação / regulação			2,4	2,3						
g) Emergência contínua de novos riscos			2,3	2,2						
Total (Valor médio)	2,5	2,6	2,4	2,25	3,2	3,2	3,1	2,9	3,1	2,95

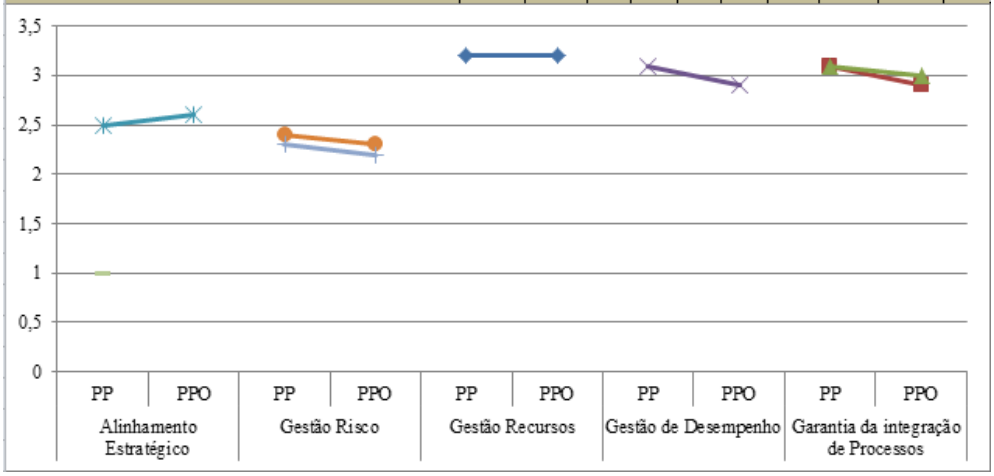


Gráfico 5.52- Factores Inibidores: Mapeamento ISACA (Consultor das TI)

O grupo profissional "Gestor/Funcionário da Segurança" também coloca o foco da motivação nos elementos pertencentes ao pilar de resultados – "*Gestão de Recursos*". Contudo, é este grupo que posiciona o pilar de resultados – "*Alinhamento Estratégico*" na melhor posição, classificando-a em segundo lugar. Neste sentido, pode-se inferir que a motivação deste grupo profissional para a adopção de um Sistema de Gestão de Segurança da Informação aproxima-se melhor da visão da cultura de segurança da informação mais direccionada, não somente à protecção dos activos, mas também como alavanca para a criação de valor para as organizações. A tabela/gráfico (Gráfico 5.53) seguinte ilustra o acima mencionado.

Factores Motivadores (Nível médio de importância - Gestor/Funcionário da Segurança)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Evitar perdas financeiras			3,7	3,7						
b) Ocorrência de incidente anterior			3,3	3,3						
c) Garantir a disponibilidade, confidencialidade e integridade da Informação					4	4				
d) Planear a segurança da informação antes da implementação das novas tecnologias									3,3	3,7
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança							3,7	4		
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	3,7	3,7								
g) Emergência contínua de novos riscos			3,7	3,7						
h) Alterações contínuas na legislação/regulação			3,3	3,3						
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.							2,7	2,3		
Total (Valor médio)	3,7	3,7	3,5	3,5	4	4	3,2	3,15	3,3	3,7

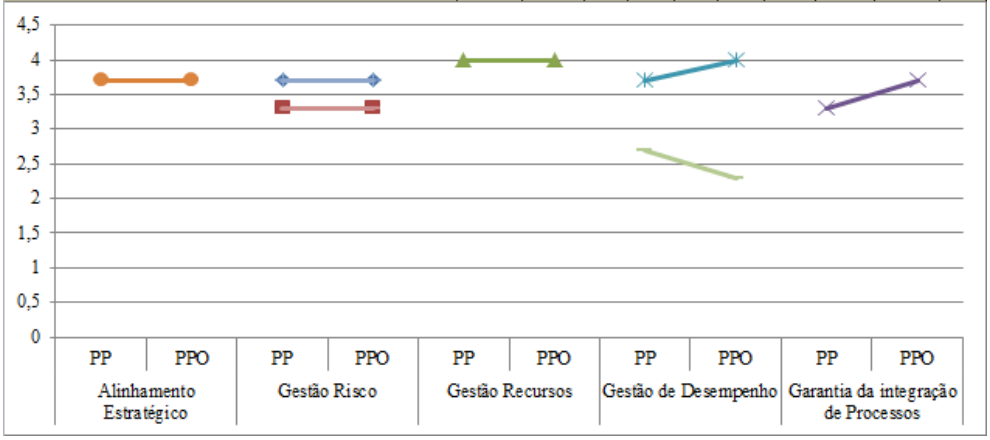


Gráfico 5.53- Factores Motivadores: Mapeamento ISACA (Gestor/Funcionário de Segurança)

Contudo, para este "Gestor/Funcionário da Segurança" verifica-se que em relação aos Factores Inibidores, o relevo cai sobre o pilar de resultados – "*Gestão de Desempenho*", onde o elemento inibidor "*Dificuldade em medir o custo/benefício*" adquire especial pontuação, verificando-se um alinhamento de opinião ao Gestor Intermédio. A tabela/gráfico (Gráfico 5.54) seguinte mostra o acima referido.

Factores Inibidores (Nivel médio de importância - Gestor/Funcionário da Segurança)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Valor do investimento					2,7	2,7				
b) Falta de conhecimento									3	3,3
c) Cultura organizacional									3	3
d) Dificuldade em medir o custo/benefício							3,7	3,7		
e) Acesso restrito à "Gestão de Topo"	3,3	3,3								
f) Alterações contínuas na legislação / regulação			3	3						
g) Emergência contínua de novos riscos			3,3	3,3						
Total (Valor médio)	3,3	3,3	3,2	3,15	2,7	2,7	3,7	3,7	3	3,15

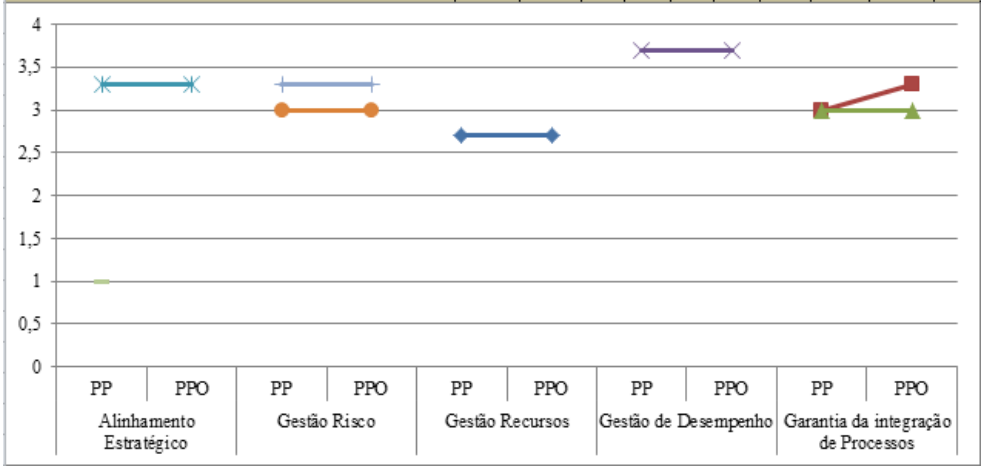


Gráfico 5.54- Factores Inibidores: Mapeamento ISACA (Gestor/Funcionário de Segurança)

Por último, mas não mesmo importante apresenta-se o posicionamento do grupo "Trabalhador", que mantém o foco das preferências motivadoras no pilar de resultados – "*Gestão de Recursos*". Porém, o pilar de resultados – "*Alinhamento Estratégico*" colhe a terceira posição, reflectindo o mesmo padrão organizacional. A tabela/gráfico (Gráfico 5.55) seguinte ilustra o acima mencionado.

Factores Motivadores (Nível médio de importância - Trabalhador)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Evitar perdas financeiras			3,5	3,4						
b) Ocorrência de incidente anterior			3,3	3,3						
c) Garantir a disponibilidade, confidencialidade e integridade da Informação					3,8	3,7				
d) Planear a segurança da informação antes da implementação das novas tecnologias									3,6	3,6
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança							3,3	3,2		
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	3,4	3,4								
g) Emergência contínua de novos riscos			3,4	3,5						
h) Alterações contínuas na legislação/regulação			3,1	3,2						
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.							3,4	3,4		
Total (Valor médio)	3,4	3,4	3,3	3,35	3,8	3,7	3,35	3,3	3,6	3,6

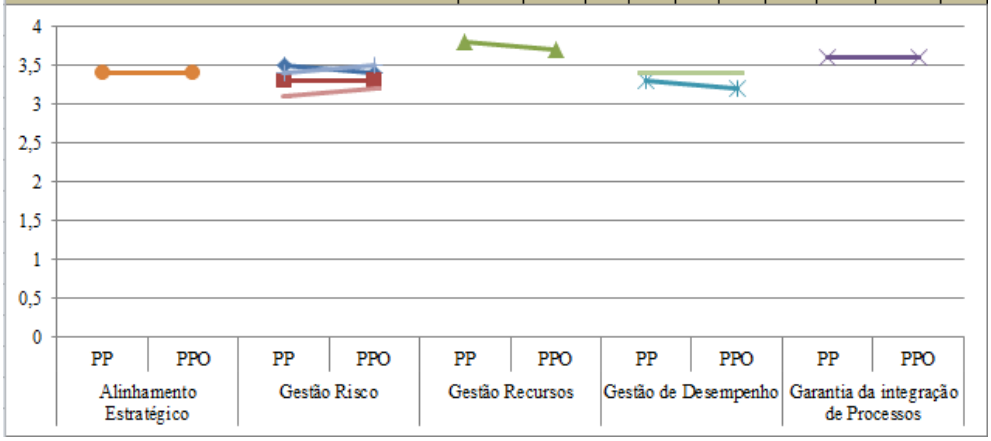


Gráfico 5.55- Factores Motivadores: Mapeamento ISACA (Trabalhador)

No entanto, este grupo profissional - Trabalhador revela, nos Factores Inibidores, o seu foco no pilar de resultados – "*Garantia da integração de Processos*", indicando os elementos inibidores relacionados com o ´factor humano´: "*Falta de conhecimento*" e "*Cultura organizacional*". A tabela/gráfico (Gráfico 5.56) seguinte mostra o acima referido.

Factores Inibidores (Nivel médio de importância - Trabalhador)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Valor do investimento					3,2	3,2				
b) Falta de conhecimento									3,5	3,4
c) Cultura organizacional									3,5	3,4
d) Dificuldade em medir o custo/benefício							3,3	3,3		
e) Acesso restrito à "Gestão de Topo"	3	2,9								
f) Alterações contínuas na legislação / regulação			2,9	3						
g) Emergência contínua de novos riscos			2,9	2,9						
Total (Valor médio)	3	2,9	2,9	2,95	3,2	3,2	3,3	3,3	3,5	3,4

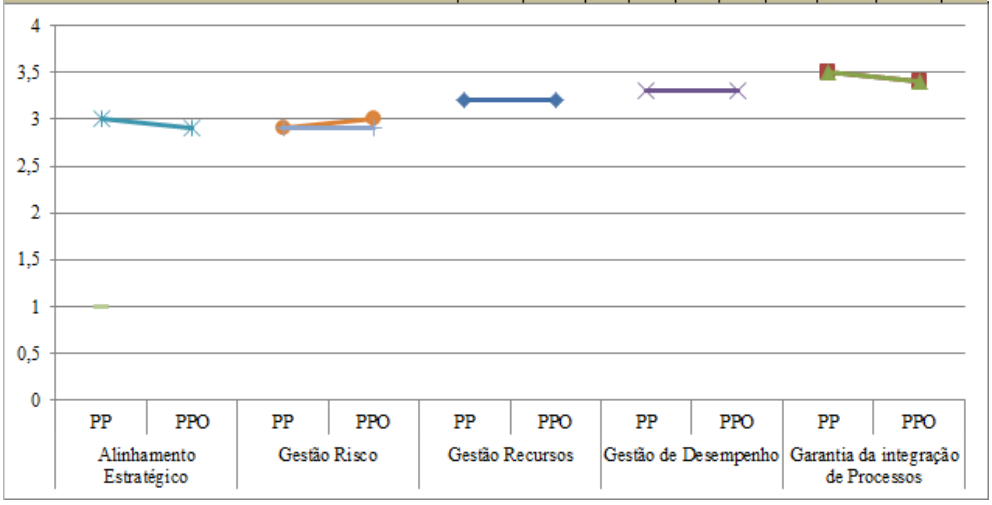


Gráfico 5.56- Factores Inibidores: Mapeamento ISACA (Trabalhador)

5.2 – Factores Críticos de Sucesso

5.2.1 - Caracterização da Amostra

Nesta parte mostram-se as deduções tiradas por meio do raciocínio representando no modelo de resultados (Figura 5.8) e referentes aos factores considerados críticos de sucesso na adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização.

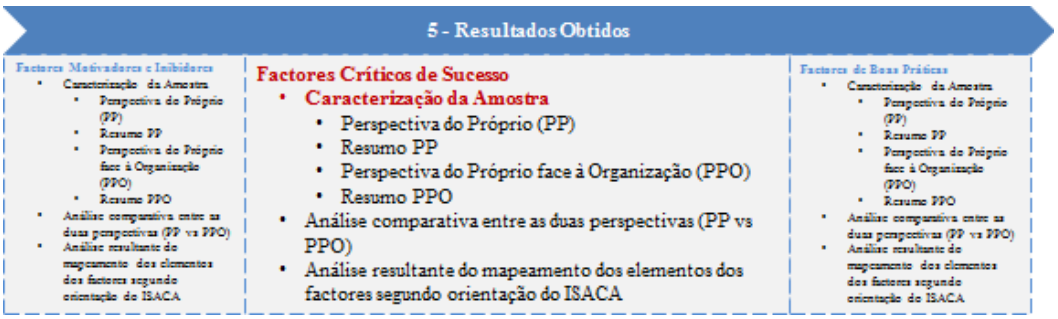


Figura 5.8- Modelo dos Resultados Obtidos: FCS

Assim, recorde-se que foram expostos aos respondentes, como Factores Críticos de Sucesso os seguintes elementos:

a) Entendimento da "Gestão de Topo" para as questões da segurança da informação

b) Suporte da Gestão de Topo

c) Responsabilização pela Segurança da Informação

d) Motivação dos funcionários

e) Programas para a conscientização, educação e formação em segurança em informação

f) Conformidade com Normas Internacionais de Segurança

g) Auditorias de Segurança da Informação

h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)

i) Política de Segurança da Informação

j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)

Deste modo, a análise de dados teve em conta a classificação (percentagem) do grau de importância dada pelos respondentes, incluindo as duas perspectivas: a do próprio e a do próprio face à organização. De modo a aferir a existência ou não de desvios entre as duas vistas, foi realizada a comparação entre as mesmas. Para isso, efectuou-se o cálculo do nível médio de importância, para cada elemento deste factor.

5.2.2 – Perspectiva do Próprio

Neste ponto e de acordo com a observação seguida conforme indicado na figura (Figura 5.9) abaixo, revelam-se os resultados deste ponto de vista, conseguidos por meio do tratamento dos dados efectuados às respostas obtidas na décima terceira questão do questionário elaborado (ver Anexo A).

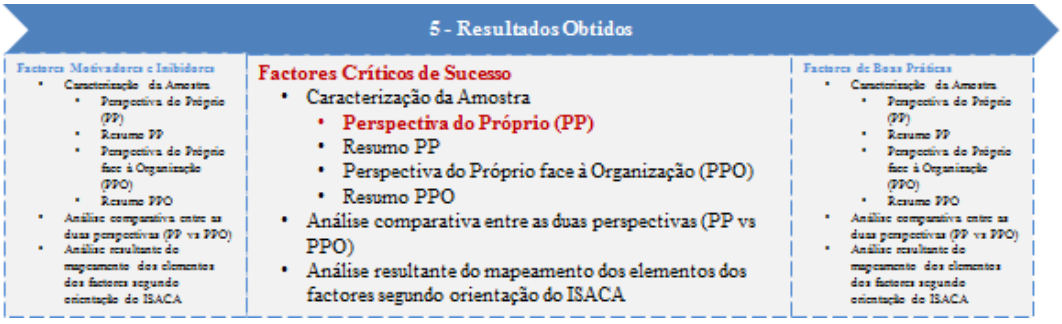


Figura 5.9- Modelo dos Resultados Obtidos: FCS/PP

Neste contexto, numa primeira fase, analisou-se a totalidade das respostas, verificando-se que, para este factor, e, de uma forma global, os dez elementos considerados como críticos de

sucesso foram classificados nas categorias “Muito importante” ou “Importante”, havendo uma predominância da categoria “Importante”.

Nesta última, seis dos dez elementos críticos de sucesso considerados obtêm votações acima da metade percentual (50,00%) e quatro dos dez elementos surgem seleccionados na categoria “Muito importante”, também, com valores percentuais significativos (superiores a 50,00%).

Contudo, os elementos críticos de sucesso mais votados na categoria “Muito importante” são: “*Entendimento da Gestão de Topo para as questões da segurança da informação*” (61,16%), “*Suporte da Gestão de Topo*” (54,55%), “*Responsabilização pela Segurança da Informação*” e “*Motivação dos funcionários*” que aparecem com valores iguais (53,72%).

Na categoria “Importante” revelam-se cinco elementos críticos de sucesso mais seleccionados, a saber: “*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*” (66,12%), “*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*” (59,50%), “*Auditorias de Segurança da Informação*” (55,37%), “*Política de Segurança da Informação*” (54,55%) e “*Conformidade com Normas Internacionais de Segurança*” (52,89%),

Porém, os três elementos mais votados na categoria “Pouco Importante” são três dos seis elementos apontados na categoria “Importante”, nomeadamente: “*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*” (15,70%), “*Conformidade com Normas Internacionais de Segurança*” (13,22%) e “*Auditorias de Segurança da Informação*” (12,40%).

Na categoria “Não é importante” são mencionados, com igualdade de pontuação (0,83%) dois dos dez elementos críticos de sucesso: “*Programas para a conscientização, educação e formação em segurança em informação*” e “*Conformidade com Normas Internacionais de Segurança*”. No gráfico (Gráfico 5.57) seguinte encontra-se o pormenor do anteriormente mencionado.

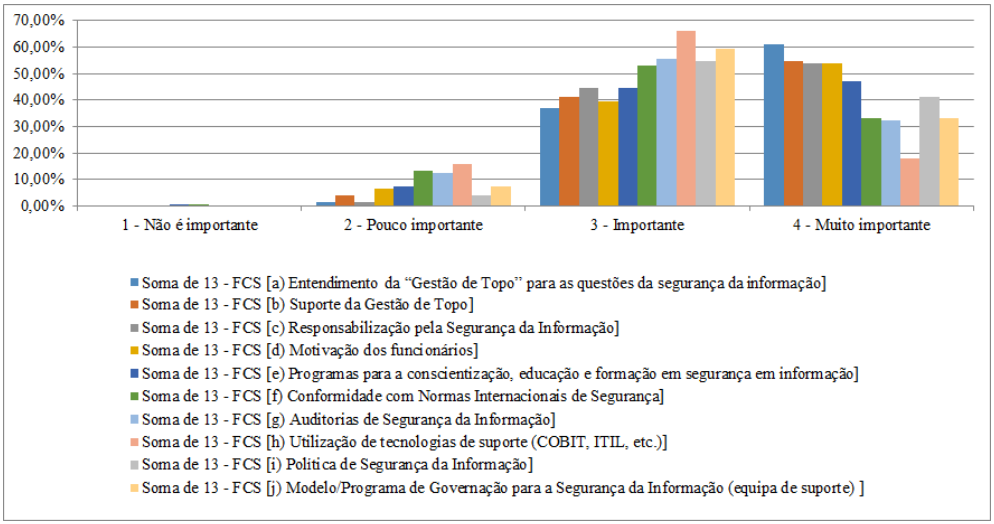


Gráfico 5.57- Factores Críticos de Sucesso - PP (Global)

Numa segunda fase, foram analisadas as respostas dos participantes, tendo em conta a sua função, uma vez que, assim, poder-se-ia encontrar mais algumas vistas para este factor, ou seja, que elementos são considerados como Factores Críticos de Sucesso na implementação/adopção de um SGSI para um Gestor de Topo? E para um Gestor Intermédio? E para um Gestor das TI? E para um Consultor das TI? E para um Gestor / Funcionário da Segurança? E para um Trabalhador? Após a procura, obteve-se os seguintes resultados.

Do ponto de vista do Gestor de Topo - conforme gráfico (Gráfico 5.58) a seguir, comprova-se que todos os elementos são considerados como Factores Críticos de Sucesso e classificados com valores acima da metade percentual (50,00%), quando somados os valores nas categorias "Muito importante" ou "Importante, situando-se o enfoque da votação na categoria "Importante".

Por um lado, cinco dos dez elementos críticos de sucesso considerados, nomeadamente, "*Suporte da Gestão de Topo*", "*Responsabilização pela Segurança da Informação*", "*Motivação dos funcionários*", "*Política de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" atingem o total da votação (100,00%), quando somados os resultados percentuais nas categorias "Muito importante" e "Importante".

Por outro lado, o elemento "*Entendimento da Gestão de Topo para as questões da segurança da informação*" é o mais votado (90,00%), como factor crítico de sucesso na categoria "Muito Importante".

Porém, na categoria "Importante", os respondentes seleccionam, igualmente (70,00%), os seguintes elementos: "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" e "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*".

Note-se que, para este grupo profissional, nenhum dos elementos considerados é classificado na categoria "Não é importante".

Todavia, o elemento "*Conformidade com Normas Internacionais de Segurança*" é classificado na categoria "Pouco importante" (20,00%).

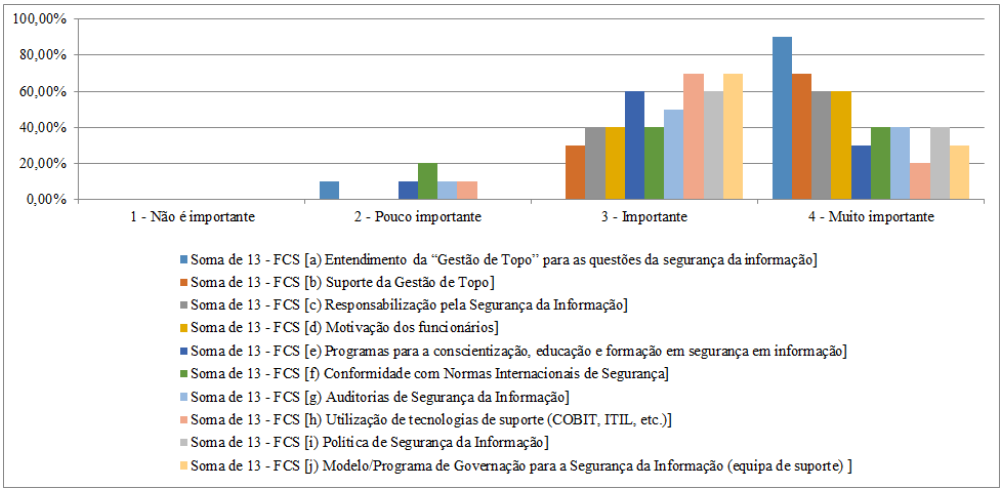


Gráfico 5.58- Factores Críticos de Sucesso - PP (Gestor de Topo)

Do ponto de vista do Gestor Intermédio – conforme gráfico (Gráfico 5.59) seguinte, verifica-se que todos os elementos são considerados como Factores Críticos de Sucesso e classificados com valores acima da metade percentual (50,00%), quando somados os valores nas categorias "Muito importante" ou "Importante, situando-se o enfoque da votação na categoria "Importante".

Contudo, três dos dez elementos, designadamente, "*Entendimento da Gestão de Topo para as questões da segurança da informação*", "*Suporte da Gestão de Topo*" e "*Responsabilização pela Segurança da Informação*", atingem o total da votação (100,00%), quando somados os resultados percentuais nas categorias "Muito importante" e "Importante". É de notar, que o elemento crítico de sucesso "*Motivação dos funcionários*" é pontuado de igual forma (46,15%) nas duas categorias.

Na categoria "Importante", o elemento crítico de sucesso "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" surge como o mais votado (76,92%).

Todavia, comprova-se que os gestores intermédios na categoria "Pouco importante" apontam como elemento crítico de sucesso mais votado a "*Utilização de tecnologias de suporte (COBIT,*

ITIL, etc.)" (19,23%) e votam, ainda, na categoria "Não é importante", num único elemento: "*Conformidade com Normas Internacionais de Segurança*" (3,85%).

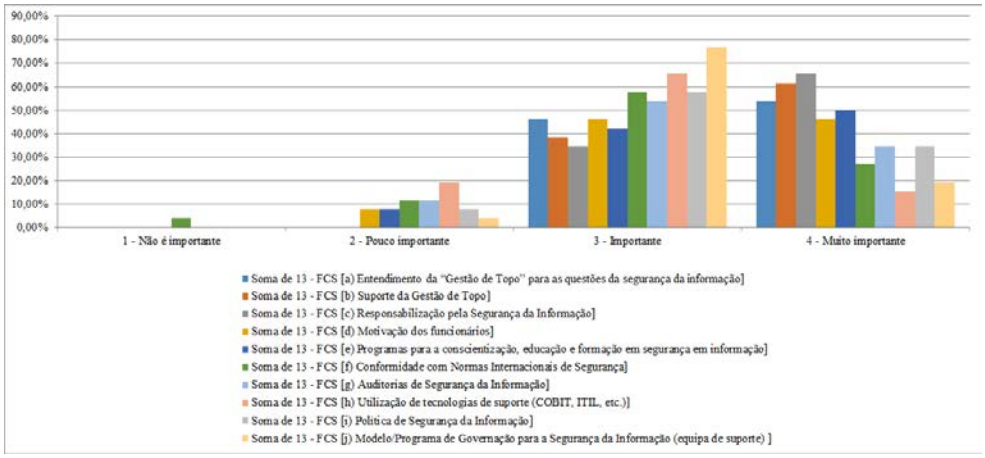


Gráfico 5.59- Factores Críticos de Sucesso - PP (Gestor Intermédio)

Do ponto de vista do Gestor das TI – neste grupo profissional, os elementos considerados como Factores Críticos de Sucesso surgem sempre maioritariamente populados nas categorias "Muito importante" e "Importante", notando-se um enfoque na categoria "Importante". Nesta categoria, oito, dos dez elementos, obtêm valores superiores à metade percentual (50,00%).

De realçar que, quatro dos dez elementos críticos de sucesso considerados, nomeadamente, "*Entendimento da Gestão de Topo para as questões da segurança da informação*", "*Suporte da Gestão de Topo*", "*Responsabilização pela Segurança da Informação*" e "*Programas para a conscientização, educação e formação em segurança em informação*", atingem a totalidade da votação (100,00%), quando somados os resultados percentuais nas categorias "Muito importante" e "Importante".

Para este gestor, nota-se que o elemento crítico de sucesso "*Entendimento da Gestão de Topo para as questões da segurança da informação*" (64,71%) é o mais votado na categoria "Muito importante". Com o mesmo valor, mas na categoria "Importante" mostram-se também mais três elementos: "*Motivação dos funcionários*", "*Programas para a conscientização, educação e formação em segurança em informação*" e "*Auditorias de Segurança da Informação*". Porém, o elemento crítico de sucesso mais votado nesta categoria é "*Conformidade com Normas Internacionais de Segurança*" (70,59%).

Na categoria "Pouco Importante", este grupo profissional, aponta como elemento crítico de sucesso mais votado a "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" (17,65%).

Na categoria "Não é importante" não é indicado nenhum elemento. No gráfico (Gráfico 5.60) a seguir ilustra-se o atrás mencionado.

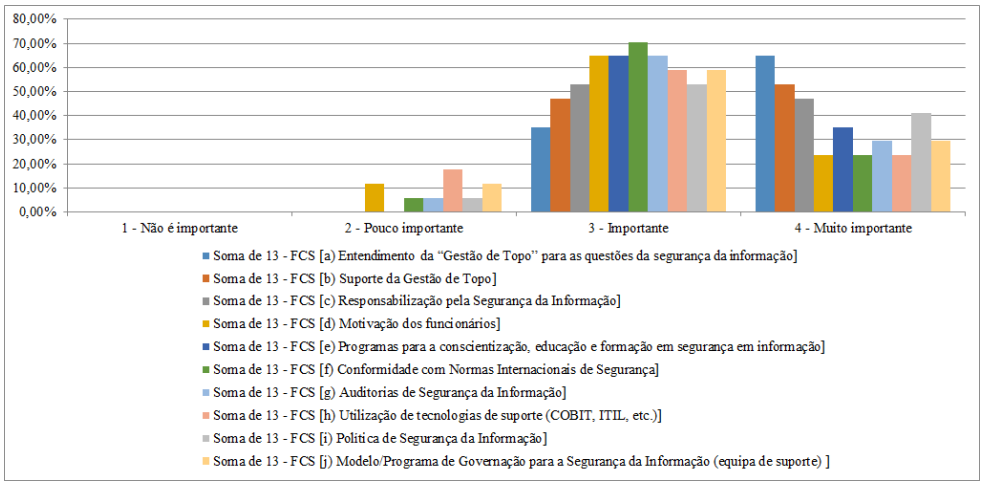


Gráfico 5.60- Factores Críticos de Sucesso - PP (Gestor das TI)

Do ponto de vista do Consultor das TI – nesta perspectiva verifica-se, novamente, que os dez elementos críticos de sucesso considerados agrupam, maioritariamente, as preferências de votação nas categorias "Muito importante" e "Importante", embora o enfoque esteja, mais uma vez, na categoria "Importante".

Todavia, este grupo profissional destaca o elemento crítico de sucesso "*Entendimento da Gestão de Topo para as questões da segurança da informação*" atribuindo-lhe a maior votação (71,43%) na categoria "Muito importante", sendo também este o valor mais votado de todas as categorias. Este mesmo elemento e o elemento "*Suporte da Gestão de Topo*" agregam o total da votação (100,00%), quando somados os valores nas categorias "Muito importante" e "Importante". Relativamente a este último elemento mencionado, as opiniões, neste grupo profissional, encontram-se igualmente divididas, visto que cada categoria agrega metade (50,00%) das votações.

Na categoria "Importante", o elemento crítico de sucesso mais votado é "*Conformidade com normas internacionais de segurança*" que agrupa maioritariamente as preferências (64,29%).

Relativamente à categoria "Pouco importante" aparecem oito dos dez elementos populados, surgindo, como mais votados, os elementos críticos de sucesso "*Auditorias de Segurança da Informação*" e "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" que apresentam a mesma classificação percentual (28,57%).

Na categoria "Não é importante" é apenas votado um elemento crítico de sucesso "*Programas para a conscientização, educação e formação em segurança em informação*" (7,14%). O gráfico (Gráfico 5.61) seguinte mostra o acima referido.

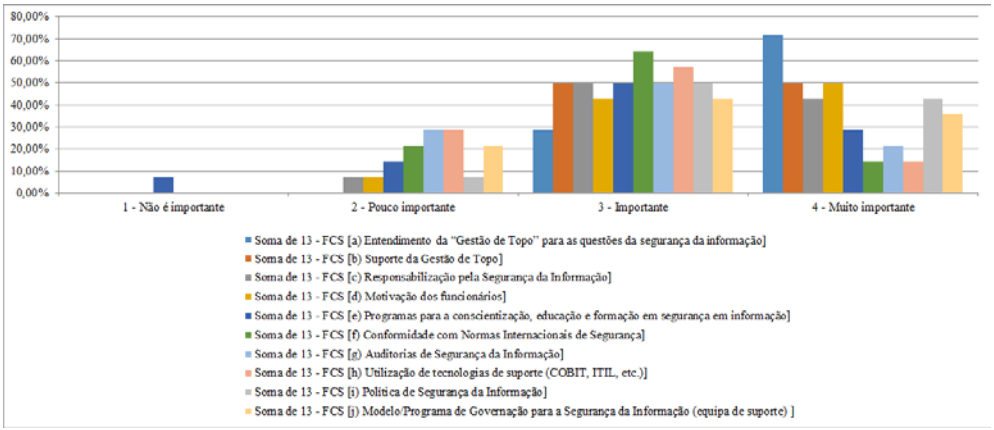


Gráfico 5.61- Factores Críticos de Sucesso - PP (Consultor das TI)

Do ponto de vista do Gestor / Funcionário da Segurança – esta classe apresenta uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). Todos os elementos surgem com votação nas categorias "Muito importante" e "Importante", não aparecendo populadas as categorias "Pouco importante" e "Não é importante".

Contudo, na categoria "Importante" existem dois elementos críticos de sucesso que obtêm a totalidade da votação (100,00%): "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Política de Segurança da Informação*".

O gráfico (Gráfico 5.62) seguinte mostra o acima indicado.

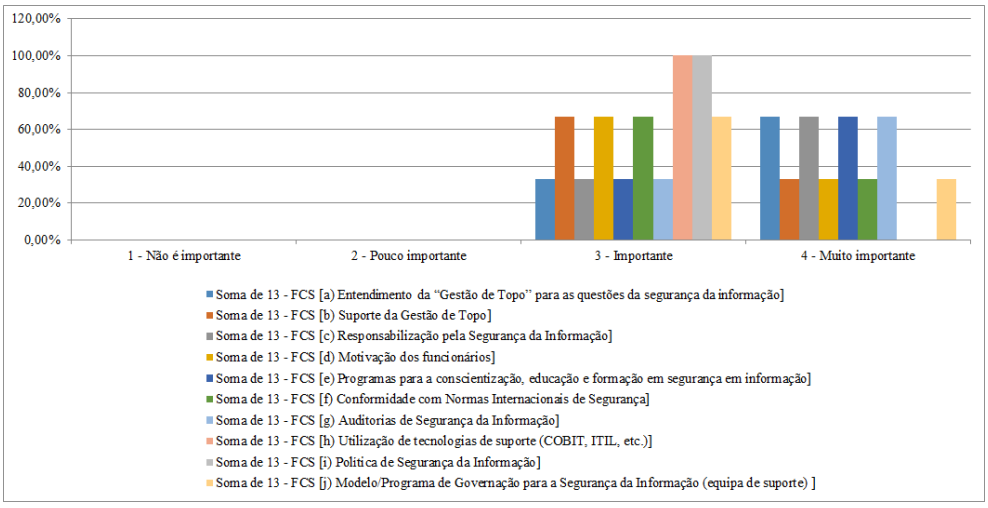


Gráfico 5.62- Factores Críticos de Sucesso - PP (Gestor/Funcionário de Segurança)

Do ponto de vista do Trabalhador – nesta perspectiva, cinco dos dez elementos críticos de sucesso considerados, encontram-se com prevalência da votação, apresentando valores superiores à metade percentual (50,00%) na categoria "Muito importante". O mais votado é "*Motivação dos funcionários*" (68,63%). Com esta mesma votação, mas na categoria "Importante" aparece o elemento crítico de sucesso "*Utilização de tecnologias de suporte*

(COBIT, ITIL, etc.)". Ainda nesta categoria, este grupo selecciona quatro dos dez elementos atribuindo-lhes votações significativas (superiores a 50,00%), a saber: "*Auditorias de Segurança da Informação*" (56,86%), "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" (68,63%), "*Política de Segurança da Informação*" (50,98%) e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*"(52,94%).

Por outro lado, na categoria "Pouco importante" todos os elementos surgem populados. Porém, o elemento crítico de sucesso que agrupa maior pontuação é "*Conformidade com normas internacionais de segurança*" (13,73%) seguido dos elementos "*Auditorias de Segurança da Informação*" e "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*", os quais obtêm classificação idêntica (11,76%).

Na categoria "Não é importante" não existem elementos populados. O gráfico (Gráfico 5.63) seguinte mostra o acima exposto.

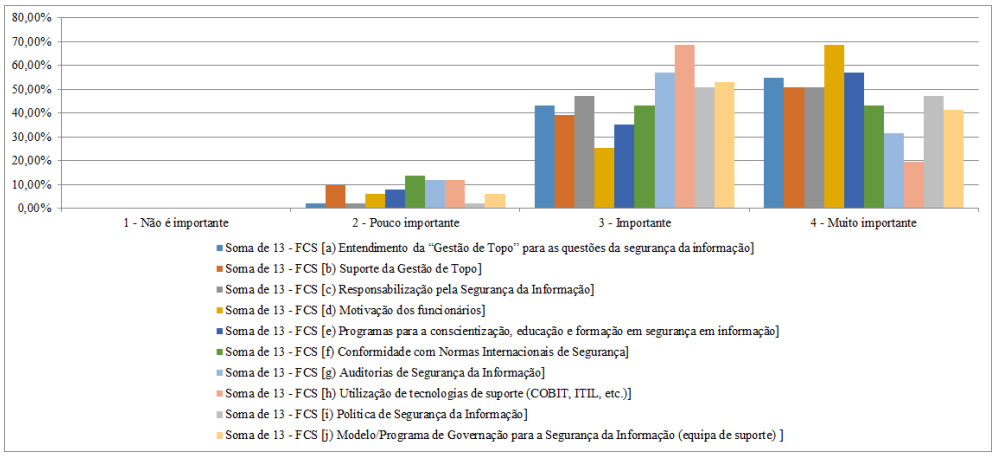


Gráfico 5.63- Factores Críticos de Sucesso - PP (Trabalhador)

5.2.3 – Resumo da Perspectiva do Próprio

Nesta parte e conforme ilustrado na figura abaixo (Figura 5.10), segue-se a síntese dos resultados obtidos da análise dos Factores Críticos de Sucesso segundo a perspectiva do próprio.

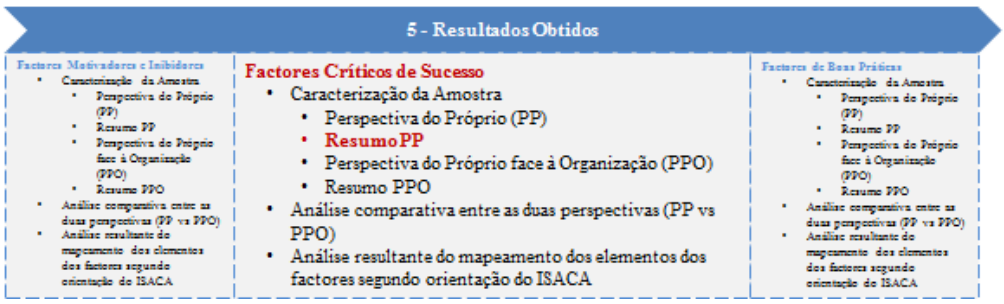


Figura 5.10- Modelo dos Resultados Obtidos: FCS/Resumo da PP

Resumindo, na tabela (Tabela 5.19) seguinte apresenta-se a ordenação pela categoria "Muito importante" e "Não é importante" dos elementos considerados para o estudo como Factores Críticos de Sucesso, segundo cada uma das vistas dadas pela função do respondente.

Desta forma, conforme se pode visualizar, o elemento crítico de sucesso "*Entendimento da "Gestão de Topo" para as questões da segurança da informação*" é o mais referido em primeiro lugar na categoria "Muito importante". Porém, o gestor intermédio e o trabalhador colocam-no em terceiro lugar. Todavia, o gestor intermédio selecciona, em primeiro lugar, o elemento crítico de sucesso "*Responsabilização pela Segurança da Informação*" e o Trabalhador aponta, preferencialmente, o elemento "*Motivação dos funcionários*".

Relativamente ao segundo elemento crítico de sucesso mais referenciado, revela-se o elemento "*Suporte da Gestão de Topo*" que é seleccionado por todos os grupos funcionais com excepção do Trabalhador que vota, para esta posição, no elemento "*Programas para a conscientização, educação e formação em segurança em informação*".

Verifica-se, ainda, que na categoria "Não é importante" é, apenas, apontado o elemento crítico de sucesso "*Conformidade com Normas Internacionais de Segurança*" pelos gestores intermédios e o elemento "*Programas para a conscientização, educação e formação em segurança em informação*" é referido pelo Consultor das TI.

Factores Críticos de Sucesso - PP (- Elemento não é referido pelos respondentes)		13 - FCS [a] Entendimento da "Gestão de Topo" para as questões da segurança da informação]	13 - FCS [b] Suporte da Gestão de Topo]	13 - FCS [c] Responsabilização pela Segurança da Informação]	13 - FCS [d] Motivação dos funcionários]	13 - FCS [e] Programas para a conscientização, educação e formação em segurança em informação]	13 - FCS [f] Conformidade com Normas Internacionais de Segurança]	13 - FCS [g] Auditorias de Segurança da Informação]	13 - FCS [h] Utilização de tecnologias de suporte (COBIT, ITIL, etc.)]	13 - FCS [i] Política de Segurança da Informação]	13 - FCS [j] Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)]
Gestor de Topo	Muito importante	1	2	3	3	5	4	4	6	4	5
	Não é importante	-	-	-	-	-	-	-	-	-	-
Gestor Intermédio	Muito importante	3	2	1	5	4	7	6	9	6	8
	Não é importante	-	-	-	-	-	1	-	-	-	-
Gestor das TI	Muito importante	1	2	3	7	5	7	6	7	4	6
	Não é importante	-	-	-	-	-	-	-	-	-	-
Consultor das TI	Muito importante	1	2	3	2	5	7	6	7	3	4
	Não é importante	-	-	-	-	1	-	-	-	-	-
Gestor / Funcionário da Segurança	Muito importante	1	2	1	2	1	2	1	-	-	2
	Não é importante	-	-	-	-	-	-	-	-	-	-
Trabalhador	Muito importante	3	4	4	1	2	6	8	9	5	7
	Não é importante	-	-	-	-	-	-	-	-	-	-
Global	**Muito importante**	**1**	**2**	**3**	**3**	**4**	**6**	**7**	**8**	**5**	**6**
	Não é importante	-	-	-	-	**1**	**1**	-	-	-	-

Tabela 5.19- Factores Críticos de Sucesso - PP: Ordenação das preferências

5.2.4 – Perspectiva do Próprio face à Organização

Neste item, seguindo a linha de orientação da apresentação dos resultados (Figura 5.11), esclarecem-se os resultados obtidos para este ponto de vista, referindo-se ao tratamento dos dados efectuados às respostas alcançadas na décima quarta questão do questionário elaborado (ver Anexo A).

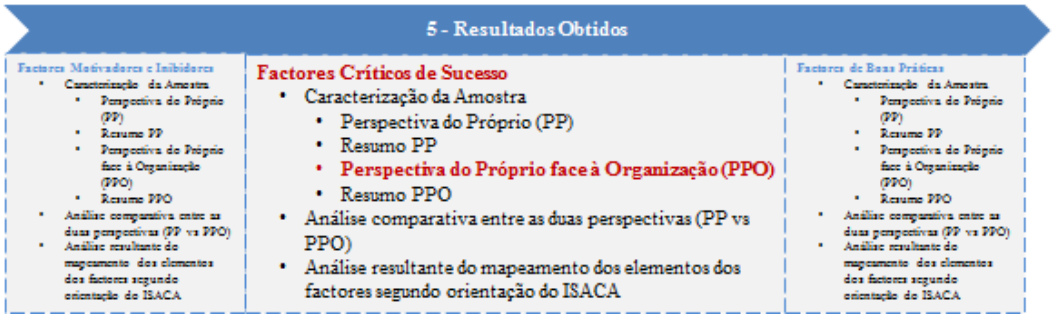


Figura 5.11- Modelo dos Resultados Obtidos: FCS/Perspectiva do PPO

Assim, numa primeira fase, analisou-se a totalidade das respostas, verificando-se que, para este factor e, de uma forma global, os dez elementos críticos de sucesso atrás identificados são classificados nas categorias "Muito importante" ou "Importante", havendo uma predominância na categoria "Importante". Nesta última, cinco dos dez elementos críticos de sucesso obtêm votações acima da metade percentual (50,00%) e quatro dos mesmos aparecem seleccionados na categoria "Muito importante", também, com valores percentuais superiores à metade (50,00%).

Contudo, os elementos críticos de sucesso mais votados na categoria "Muito importante" são: "Entendimento da Gestão de Topo para as questões da segurança da informação" (59,50%), "Suporte da Gestão de Topo" e a "Responsabilização pela Segurança da Informação", com idêntica pontuação (52,89%) e "Motivação dos funcionários" mostra-se com o valor dentro da mesma gama (50,41%).

Na categoria "Importante" encontram-se os seguintes cinco elementos críticos de sucesso mais seleccionados, a saber: "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" (62,81%), "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" (60,33%), "*Política de Segurança da Informação*" (58,68%), "*Conformidade com Normas Internacionais de Segurança*" (57,85%) e "*Auditorias de Segurança da Informação*" (57,02%).

Porém, os dois elementos críticos de sucesso mais votados na categoria "Pouco Importante" são: "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" (19,01%) e "*Motivação dos funcionários*" (13,22%), sendo o primeiro elemento mencionado, um dos mais bem classificados na categoria "Importante" e o segundo, um dos mais indicados na categoria "Muito importante".

Na categoria “Não é importante” surgem seis dos dez elementos críticos de sucesso, sendo estes, no entanto, populados, cada um, com valores pouco significativos (inferiores a 2,00%). O gráfico (Gráfico 5.50) seguinte mostra o acima exposto.

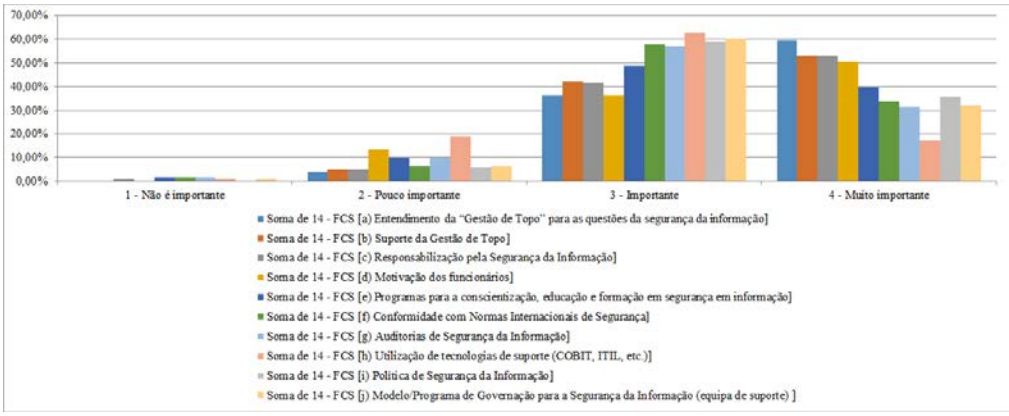


Gráfico 5.64- Factores Críticos de Sucesso: PPO (Global)

Numa segunda fase, analisou-se as respostas dos participantes, tendo em conta a sua função, de forma a, eventualmente, encontrar perfis de selecção diferentes para este factor, ou seja, que elementos são considerados como Factores Críticos de Sucesso na implementação/adopção de um SGSI para um Gestor de Topo? E para um Gestor Intermédio? E para um Gestor das TI? E para um Consultor das TI? E para um Gestor / Funcionário da Segurança? E para um Trabalhador? Analisou-se e obteve-se os seguintes resultados.

Do ponto de vista do Gestor de Topo - conforme gráfico (Gráfico 5.65) a seguir, comprova-se que todos os elementos são considerados como Factores Críticos de Sucesso e classificados com percentagens significativas (acima dos 80,00%), quando somados os valores nas categorias “Muito importante” ou “Importante, pois que, em cinco dos elementos, as preferências situam-se na categoria “Muito importante” e, nas outras cinco, a maioria da votação encontra-se na categoria “Importante”.

Por outro lado, o elemento mais votado entre os Factores Críticos de Sucesso na categoria “Muito Importante” é: “*Entendimento da Gestão de Topo para as questões da segurança da informação*” (80,00%). Mas, este elemento também aparece como o mais votado na categoria “Pouco importante” (20,00%). Nesta categoria aparecem, igualmente pontuados (10,00%), oito dos dez elementos críticos de sucesso considerados.

Na categoria “Importante” são seleccionados pelos respondentes os seguintes elementos críticos de sucesso: “*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*” e “*Política de Segurança da Informação*”, apresentando igual votação (70,00%). Contudo, este último elemento atinge a

totalidade (100,00%) da votação, quando somadas as preferências indicadas na categoria "Muito importante" (30,00%) e "Importante" (70,00%).

Neste grupo profissional, cinco dos dez elementos críticos de sucesso considerados obtêm, ainda, iguais votações (10,00%) na categoria "Não é importante": "*Programas para a conscientização, educação e formação em segurança em informação*", "*Conformidade com Normas Internacionais de Segurança*", "*Auditorias de Segurança da Informação*", "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*".

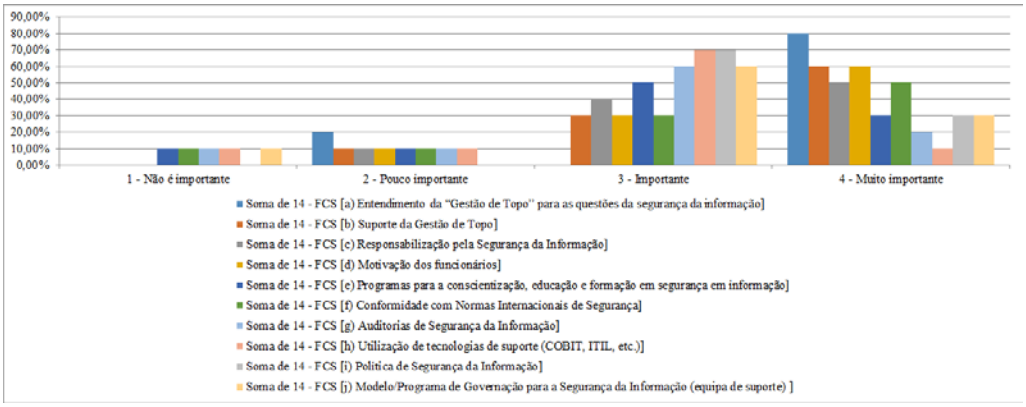


Gráfico 5.65- Factores Críticos de Sucesso: PPO (Gestor de Topo)

Do ponto de vista do Gestor Intermédio – conforme gráfico (Gráfico 5.66) seguinte, verifica-se que todos os elementos são considerados como Factores Críticos de Sucesso e classificados com valores maioritários (acima dos 50,00%) nas categorias "Muito importante" ou "Importante, situando-se o enfoque da votação na categoria "Importante".

Contudo, os três elementos críticos de sucesso mais votados na categoria "Muito importante" são: "*Responsabilização pela Segurança da Informação*" (61,54%), "*Entendimento da Gestão de Topo para as questões da segurança da informação*" (57,69%) e "*Suporte da Gestão de Topo*" (53,85%).

Na categoria "Importante" surge, em primeiro lugar, o elemento crítico de sucesso "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" (69,23%), seguido do elemento "*Conformidade com Normas Internacionais de Segur*ança" (61,54%). Em terceira posição, nesta categoria, aparecem três elementos com a mesma votação (57,69%): "*Política de Segurança da Informação*", "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Auditorias de Segurança da Informação*". Porém, estes dois últimos elementos são os dois mais populados na categoria "Pouco importante", reunindo, respectivamente, as classificações de (26,92%) e (15,38%). Com esta classificação e nesta

categoria surgem também os elementos: "*Motivação dos funcionários*" e "*Programas para a conscientização, educação e formação em segurança em informação*". Nenhum elemento é populado na categoria "Não é importante".

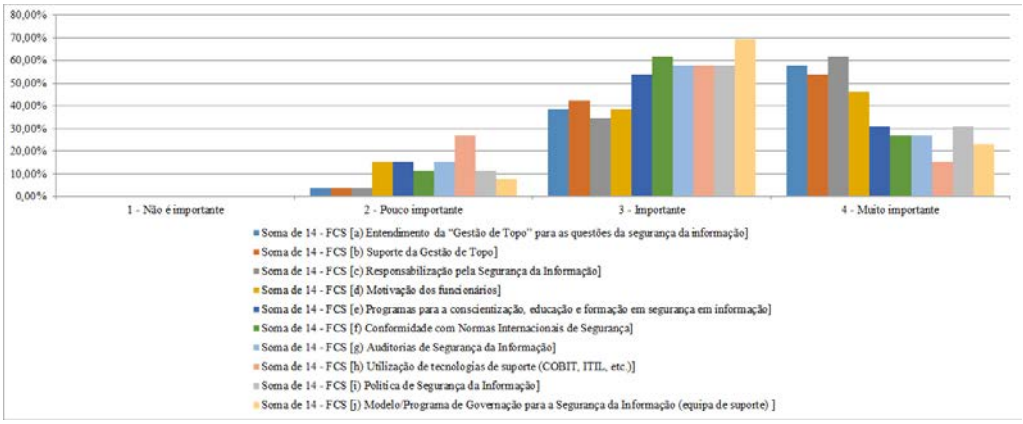


Gráfico 5.66- Factores Críticos de Sucesso: PPO (Gestor Intermédio)

Do ponto de vista do Gestor das TI – neste grupo profissional, os elementos considerados como Factores Críticos de Sucesso também surgem sempre maioritariamente populados nas categorias "Muito importante" ou "Importante", notando-se um enfoque na categoria "Importante". Nesta categoria, oito dos dez elementos considerados obtêm valores superiores à metade percentual (50,00%).

Todavia, cinco dos dez elementos críticos de sucesso, designadamente, "*Entendimento da Gestão de Topo para as questões da segurança da informação*", "*Suporte da Gestão de Topo*", "*Responsabilização pela Segurança da Informação*", "*Programas para a conscientização, educação e formação em segurança em informação*" e "*Conformidade com Normas Internacionais de Segurança*" atingem a totalidade da votação (100,00%), quando somados os resultados percentuais nas categorias "Muito importante" e "Importante".

Para este gestor, verifica-se, que o elemento crítico de sucesso "*Entendimento da Gestão de Topo para as questões da segurança da informação*" (64,71%) é o mais votado na categoria "Muito importante". Com este valor, mas na categoria "Importante" encontram-se, ainda, os quatro elementos seguintes: "*Motivação dos funcionários*", "*Programas para a conscientização, educação e formação em segurança em informação*", "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*". Mas, o elemento mais votado nesta categoria é "*Conformidade com Normas Internacionais de Segurança*" (76,47%).

Na categoria "Pouco Importante", este grupo profissional, aponta como elemento crítico de sucesso mais votado a "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" (11,76%),

surgindo de seguida quatro elementos em igualdade de votação (5,88%): "*Motivação dos funcionários*", "*Auditorias de Segurança da Informação*", "*Política de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*".

Nenhum elemento crítico de sucesso é populado na categoria "Não é importante". O gráfico (Gráfico 5.67) seguinte ilustra o atrás mencionado.

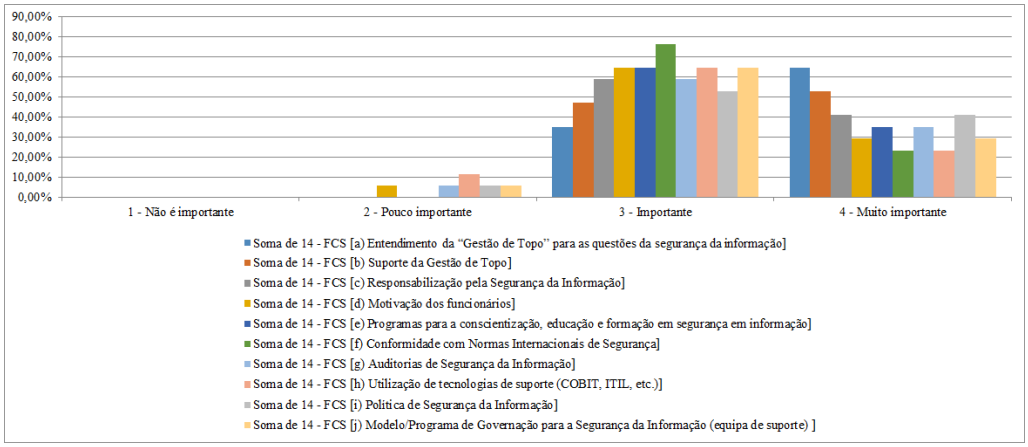


Gráfico 5.67- Factores Críticos de Sucesso: PPO (Gestor das TI)

Do ponto de vista do Consultor das TI – nesta perspectiva verifica-se, novamente, que os dez elementos críticos de sucesso considerados agrupam, maioritariamente as preferências de votação nas categorias "Muito importante" ou "Importante", embora o enfoque esteja mais uma vez na categoria "Importante". No entanto, este grupo profissional destaca o elemento "*Entendimento da Gestão de Topo para as questões da segurança da informação*" atribuindo-lhe uma votação significativa (71,43%) na categoria "Muito importante". Este elemento agrega a totalidade (100,00%) da votação quando, somados os valores nas categorias "Muito importante" e "Importante".

Na categoria "Importante" o elemento crítico de sucesso "*Programas para a conscientização, educação e formação em segurança em informação*" revela-se como o mais votado e agrupa uma percentagem significativa (71,43%) das preferências. Na segunda e terceira posição encontram-se os elementos: "*Conformidade com Normas Internacionais de Segurança*" (64,29%), "*Política de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*", ambos com pontuação idêntica (57,14%).

Já na categoria "Pouco importante" aparecem nove dos dez elementos populados. Os elementos críticos de sucesso mais votados foram "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" (42,86%), seguidos dos elementos "*Auditorias de Segurança da Informação*" e

"*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*", que obtém o mesmo valor percentual (21,43%).

Na categoria "Não é importante" é, apenas, votado um elemento crítico de sucesso "*Programas para a conscientização, educação e formação em segurança em informação*" (7,14%). No gráfico (Gráfico 5.68) seguinte visualiza-se o acima descrito.

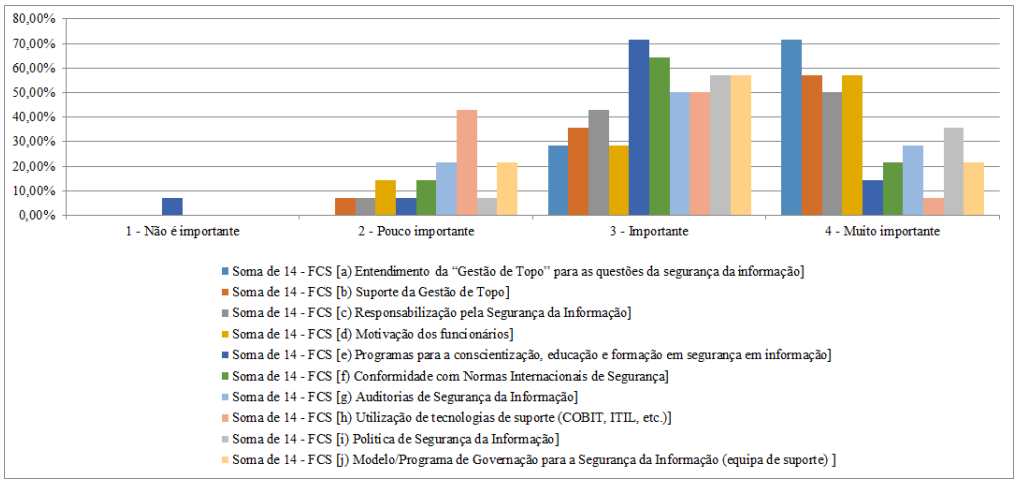


Gráfico 5.68- Factores Críticos de Sucesso: PPO (Consultor das TI)

Do ponto de vista do Gestor / Funcionário da Segurança – esta classe apresenta uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). Os elementos críticos de sucesso considerados apresentam todos valores iguais à totalidade percentual (100,00%), quando somados nas categorias "Muito importante" e "Importante", com prevalência nesta última.

Todavia, na categoria "Importante" existem três elementos críticos de sucesso que obtêm a unanimidade (100,00%) da votação: "*Conformidade com Normas Internacionais de Segurança*", "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Política de Segurança da Informação*". O gráfico (Gráfico 5.69) seguinte mostra o acima mencionado.

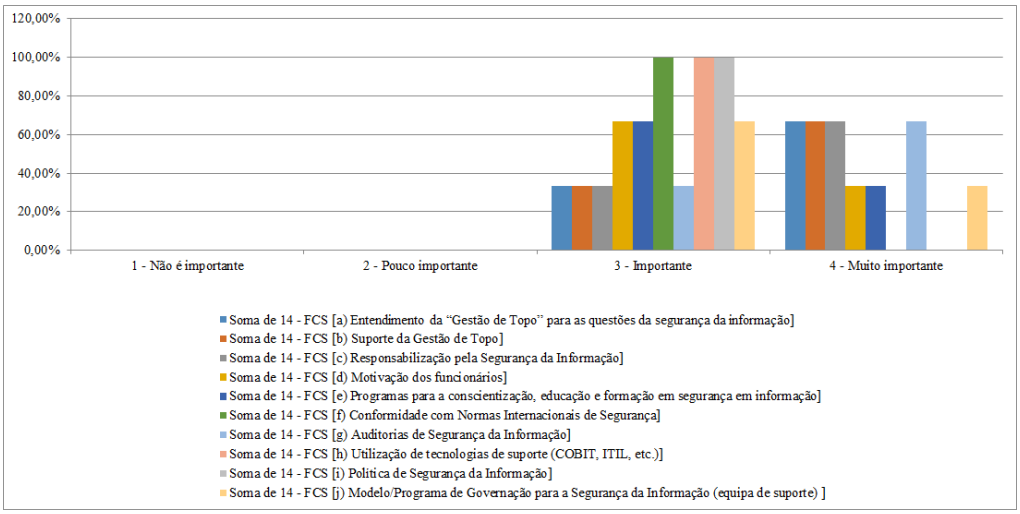


Gráfico 5.69- Factores Críticos de Sucesso: PPO (Gestor/Funcionário da Segurança)

Do ponto de vista do Trabalhador – nesta vista, cinco dos dez elementos críticos de sucesso considerados, revelam-se, preferencialmente, votados na categoria "Muito importante", apresentando, quatro elementos, com valores superiores à metade percentual (50,00%). O mais votado é "*Motivação dos funcionários*" (56,86%), seguido, respectivamente, dos seguintes elementos: "*Programas para a conscientização, educação e formação em segurança em informação*" (54,90%), "*Responsabilização pela Segurança da Informação*" (52,94%) e "*Entendimento da Gestão de Topo para as questões da segurança da informação*" (50,98%).

Na categoria "Importante" surgem também cinco dos dez elementos críticos de sucesso considerados com votações maioritárias (superiores a 50,00%): "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" (64,71%), "*Auditorias de Segurança da Informação*" (58,82%), "*Política de Segurança da Informação*" (56,86%), "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" (54,90%) e "*Conformidade com Normas Internacionais de Segurança*" (50,98%).

Por outro lado, na categoria "Pouco importante" todos os elementos mostram-se populados. Porém, o elemento crítico de sucesso que agrupa maior pontuação é "*Motivação dos funcionários*" (15,69%) seguido dos elementos "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" (13,73%) e "*Programas para a conscientização, educação e formação em segurança em informação*" (11,76%).

Na categoria "Não é importante" existem três elementos críticos de sucesso populados com valores idênticos (1,96%). No gráfico (Gráfico 5.70) seguinte visualiza-se o acima mencionado.

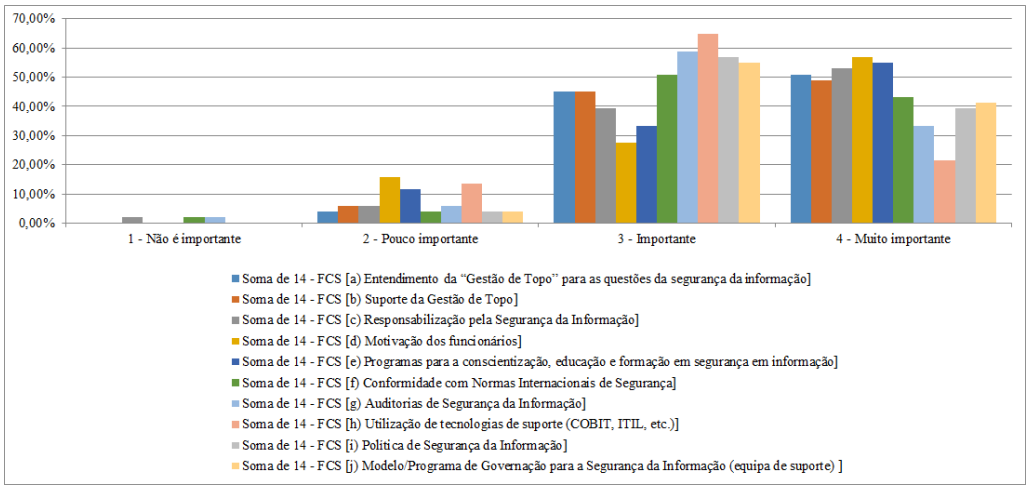


Gráfico 5.70- Factores Críticos de Sucesso: PPO (Trabalhador)

5.2.5 – Resumo da Perspectiva do Próprio face à Organização

Em conformidade com o referencial indicado na figura seguinte (Figura 5.12), este ponto sintetiza os resultados obtidos para os Factores Críticos de Sucesso segundo a perspectiva do próprio face à organização.

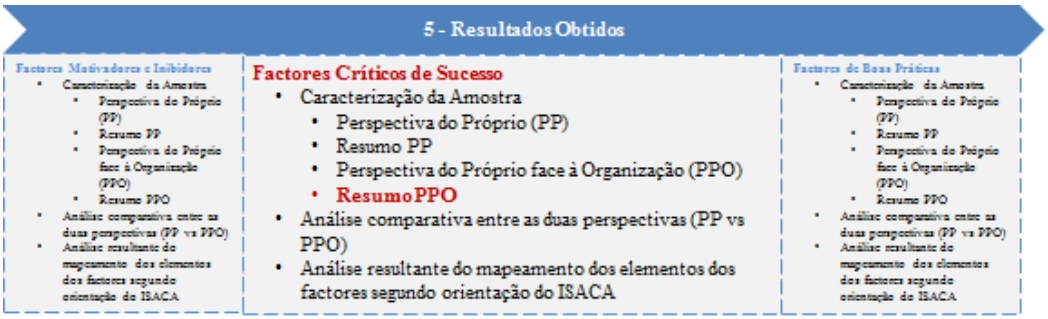


Figura 5.12- Modelo dos Resultados Obtidos: FCS/Resumo da PPO

Assim, resumindo, na tabela (Tabela 5.20) seguinte apresenta-se a ordenação pelas categorias "Muito importante" e "Não é importante" dos elementos considerados para o estudo como Factores Críticos de Sucesso, segundo cada uma das vistas dadas pela função do respondente.

Conforme se pode visualizar, o elemento crítico de sucesso "*Entendimento da "Gestão de Topo" para as questões da segurança da informação*" é referido, essencialmente, em primeiro lugar, na categoria "Muito importante". Porém, o Gestor Intermédio coloca-o em segundo lugar e o Trabalhador aponta-o em quarto lugar.

O Gestor Intermédio selecciona em primeiro lugar o elemento crítico de sucesso "*Responsabilização pela Segurança da Informação*" e o Trabalhador aponta, preferencialmente, o elemento "*Motivação dos funcionários*".

Como segundo elemento mais referenciado, aparece o elemento "*Suporte da Gestão de Topo*" que é votado pelos gestores de topo, gestores das TI e consultores das TI.

No entanto, globalmente, o elemento crítico de sucesso "*Responsabilização pela Segurança da Informação*" surge também, como segundo elemento mais votado, contribuindo para isso as preferências dos gestores intermédios e gestores/funcionários da segurança, que os classificam em primeiro lugar.

De notar um alinhamento das posições dos gestores de topo e dos consultores das TI que mostram as mesmas preferências nas suas escolhas do primeiro, segundo e terceiro elementos. O Gestor das TI apresenta preferência idêntica para o primeiro elemento. No entanto, para as outras posições encontram-se algumas divergências.

Verifica-se ainda que, na categoria "Não é importante", seis dos dez elementos são apontados: "*Responsabilização pela Segurança da Informação*", "*Programas para a conscientização, educação e formação em segurança em informação*", "*Conformidade com Normas Internacionais de Segurança*", "*Auditorias de Segurança da Informação*", "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*".

Factores Críticos de Sucesso -PPO (- Elemento não é referido pelos respondentes)		13 - FCS [a] Entendimento da "Gestão de Topo" para as questões da segurança da informação]	13 - FCS [b] Suporte da Gestão de Topo]	13 - FCS [c] Responsabilização pela Segurança da Informação]	13 - FCS [d] Motivação dos funcionários]	13 - FCS [e] Programas para a conscientização, educação e formação em segurança em informação]	13 - FCS [f] Conformidade com Normas Internacionais de Segurança]	13 - FCS [g] Auditorias de Segurança da Informação]	13 - FCS [h] Utilização de tecnologias de suporte (COBIT, ITIL, etc.)]	13 - FCS [i] Política de Segurança da Informação]	13 - FCS [j] Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)]
Gestor de Topo	Muito importante	1	2	3	2	4	3	5	6	4	4
	Não é importante	-	-	-	-	1	1	1	1	-	1
Gestor Intermédio	Muito importante	2	3	1	4	5	6	6	8	5	7
	Não é importante	-	-	-	-	-	-	-	-	-	-
Gestor das TI	Muito importante	1	2	3	5	4	6	4	6	3	5
	Não é importante	-	-	-	-	-	-	-	-	-	-
Consultor das TI	Muito importante	1	2	3	2	7	6	5	8	4	6
	Não é importante	-	-	-	-	1	-	-	-	-	-
Gestor / Funcionário da Segurança	Muito importante	1	1	1	2	2	-	1	-	-	2
	Não é importante	-	-	-	-	-	-	-	-	-	-
Trabalhador	Muito importante	4	5	3	1	2	6	9	10	8	7
	Não é importante	-	-	1	-	-	1	1	-	-	-
Global	**Muito importante**	**1**	**2**	**2**	**3**	**4**	**6**	**8**	**9**	**5**	**7**
	Não é importante	**-**	**-**	**2**	**-**	**1**	**1**	**1**	**2**	**-**	**2**

Tabela 5.20- Factores Críticos de Sucesso - PPO: Ordenação das preferências

5.2.6 – Análise Comparativa entre as duas Perspectivas (Próprio e Próprio face à Organização)

Neste ponto, apresentam-se os resultados comparativos das duas perspectivas dos respondentes (a do próprio e a do próprio face à organização/sector) relativamente aos Factores Críticos de Sucesso considerados.

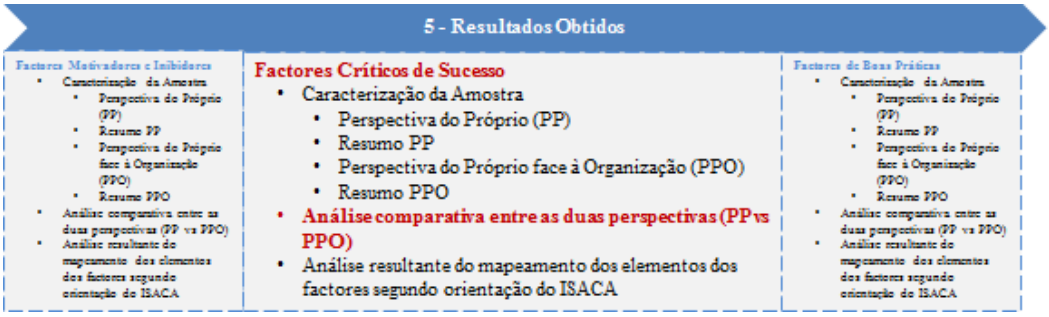


Figura 5.13- Modelo dos Resultados Obtidos: FCS/Análise Comparativa

Assim, primeiramente efectuou-se o cálculo do nível médio de importância para cada elemento deste factor, através da seguinte fórmula:

$$\text{Nível médio de importância} = \frac{\sum_{c=1}^{4}(nº\ de\ referências\ ao\ elemento * c)}{n.º\ de\ respondentes}$$

em que a variável "c" corresponde ao valor da categoria de classificação (1-Não é importante; 2-Pouco importante; 3-Importante e 4-Muito importante) seleccionado pelo respondente para o elemento em causa.

Deste modo, na tabela (Tabela 5.21) seguinte, mostram-se os valores médios encontrados para todos os elementos considerados como Factores Críticos de Sucesso, tendo em conta todas as respostas chegadas.

Factores Críticos de Sucesso	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,6	3,6	0,0
Suporte da Gestão de Topo	3,5	3,5	0,0
Responsabilização pela Segurança da Informação	3,5	3,5	0,0
Motivação dos funcionários	3,5	3,4	0,1
Programas para a conscientização, educação e formação em segurança em informação	3,4	3,3	0,1
Conformidade com Normas Internacionais de Segurança	3,2	3,2	0,0
Auditorias de Segurança da Informação	3,2	3,2	0,0
Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	3,0	3,0	0,0
Política de Segurança da Informação	3,4	3,3	0,1
Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,3	3,2	0,1

Tabela 5.21- Factores Críticos de Sucesso: valores Nível Médio de Importância (Global)

Na tabela (Tabela 5.21) anterior, verifica-se que, em quatro dos dez elementos considerados como Factores Críticos de Sucesso para a adopção/implementação de um SGSI numa organização do sector das Águas e Saneamento em Portugal, a perspectiva do próprio apresenta desvios na classificação dos mesmos relativamente à perspectiva do próprio face à organização.

Assim, comprova-se, ainda, que o nível médio de importância - na perspectiva do próprio, é maior em todos os elementos considerados, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, apresentando um valor de desvio igual (0,1) para todos os elementos: "*Motivação dos funcionários*", "*Programas para a conscientização, educação e formação em segurança em informação*", "*Política de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*".

Para uma melhor visualização desses desvios mostra-se, seguidamente, o gráfico (Gráfico 5.71) radar:

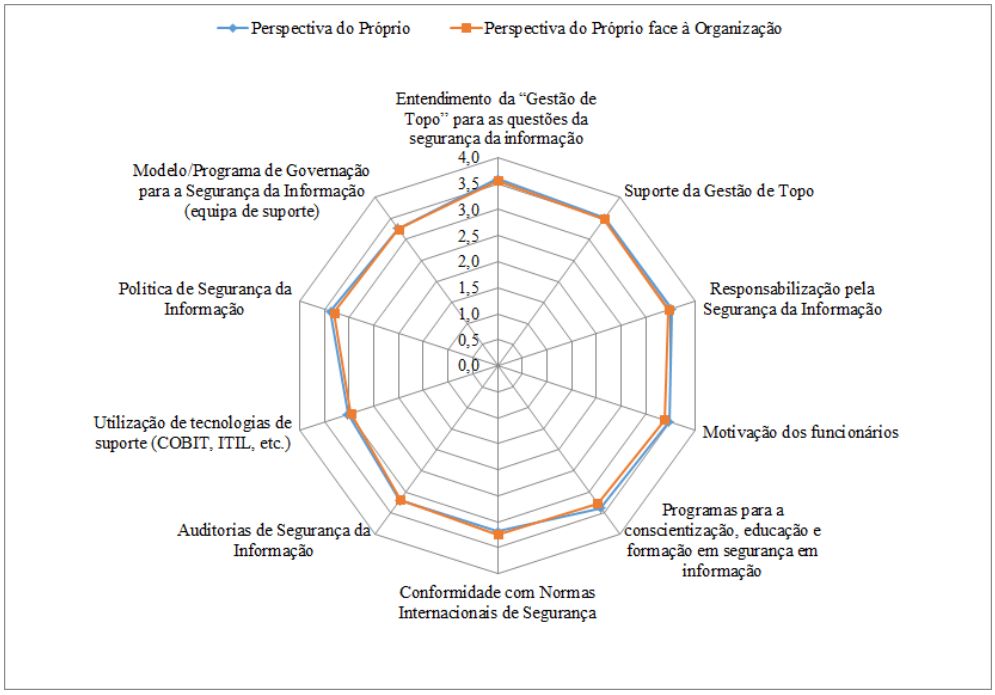


Gráfico 5.71- Factores Críticos de Sucesso: Comparação entre PP e PPO (Global)

De forma a compreender melhor a origem dos desvios, isto é, para se aferir que tipo de respondentes contribuíram para a apresentação destes desvios, elaborou-se também o cálculo do nível médio de importância para cada elemento deste factor, cruzando-se com o tipo de função do respondente, chegando-se aos seguintes resultados:

Do ponto de vista do Gestor de Topo - a tabela (Tabela 5.22) seguinte, mostra que as opiniões dos gestores de topo, que representam (8,26%) dos respondentes, apresentam desvios em todos

os elementos com excepção do elemento crítico de sucesso "*Conformidade com Normas Internacionais de Segurança*".

Assim, pode também verificar-se que o nível médio de importância - na perspectiva do próprio, é maior em todos os elementos críticos de sucesso considerados, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, apresentando um maior valor de desvio nos elementos "*Auditorias de Segurança da Informação*" (0,4) e "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" (0,3).

Factores Críticos de Sucesso	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,8	3,6	0,2
Suporte da Gestão de Topo	3,7	3,5	0,2
Responsabilização pela Segurança da Informação	3,6	3,4	0,2
Motivação dos funcionários	3,6	3,5	0,1
Programas para a conscientização, educação e formação em segurança em informação	3,2	3,0	0,2
Conformidade com Normas Internacionais de Segurança	3,2	3,2	0,0
Auditorias de Segurança da Informação	3,3	2,9	0,4
Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	3,1	2,8	0,3
Política de Segurança da Informação	3,4	3,3	0,1
Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,3	3,1	0,2

Tabela 5.22- Factores Críticos de Sucesso: valores Nível Médio de Importância (Gestor de Topo)

O gráfico (Gráfico 5.72) radar que se segue reflecte as diferenças acima mencionadas.

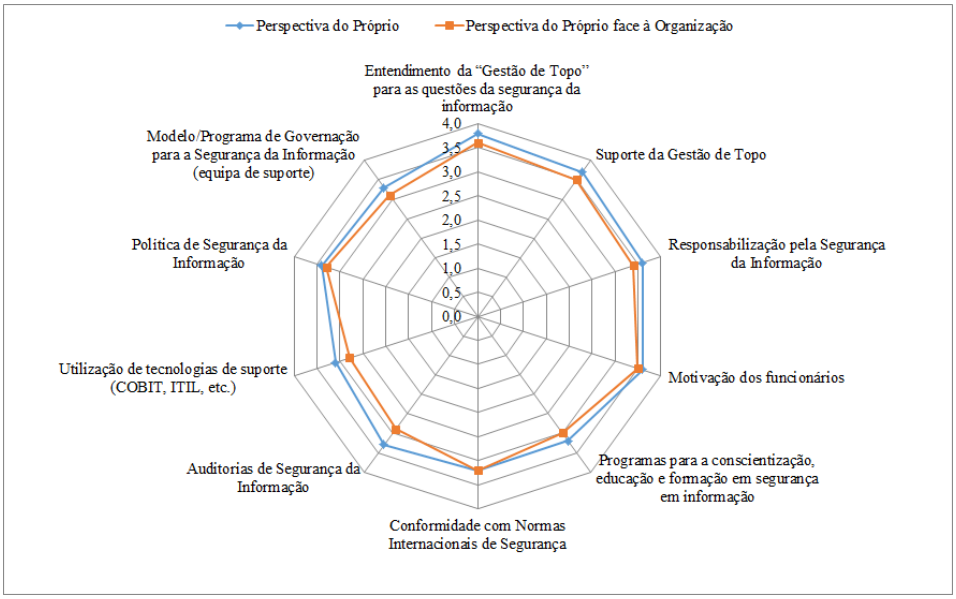


Gráfico 5.72- Factores Críticos de Sucesso: Comparação entre PP e PPO (Gestor de Topo)

Do ponto de vista do Gestor Intermédio - a tabela (Tabela 5.23) seguinte, mostra que as opiniões dos gestores intermédios, que representam (21,49%) dos respondentes, apresentam

também desvios em todos os elementos críticos de sucesso considerados, com excepção do elemento "*Entendimento da Gestão de Topo para as questões da segurança da informação*".

Contudo, comprova-se que o nível médio de importância - na perspectiva do próprio, é maior em sete dos dez elementos críticos de sucesso considerados, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, revelando-se um maior valor de desvio (0,2) no elemento: "*Programas para a conscientização, educação e formação em segurança em informação*".

Todavia, nos elementos críticos de sucesso "*Conformidade com Normas Internacionais de Segurança*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" acontece o contrário: a pontuação do nível médio de importância é maior quando apresenta a sua perspectiva face à organização.

Factores Críticos de Sucesso	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,5	3,5	0,0
Suporte da Gestão de Topo	3,6	3,5	0,1
Responsabilização pela Segurança da Informação	3,7	3,6	0,1
Motivação dos funcionários	3,4	3,3	0,1
Programas para a conscientização, educação e formação em segurança em informação	3,4	3,2	0,2
Conformidade com Normas Internacionais de Segurança	3,1	3,2	-0,1
Auditorias de Segurança da Informação	3,2	3,1	0,1
Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	3,0	2,9	0,1
Política de Segurança da Informação	3,3	3,2	0,1
Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,1	3,2	-0,1

Tabela 5.23- Factores Críticos de Sucesso: valores Nível Médio de Importância (Gestor Intermédio)

O gráfico (Gráfico 5.73) radar abaixo ilustra as diferenças acima expostas.

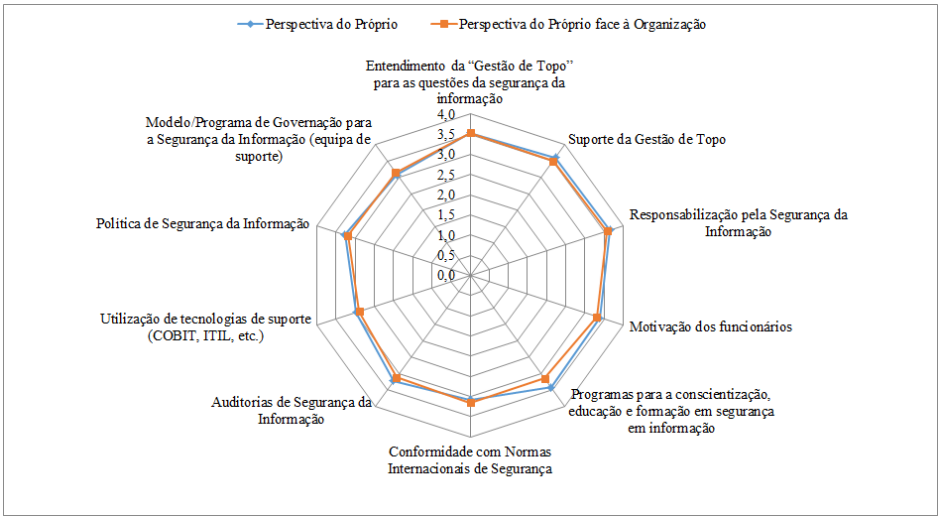


Gráfico 5.73- Factores Críticos de Sucesso: Comparação entre PP e PPO (Gestor Intermédio)

Do ponto de vista do Gestor das TI - a tabela (Tabela 5.24) a seguir, reflecte as opiniões dos gestores das TI, que representam (14,05%) dos respondentes, apresentando, também, desvios para todos os elementos críticos de sucesso considerados, com excepção do elemento "*Entendimento da "Gestão de Topo" para as questões da segurança da informação*".

Assim, constata-se que o nível médio de importância - na perspectiva do próprio, é maior em sete dos dez elementos considerados, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, mostrando um maior valor de desvio (0,2) no elemento: "*Programas para a conscientização, educação e formação em segurança em informação*".

No entanto, nos elementos "*Conformidade com Normas Internacionais de Segurança*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" acontece o contrário: a pontuação do nível médio de importância é maior quando apresenta a sua perspectiva face à organização e atinge um valor absoluto de desvio igual (0,1).

Factores Críticos de Sucesso	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,5	3,5	0,0
Suporte da Gestão de Topo	3,6	3,5	0,1
Responsabilização pela Segurança da Informação	3,7	3,6	0,1
Motivação dos funcionários	3,4	3,3	0,1
Programas para a conscientização, educação e formação em segurança em informação	3,4	3,2	0,2
Conformidade com Normas Internacionais de Segurança	3,1	3,2	-0,1
Auditorias de Segurança da Informação	3,2	3,1	0,1
Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	3,0	2,9	0,1
Política de Segurança da Informação	3,3	3,2	0,1
Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,1	3,2	-0,1

Tabela 5.24- Factores Críticos de Sucesso: valores Nível Médio de Importância (Gestor das TI)

No gráfico (Gráfico 5.74) radar abaixo ilustra-se as diferenças acima apontadas.

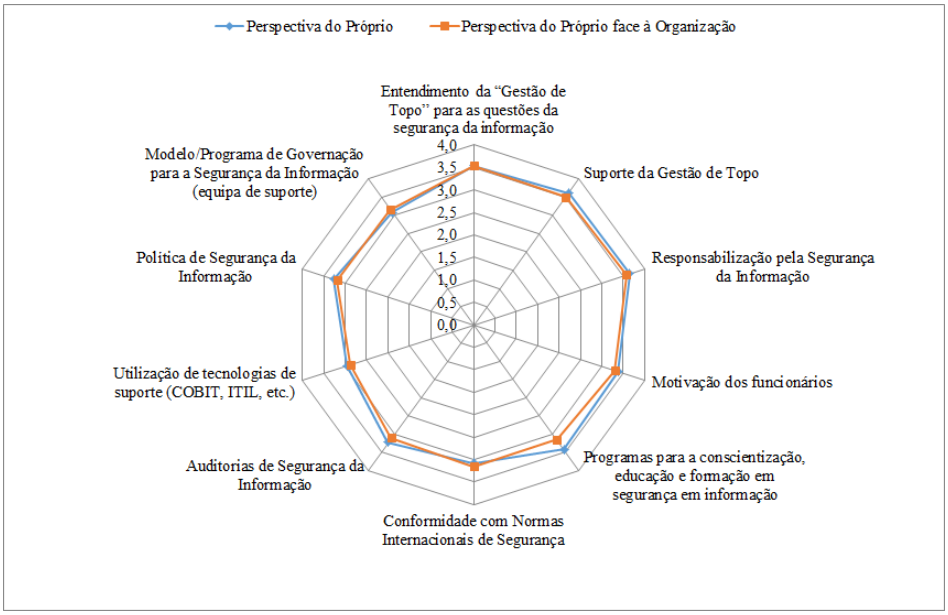


Gráfico 5.74- Factores Críticos de Sucesso: Comparação entre PP e PPO (Gestor das TI)

Do ponto de vista do Consultor das TI - a tabela (Tabela 5.25) seguinte, revela que as opiniões dos consultores das TI, que representam (11,57%) dos respondentes, apresentam desvios em seis dos dez elementos críticos de sucesso considerados.

Contudo, verifica-se que o nível médio de importância - na perspectiva do próprio, é maior em três dos dez elementos críticos de sucesso considerados, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, apresentando um maior valor de desvio (0,3) no elemento: "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*".

Mas, nos elementos críticos de sucesso "*Conformidade com Normas Internacionais de Segurança*", "*Auditorias de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" acontece o contrário: a pontuação do nível médio de importância é maior quando apresenta a sua perspectiva face à organização. Nos dois primeiros elementos o valor do desvio é de (0,2) e no terceiro elemento, o desvio atinge o valor absoluto de (0,3).

Factores Críticos de Sucesso	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,7	3,7	0,0
Suporte da Gestão de Topo	3,5	3,5	0,0
Responsabilização pela Segurança da Informação	3,4	3,4	0,0
Motivação dos funcionários	3,4	3,4	0,0
Programas para a conscientização, educação e formação em segurança em informação	3,0	2,9	0,1
Conformidade com Normas Internacionais de Segurança	2,9	3,1	-0,2
Auditorias de Segurança da Informação	2,9	3,1	-0,2
Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	2,9	2,6	0,3
Política de Segurança da Informação	3,4	3,3	0,1
Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	2,7	3,0	-0,3

Tabela 5.25- Factores Críticos de Sucesso: valores Nível Médio de Importância (Consultor das TI)

O gráfico (Gráfico 5.75) radar abaixo indica as diferenças acima referidas.

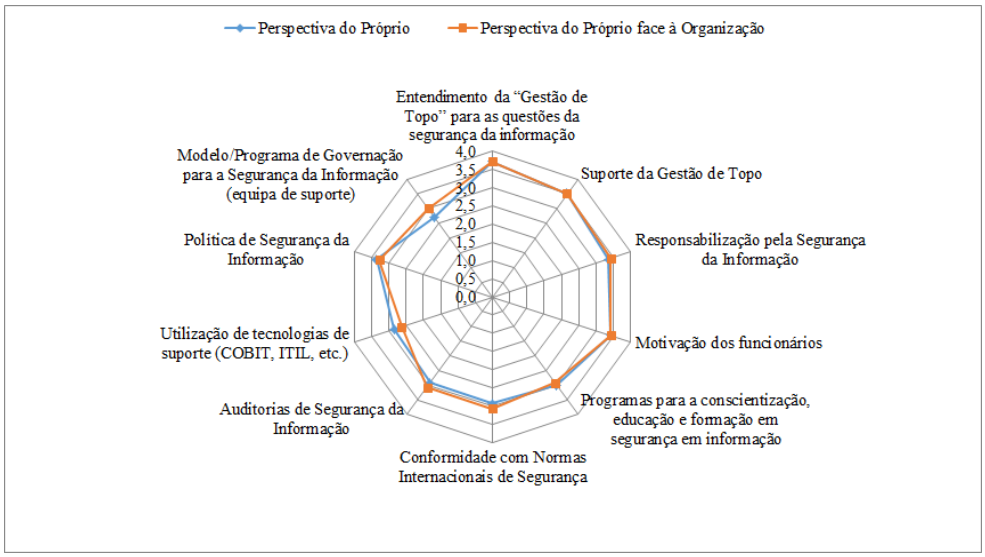


Gráfico 5.75- Factores Críticos de Sucesso: Comparação entre PP e PPO (Consultor das TI)

Do ponto de vista do Gestor/Funcionário de Segurança – esta classe apresenta uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). No entanto, mesmo assim, refira-se que aparecem três dos dez elementos críticos de sucesso considerados com desvios entre as duas perspectivas apresentadas.

Deste modo, verifica-se que o nível médio de importância - na perspectiva do próprio, é maior em dois dos dez elementos críticos de sucesso considerados, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, apresentando um maior valor de desvio nos elementos: "*Programas para a conscientização, educação e formação em segurança em informação*" (0,4) e "*Conformidade com Normas Internacionais de Segurança*" (0,3).

Porém, no elemento crítico de sucesso "*Suporte da Gestão de Topo*" acontece o contrário: a pontuação do nível médio de importância é maior, quando apresenta a sua perspectiva face à organização. O valor absoluto do desvio, neste caso, é de (0,4).

A tabela (Tabela 5.26) seguinte confirma esta afirmação.

Factores Críticos de Sucesso	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,7	3,7	0,0
Suporte da Gestão de Topo	3,3	3,7	-0,4
Responsabilização pela Segurança da Informação	3,7	3,7	0,0
Motivação dos funcionários	3,3	3,3	0,0
Programas para a conscientização, educação e formação em segurança em informação	3,7	3,3	0,4
Conformidade com Normas Internacionais de Segurança	3,3	3,0	0,3
Auditorias de Segurança da Informação	3,7	3,7	0,0
Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	3,0	3,0	0,0
Política de Segurança da Informação	3,0	3,0	0,0
Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,3	3,3	0,0

Tabela 5.26- Factores Críticos de Sucesso: valores Nível Médio de Importância (Gestor/Funcionário da Segurança)

O gráfico (Gráfico 5.76) radar abaixo mostra as diferenças acima mencionadas.

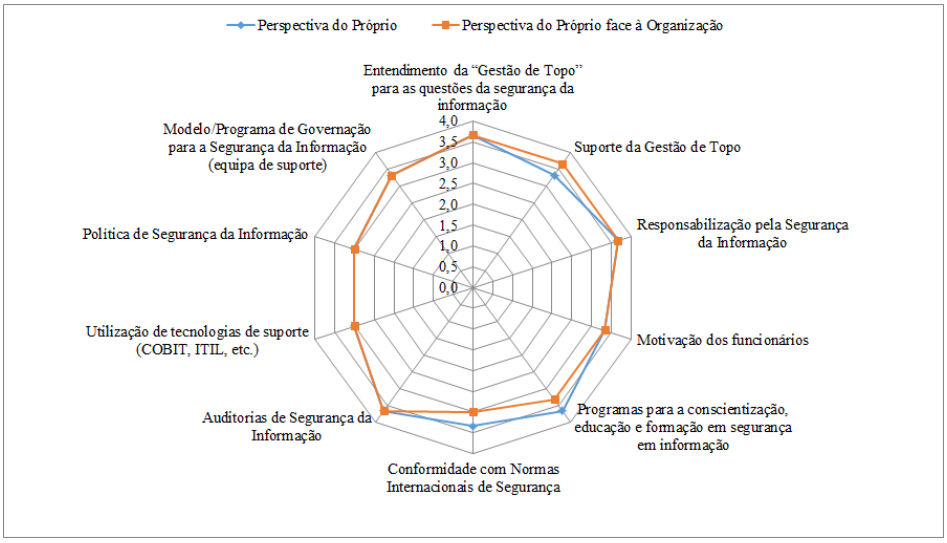


Gráfico 5.76- Factores Críticos de Sucesso: Comparação entre PP e PPO (Gestor/Funcionário da Segurança)

Do ponto de vista do Trabalhador - na tabela (Tabela 5.27) seguinte, constata-se que as opiniões dos trabalhadores, que representam (42,15%) dos respondentes, evidenciam desvios em seis dos dez elementos críticos de sucesso considerados.

Todavia, verifica-se que o nível médio de importância - na perspectiva do próprio, é maior em quatro dos dez elementos críticos de sucesso considerados, quando comparado com o nível

médio de importância – na perspectiva do próprio face à organização, revelando-se um valor maior de desvio (0,2) no elemento: "*Motivação dos funcionários*".

No entanto, nos elementos críticos de sucesso "*Conformidade com Normas Internacionais de Segurança*", e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" acontece o contrário: a pontuação do nível médio de importância é maior quando apresenta a sua perspectiva face à organização. Neste caso, o segundo elemento mostra, também, um maior valor absoluto de desvio (0,2).

Factores Críticos de Sucesso	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,5	3,5	0,0
Suporte da Gestão de Topo	3,4	3,4	0,0
Responsabilização pela Segurança da Informação	3,5	3,4	0,1
Motivação dos funcionários	3,6	3,4	0,2
Programas para a conscientização, educação e formação em segurança em informação	3,5	3,4	0,1
Conformidade com Normas Internacionais de Segurança	3,3	3,4	-0,1
Auditorias de Segurança da Informação	3,2	3,2	0,0
Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	3,1	3,1	0,0
Política de Segurança da Informação	3,5	3,4	0,1
Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,2	3,4	-0,2

Tabela 5.27- Factores Críticos de Sucesso: valores Nível Médio de Importância (Trabalhador)

O gráfico (Gráfico 5.77) radar abaixo revela as diferenças acima mencionadas.

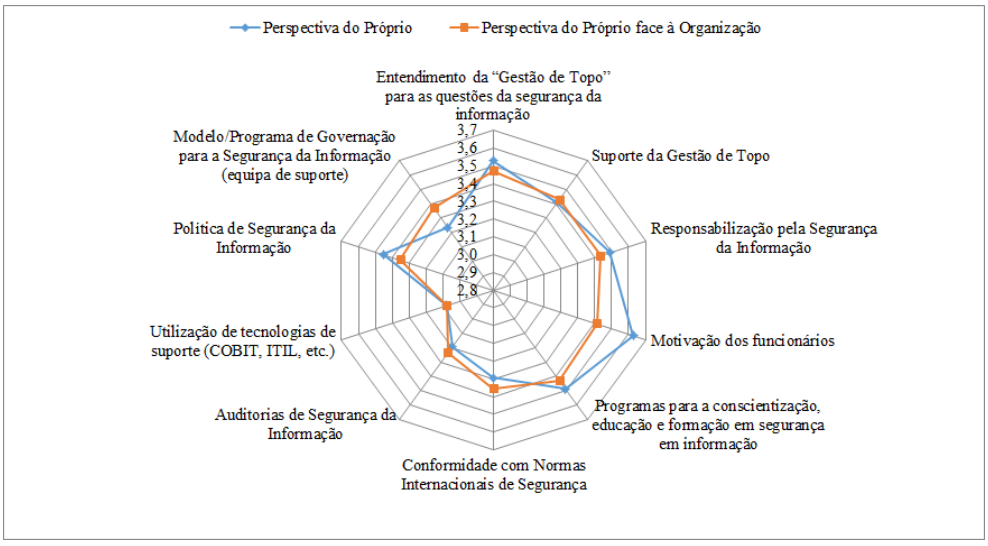


Gráfico 5.77- Factores Críticos de Sucesso: Comparação entre PP e PPO (Trabalhador)

5.2.7 – Análise resultante do mapeamento dos elementos do factor segundo a orientação - ISACA

Retomando o referencial abaixo ilustrado (Figura 5.14), nesta parte apresentam-se os resultados alcançados por meio da análise efectuada ao cruzamento dos dados obtidos e o mapeamento dos elementos críticos de sucesso segundo orientação do ISACA [124] que refere: «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*».

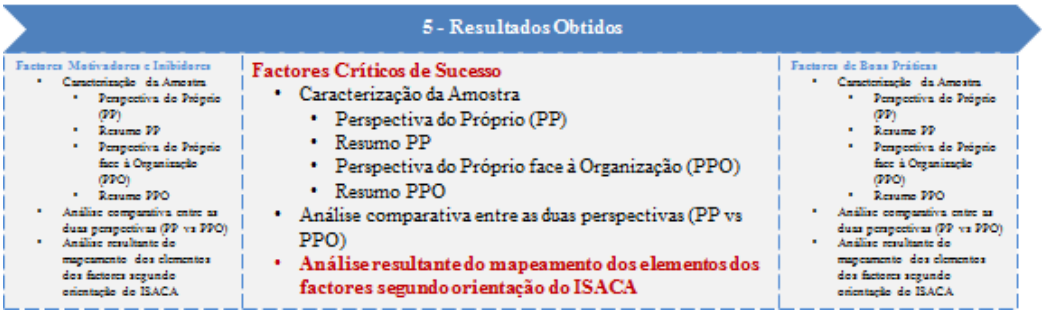


Figura 5.14- Modelo dos Resultados Obtidos: FCS/Análise Mapeamento ISACA

Assim, para a realização da análise acima referida, partiu-se dos valores médios de importância encontrados para os elementos considerados na caracterização dos Factores Críticos de Sucesso e, enquadraram-se os mesmos nos principais resultados que o programa da segurança deverá trabalhar, conforme indicado no ponto 4.2 deste documento.

Neste contexto, o estudo revela que, globalmente, os elementos considerados críticos de sucesso para a adopção/implementação dum Sistema de Gestão da Segurança da Informação nas organizações centram-se nos pilares de resultados: "*Gestão de Desempenho*" e "*Alinhamento Estratégico*" e apresentam pontuações de nível médio de importância idênticas, na ordem dos (3,4 – 3,5). De notar o enfase do nível médio de importância nos elementos "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*", "*Suporte da Gestão de Topo*" e "*Responsabilização pela Segurança da Informação*" que denota um baixo nível de maturidade do sector, em matéria de Segurança da Informação. De facto, estudos têm demostrado que quando as organizações apresentam níveis de maturidade elevados, nestas matérias, os factores críticos apontados centram-se mais nos processos que nas estruturas.

De realçar, ainda, que o item "*Motivação dos funcionários*", elemento crítico de sucesso relacionado com o ´factor humano´ revela também, na perspectiva do próprio, um nível médio de importância de dimensão paralela aos acima mencionados, pelo que pode ser visto como um

reconhecimento a ter em conta para a gestão da mudança. A tabela/gráfico (Gráfico 5.78) seguinte mostra o acima referido.

Factores Críticos de Sucesso (Nível médio de importância - Global)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,6	3,6								
b) Suporte da Gestão de Topo	3,5	3,5								
c) Responsabilização pela Segurança da Informação							3,5	3,5		
d) Motivação dos funcionários							3,5	3,4		
e) Programas para a conscientização, educação e formação em segurança em informação			3,4	3,3						
f) Conformidade com Normas Internacionais de Segurança			3,2	3,2						
g) Auditorias de Segurança da Informação									3,2	3,2
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)					3	3				
i) Política de Segurança da Informação	3,4	3,3								
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,3	3,2								
Total (Valor médio)	3,45	3,4	3,3	3,25	3	3	3,5	3,45	3,2	3,2

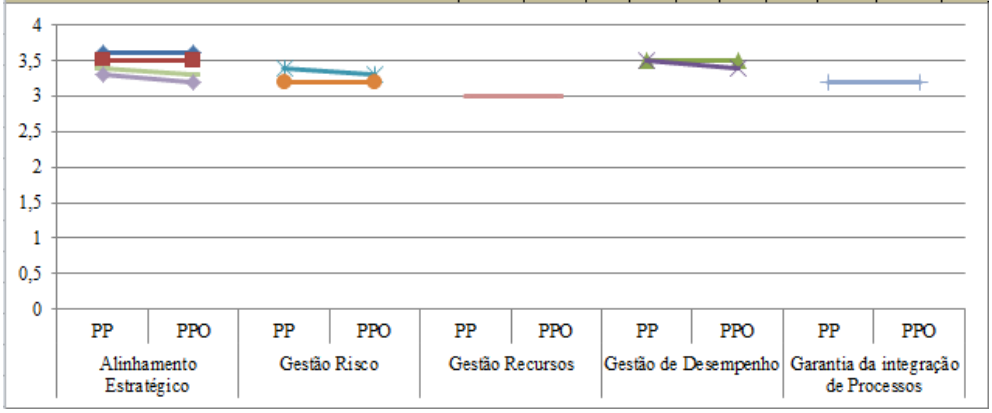


Gráfico 5.78- Factores Críticos de Sucesso: Mapeamento ISACA (Global)

Contudo, se se analisar os resultados tendo em conta a função do respondente, verifica-se que o enfoque do pilar de resultados não muda com o grupo profissional, com excepção do grupo profissional Gestor/Funcionário da Segurança que atribui o enfoque aos pilares de resultados – "*Garantia da integração de Processos*" e "*Gestão de Desempenho*".

Assim, o Gestor de Topo mantém o foco nos pilares de resultados: "*Gestão de Desempenho*" e "*Alinhamento Estratégico*", apresentando pontuações de nível médio de importância, na ordem dos (3,3 – 3,6). Contudo, em ambos os pilares, revela-se um desvio, na ordem dos (0,2) pontos entre as perspectivas do próprio e a do próprio face à organização, isto é, na perspectiva do próprio, o mesmo, atribui um nível médio de importância superior, quando comparado com o valor do nível médio de importância que atribuí na perspectiva do próprio face à organização. De realçar, também, que os elementos críticos de sucesso atribuídos ao pilar de resultados – "*Gestão de Desempenho*" estão fortemente relacionados com o ´factor humano´, indiciando uma defesa, por parte deste grupo profissional, do sucesso na adopção/implementação dum Sistema

de Gestão da Segurança da Informação nas organizações, centrado nos elementos "*Responsabilização da Segurança da Informação*" e "*Motivação dos funcionários*" enquanto do lado do pilar de resultados – "*Alinhamento Estratégico*" centra a sua opinião principalmente nos elementos "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" *e "Suporte da Gestão de Topo"*. A tabela/gráfico (Gráfico 5.79) seguinte mostra o acima referido.

Factores Críticos de Sucesso (Nível médio de importância - Gestor de Topo)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,8	3,6								
b) Suporte da Gestão de Topo	3,7	3,5								
c) Responsabilização pela Segurança da Informação							3,6	3,4		
d) Motivação dos funcionários							3,6	3,5		
e) Programas para a conscientização, educação e formação em segurança em informação			3,2	3						
f) Conformidade com Normas Internacionais de Segurança			3,2	3,2						
g) Auditorias de Segurança da Informação									3,3	2,9
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)					3,1	2,8				
i) Política de Segurança da Informação	3,4	3,3								
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,3	3,1								
Total (Valor médio)	3,55	3,375	3,2	3,1	3,1	2,8	3,6	3,45	3,3	2,9

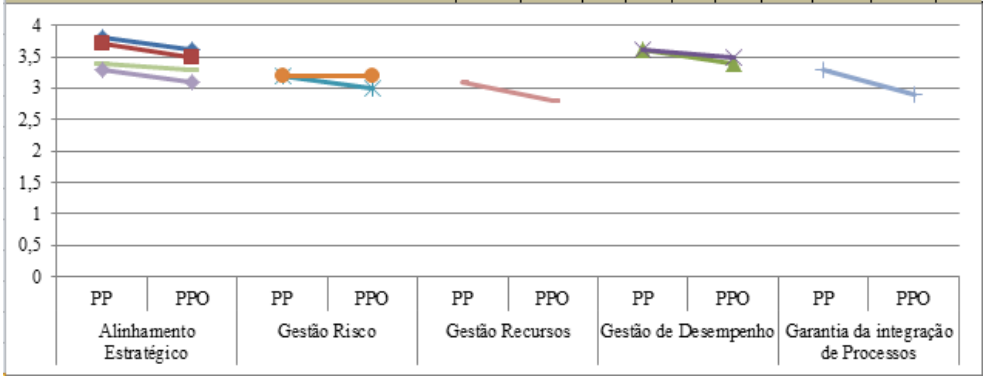


Gráfico 5.79- Factores Críticos de Sucesso: Mapeamento ISACA (Gestor de Topo)

O Gestor Intermédio segue a mesma linha da perspectiva do Gestor de Topo, embora atribua pontuações de níveis médios de importância ligeiramente inferiores, apresentando valores na ordem dos (3,3 – 3,55). A tabela/gráfico (Gráfico 5.80) seguinte mostra o acima referido.

Factores Críticos de Sucesso (Nível médio de importância - Gestor Intermédio)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,5	3,5								
b) Suporte da Gestão de Topo	3,6	3,5								
c) Responsabilização pela Segurança da Informação							3,7	3,6		
d) Motivação dos funcionários							3,4	3,3		
e) Programas para a conscientização, educação e formação em segurança em informação			3,4	3,2						
f) Conformidade com Normas Internacionais de Segurança			3,1	3,2						
g) Auditorias de Segurança da Informação									3,2	3,1
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)					3	2,9				
i) Politica de Segurança da Informação	3,3	3,2								
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,1	3,2								
Total (Valor médio)	3,375	3,35	3,3	3,2	3	2,9	3,55	3,45	3,2	3,1

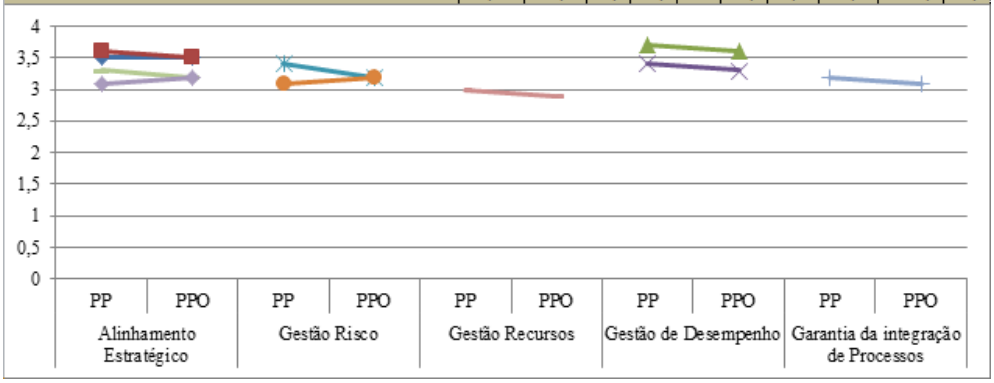


Gráfico 5.80- Factores Críticos de Sucesso: Mapeamento ISACA (Gestor Intermédio)

O Gestor das TI seguindo a mesma linha de perspectiva do Gestor de Topo, apresenta, curiosamente, pontuações de níveis médios de importância idênticos aos atribuídos pelo Gestor Intermédio, apresentando valores na ordem dos (3,3 – 3,55). A tabela/gráfico (Gráfico 5.81) seguinte mostra o acima referido.

Factores Criticos de Sucesso (Nivel médio de importância - Gestor das TI)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,5	3,5								
b) Suporte da Gestão de Topo	3,6	3,5								
c) Responsabilização pela Segurança da Informação							3,7	3,6		
d) Motivação dos funcionários							3,4	3,3		
e) Programas para a conscientização, educação e formação em segurança em informação			3,4	3,2						
f) Conformidade com Normas Internacionais de Segurança			3,1	3,2						
g) Auditorias de Segurança da Informação									3,2	3,1
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)					3	2,9				
i) Política de Segurança da Informação	3,3	3,2								
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,1	3,2								
Total (Valor médio)	3,375	3,35	3,3	3,2	3	2,9	3,55	3,45	3,2	3,1

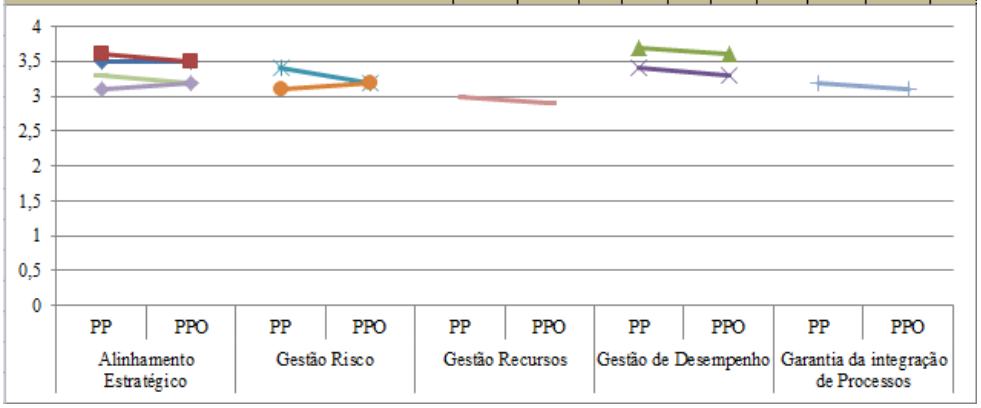


Gráfico 5.81- Factores Críticos de Sucesso: Mapeamento ISACA (Gestor das TI)

Porém, o Consultor das TI embora seguindo a mesma linha da perspectiva do Gestor das TI e Gestor Intermédio, atribuí pontuações de níveis médios de importância ligeiramente inferiores, apresentando valores na ordem dos (3,3 – 3,4). A tabela/gráfico (Gráfico 5.82) seguinte mostra o acima referido.

Factores Críticos de Sucesso (Nível médio de importância - Consultor das TI)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,7	3,7								
b) Suporte da Gestão de Topo	3,5	3,5								
c) Responsabilização pela Segurança da Informação							3,4	3,4		
d) Motivação dos funcionários							3,4	3,4		
e) Programas para a conscientização, educação e formação em segurança em informação			3	2,9						
f) Conformidade com Normas Internacionais de Segurança			2,9	3,1						
g) Auditorias de Segurança da Informação									2,9	3,1
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)					2,9	2,6				
i) Política de Segurança da Informação	3,4	3,3								
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	2,7	3								
Total (Valor médio)	3,325	3,375	3	3	2,9	2,6	3,4	3,4	2,9	3,1

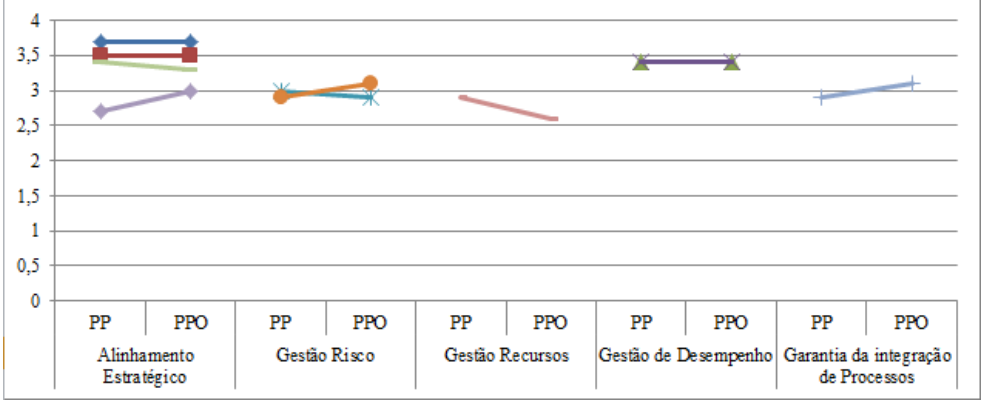


Gráfico 5.82- Factores Críticos de Sucesso: Mapeamento ISACA (Consultor das TI)

Todavia, e conforme já acima referido o Gestor/Funcionário de Segurança coloca o enfoque da criticidade do sucesso na adopção/implementação dum Sistema de Gestão da Segurança da Informação nas organizações, nos pilares de resultados – "*Garantia da integração de Processos*" e "*Gestão de Desempenho*", priorizando como elementos críticos de sucesso preferenciais a "*Responsabilização pela Segurança da Informação*" e as "*Auditorias de Segurança da Informação*". A tabela/gráfico (Gráfico 5.83) seguinte mostra o acima referido.

Factores Críticos de Sucesso (Nível médio de importância - Gestor/Funcionário da Segurança)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,7	3,7								
b) Suporte da Gestão de Topo	3,3	3,7								
c) Responsabilização pela Segurança da Informação							3,7	3,7		
d) Motivação dos funcionários							3,3	3,3		
e) Programas para a conscientização, educação e formação em segurança em informação			3,7	3,3						
f) Conformidade com Normas Internacionais de Segurança			3,3	3						
g) Auditorias de Segurança da Informação									3,7	3,7
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)					3	3				
i) Política de Segurança da Informação	3	3								
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,3	3,3								
Total (Valor médio)	3,325	3,425	3,5	3,15	3	3	3,5	3,5	3,7	3,7

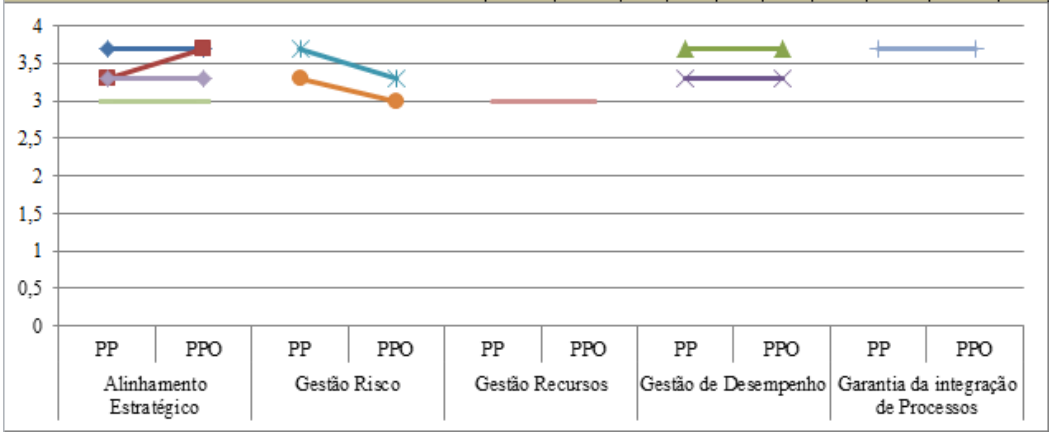


Gráfico 5.83- Factores Críticos de Sucesso: Mapeamento ISACA (Gestor/Funcionário da Segurança)

Por fim, o Trabalhador segue a mesma linha da perspectiva do Gestor de Topo, embora atribua pontuações de níveis médios de importância ligeiramente inferiores, mas apresentando uma gama mais restrita de valores na ordem dos (3,4 – 3,5). A tabela/gráfico (Gráfico 5.84) seguinte mostra o acima referido.

Factores Críticos de Sucesso (Nível médio de importância - Trabalhador)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,5	3,5								
b) Suporte da Gestão de Topo	3,4	3,4								
c) Responsabilização pela Segurança da Informação							3,5	3,4		
d) Motivação dos funcionários							3,6	3,4		
e) Programas para a conscientização, educação e formação em segurança em informação			3,5	3,4						
f) Conformidade com Normas Internacionais de Segurança			3,3	3,4						
g) Auditorias de Segurança da Informação									3,2	3,2
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)					3,1	3,1				
i) Politica de Segurança da Informação	3,5	3,4								
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,2	3,4								
Total (Valor médio)	3,4	3,425	3,4	3,4	3,1	3,1	3,55	3,4	3,2	3,2

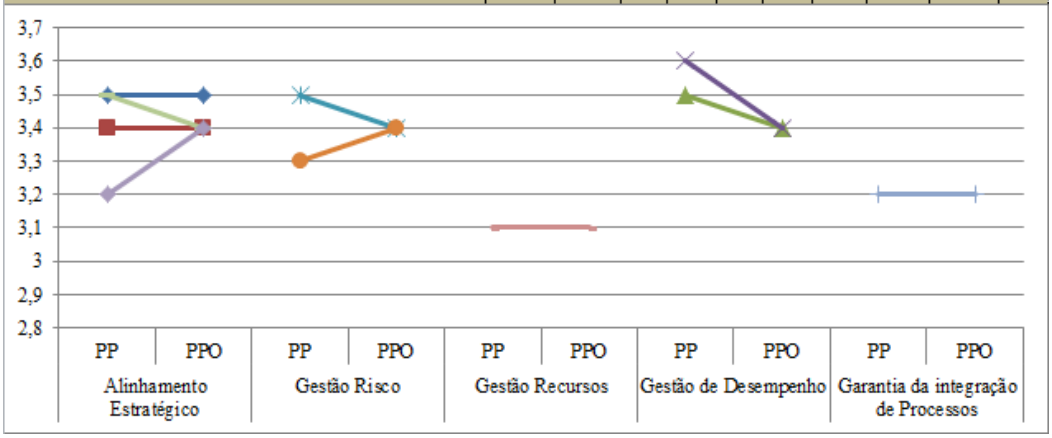


Gráfico 5.84- Factores Críticos de Sucesso: Mapeamento ISACA (Trabalhador)

5.3 - Factores de Boas Práticas

5.3.1 - Caracterização da Amostra

Neste ponto, exporemos os factos obtidos através da análise representada no modelo de resultados obtidos (Figura 5.15) e referentes aos Factores de Boas Práticas considerados na adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização.

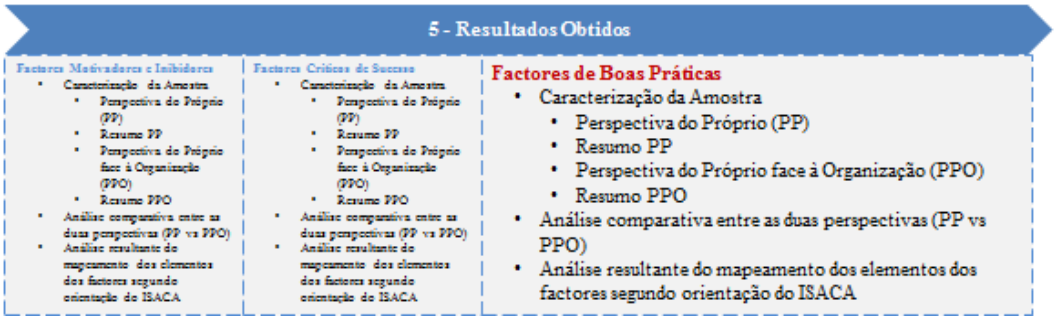


Figura 5.15- Modelo de Resultados Obtidos: FBP

Deste modo, lembra-se que foram sujeitos, aos respondentes, como Factores de Boas Práticas para a adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização, os seguintes elementos:

a) A minha senha de acesso não a partilho com ninguém

b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC

c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções

d) Devem existir programas para a conscientização, educação e formação em segurança

e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)

f) Devem existir auditorias de Segurança da Informação

g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)

h) Deve existir uma Política de Segurança da Informação

i) Deve existir Modelo/Programa de Governação para a Segurança da Informação

Assim, conforme acima indicado (Figura 5.15), a análise de dados teve em conta a classificação do grau de importância dada pelos respondentes incluindo as duas perspectivas: a do próprio e a

do próprio face à organização. De modo a aferir a existência ou não de desvios entre as duas vistas foi realizada a comparação entre as mesmas. Para tal, efectuou-se o cálculo do nível médio de importância para cada elemento deste factor.

5.3.2 - Perspectiva do Próprio

Neste item e de acordo com a referência seguida conforme indicado na figura abaixo (Figura 5.16), mostram-se os resultados deste ponto de vista, conseguidos através do tratamento dos dados efectuados às respostas obtidas na décima quinta questão do questionário elaborado (ver Anexo A).

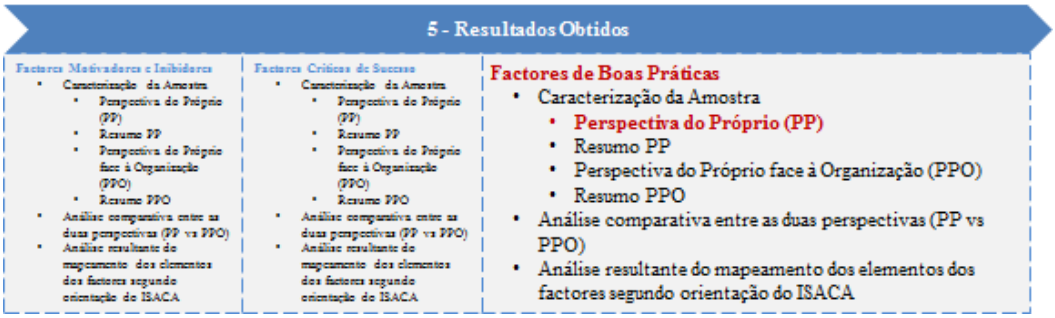


Figura 5.16- Modelo de Resultados Obtidos: FBP/PP

Logo, numa primeira fase, analisou-se a totalidade das respostas, verificando-se que, para este factor e de uma forma global, os nove elementos acima identificados são classificados nas categorias "Muito importante" ou "Importante" com uma predominância da votação na categoria "Importante". Nesta categoria, seis dos nove elementos de boas práticas considerados atingem valores superiores à metade percentual (50,00%), sendo os mais votados e com igual pontuação (64,46%) os seguintes: "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*".

Os elementos mais votados, na categoria "Muito importante", como Factores de Boas Práticas na implementação/adopção dum Sistema de Gestão da Segurança da Informação (SGSI) são: "*A minha senha de acesso não a partilho com ninguém*" (72,73%) e "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" (54,55%).

Na categoria "Pouco Importante", o elemento de boas práticas "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" surge como o mais preferido pelos respondentes (19,83%). Nesta categoria, o segundo e terceiro elementos mais votados são, respectivamente: "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" (18,18%) e "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" (14,05%).

Na categoria "Não é importante" são mencionados quatros dos nove elementos de boas práticas com valores percentuais pouco significativos (inferiores a 5,00%). No gráfico (Gráfico 5.85) seguinte encontra-se, detalhadamente o atrás indicado.

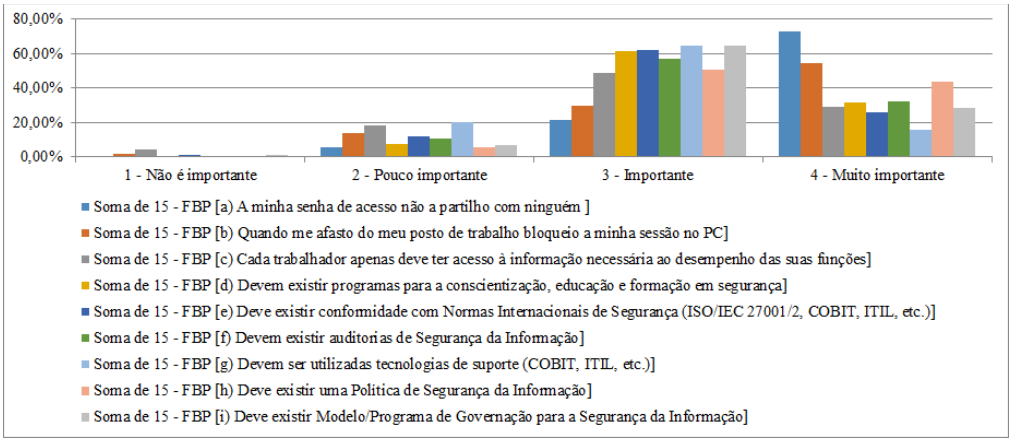


Gráfico 5.85- Factores de Boas Práticas: PP (Global)

Numa segunda fase, analisaram-se as respostas dos participantes, tendo em conta a sua função, no sentido de procurar o padrão de selecção dos elementos considerados como boas práticas na implementação/adopção de um SGSI para um Gestor de Topo, para um Gestor Intermédio, para um Gestor das TI, para um Consultor das TI, para um Gestor / Funcionário da Segurança e para um Trabalhador. Analisou-se e obteve-se os seguintes resultados.

Do ponto de vista do Gestor de Topo - conforme o gráfico (Gráfico 5.86) a seguir, verifica-se que todos os elementos são considerados como Factores de Boas Práticas e classificados com percentagens acima da metade percentual (50,00%) nas categorias "Muito importante" ou "Importante, situando-se o enfoque da votação na categoria "Muito importante".

Contudo, os elementos de boas práticas considerados "*Devem existir programas para a conscientização, educação e formação em segurança*", "*Deve existir uma Política de Segurança da Informação*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" atingem a totalidade da votação (100,00%), quando somados os resultados percentuais nas categorias "Muito importante" e "Importante".

Por outro lado, os três elementos mais votados como Factores de Boas Práticas na categoria "Muito Importante" são: "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" (80,00%), "*A minha senha de acesso não a partilho com ninguém*" e "*Devem existir auditorias de Segurança da Informação*", cada um, com igual pontuação (70,00%).

Para este grupo profissional, nenhum dos elementos de boas práticas considerados é classificado na categoria "Não é importante", mas o elemento "*Quando me afasto do meu posto de trabalho*

bloqueio a minha sessão no PC" obtém a classificação de (30,00%) e "*A minha senha de acesso não a partilho com ninguém*" atinge os (20,00%) na categoria "Pouco importante".

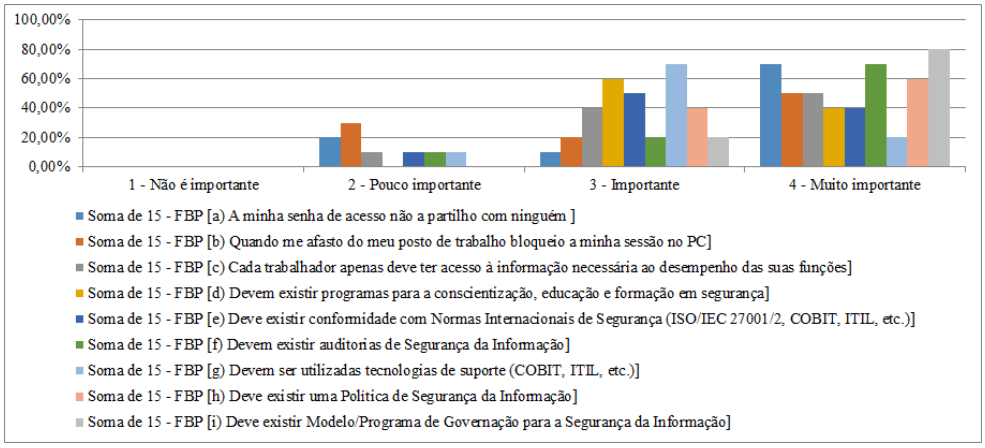


Gráfico 5.86- Factores de Boas Práticas: PP (Gestor de Topo)

Do ponto de vista do Gestor Intermédio – já para este gestor, todos os elementos continuam a ser considerados como Factores de Boas Práticas e classificados com percentagens acima da metade percentual (50,00%), quando somados os valores nas categorias "Muito importante" ou "Importante", verificando-se um enfoque maior na categoria "Importante".

Assim, na categoria "Muito importante" o elemento de boas práticas "*A minha senha de acesso não a partilho com ninguém*" é o único com uma votação maioritária (69,23%).

Na categoria "Importante", cinco dos nove elementos de boas práticas considerados atingem níveis de preferência superiores ou igual à metade percentual (50,00%), surgindo em primeiro lugar o elemento "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" (73,08%), seguido do elemento "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)"* (69,23%). Em terceiro e quarto lugar revelam-se, respectivamente, os seguintes elementos: "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" (65,38%) e "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" (61,54%). Por último, surge o elemento de boas práticas "*Devem existir auditorias de segurança da Informação*" (50,00%).

No entanto, comprova-se que todos os elementos mostram-se na categoria "Pouco importante", sendo o elemento "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" o mais votado (23,08%). Em segundo lugar surge o elemento de boas práticas "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" (15,38%). Aparecem, ainda, quatro dos nove elementos de boas práticas, classificados em terceiro lugar, com igual preferência (11,54%) e os restantes três elementos são elegíveis com apenas (3,85%) dos votos.

Na categoria "Não é importante" são apontados quatro dos nove elementos, surgindo o elemento de boas práticas "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" como o mais votado (7,69%). O gráfico (Gráfico 5.87) seguinte retrata o anteriormente mencionado.

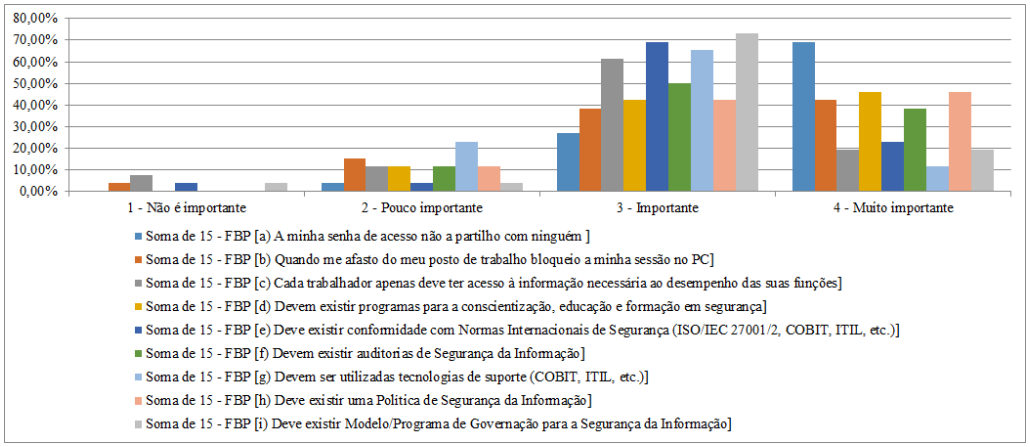


Gráfico 5.87- Factores de Boas Práticas: PP (Gestor Intermédio)

Do ponto de vista do Gestor das TI – para este gestor, conforme gráfico (Gráfico 5.88) seguinte, verifica-se que os elementos de boas práticas considerados "*A minha senha de acesso não a partilho com ninguém*" (82,35%) e "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" (76,47%) são os mais votados na categoria "Muito importante".

Porém, no primeiro elemento, o somatório das percentagens obtidas nas categorias "Muito importante" e "Importante", obtém a totalidade (100,00%) das preferências dos respondentes. O outro elemento que atinge esta mesma percentagem é "*Devem existir Auditorias de Segurança da Informação*". Mas aqui, a primazia recai na categoria "Importante" (70,59%).

Neste grupo profissional, os elementos considerados como Factores de Boas Práticas também surgem sempre maioritariamente populados nas categorias "Muito importante" e "Importante", mas o enfoque está na categoria "Importante". Nesta, seis dos nove elementos apresentam preferências na votação com valores significativos (superiores a 50,00%). Assim, os dois elementos de boas práticas mais escolhidos, nesta categoria, são: "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" e "*Devem existir programas para a conscientização, educação e formação em segurança*", assinalando valores percentuais iguais (76,47%) na votação.

Na categoria "Pouco Importante", sete dos nove elementos de boas práticas revelam-se populados, destacando-se igualmente (11,76%) dois elementos: "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Devem ser*

utilizadas tecnologias de suporte (COBIT, ITIL, etc.)". Os restantes elementos surgem todos com igual percentagem (5,88%).

O elemento de boas práticas "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" é o único elemento assinalado na categoria "Não é importante" (5,88%).

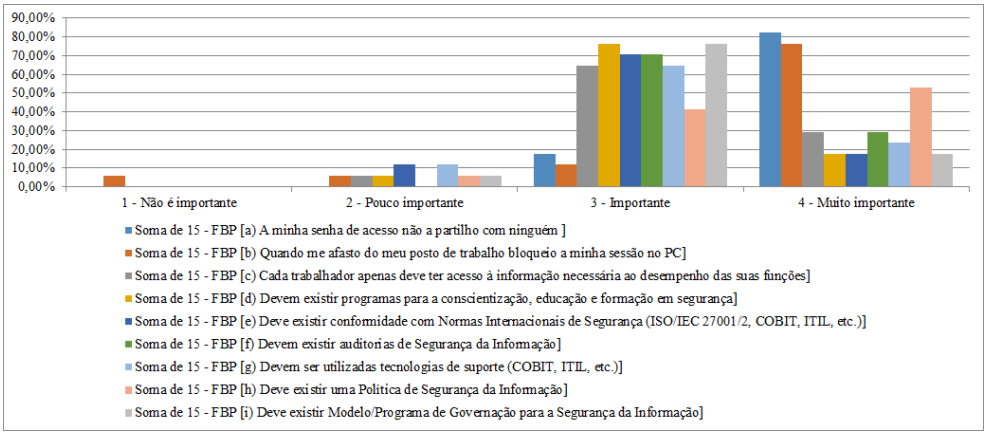


Gráfico 5.88- Factores de Boas Práticas: PP (Gestor das TI)

Do ponto de vista do Consultor das TI – nesta perspectiva verifica-se que a preferência da votação continua a incidir sobre as categorias "Muito importante" e "Importante", embora o enfoque esteja, mais uma vez, na categoria "Importante". De notar ainda, que três dos nove elementos considerados de boas práticas atingem a totalidade da votação (100,00%), quando somados os valores nestas categorias: "*A minha senha de acesso não a partilho com ninguém*", "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" e "*Deve existir uma Política de Segurança da Informação*".

Na categoria "Muito importante" os dois elementos de boas práticas mais votados são: "A minha senha de acesso não a partilho com ninguém" (85,71%) e "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" (71,43%).

Na categoria "Importante", visualizam-se dois elementos igualmente classificados em primeiro lugar (71,43%) e dois também indicados em segundo (64,29%), a saber, respectivamente: "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*"; "*Devem existir programas para a conscientização, educação e formação em segurança*" e "*Devem existir auditorias de Segurança da Informação*".

Na categoria "Pouco importante", seis dos nove elementos aparecem populados. Mas, o elemento de boas práticas "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" obtém uma votação cerca da metade percentual (42,86%) e o elemento "*Devem existir*

programas para a conscientização, educação e formação em segurança" agrupa um valor perto de um quarto (21,43%) das preferências.

Na categoria "Não é importante", apenas é votado o elemento de boas práticas: "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" (7,14%). O gráfico (Gráfico 5.89) seguinte reflecte o acima mencionado.

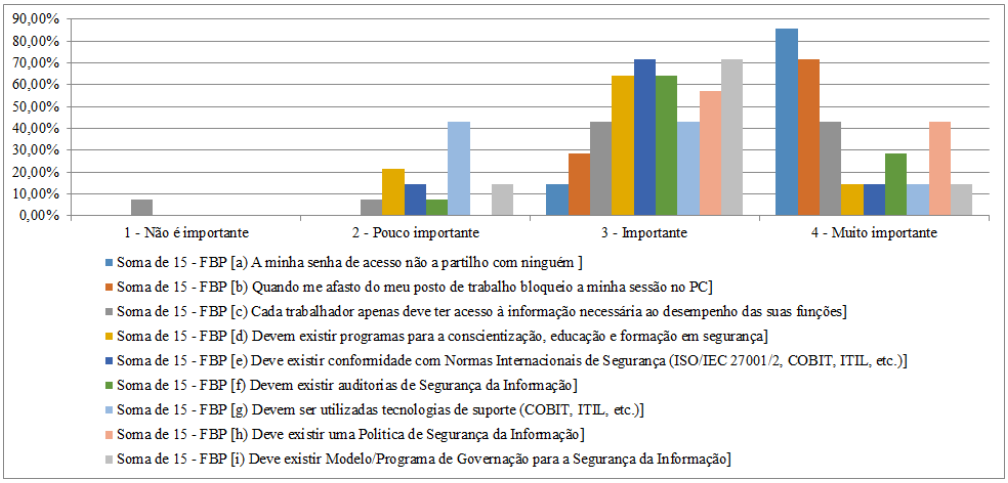


Gráfico 5.89- Factores de Boas Práticas: PP (Consultor das TI)

Do ponto de vista do Gestor / Funcionário da Segurança – esta classe apresenta uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). Os elementos apresentam todos valores percentuais acima da metade percentual (50,00%), quando somados os valores nas categorias "Muito importante" e "Importante", com prevalência nesta última. Os elementos de boas práticas "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" obtêm a totalidade da votação (100,00%) na categoria "Importante".

Na categoria "Muito importante", surgem os elementos de boas práticas "*A minha senha de acesso não a partilho com ninguém*" e "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" como os mais votados na categoria (66,67%).

Este grupo profissional aponta ainda como "Pouco importante" três dos nove elementos: "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*", "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Deve existir uma Política de Segurança da Informação*", todos com igual classificação (33,33%).

Na categoria "Não é importante" não se encontra nenhuma votação. O gráfico (Gráfico 5.90) seguinte ilustra o atrás referido.

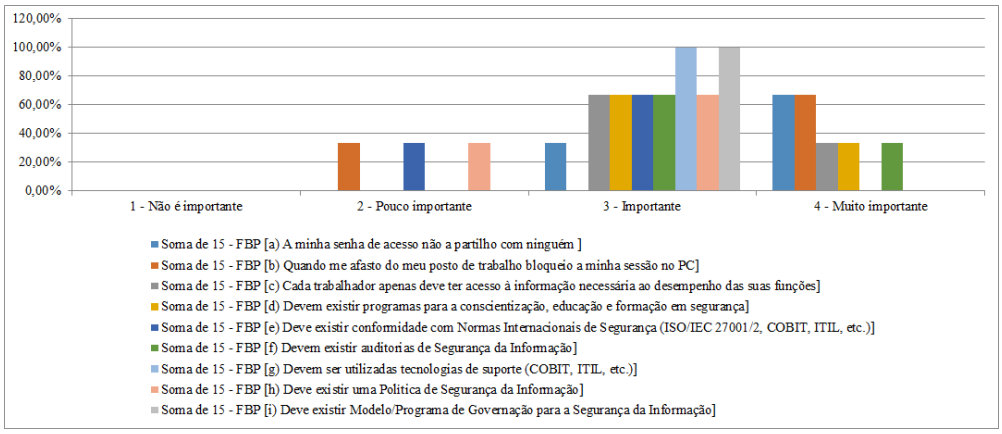


Gráfico 5.90- Factores de Boas Práticas: PP (Gestor/Funcionário da Segurança)

Do ponto de vista do Trabalhador – também nesta perspectiva, todos os elementos de boas práticas considerados, apresentam valores acima da metade percentual (50,00%), quando somados nas categorias "Importante" e "Muito importante", havendo uma predominância da votação na primeira categoria.

Assim, o elemento considerado de boas práticas mais votado na categoria "Importante" é "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" (66,67%), seguido do elemento "*Devem existir programas para a conscientização, educação e formação em segurança*" (64,71%).

Por outro lado, na categoria "Muito importante" vence o elemento de boas práticas "*A minha senha de acesso não a partilho com ninguém*" (68,63%), seguido do elemento "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" (49,02%).

Relativamente à categoria "Pouco importante" todos os elementos são considerados, agrupando maior classificação o elemento de boas práticas "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" (31,37%).

Na categoria "Não é importante" surge apenas o elemento "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" (3,92%). O gráfico (Gráfico 5.91) seguinte reflecte o acima exposto.

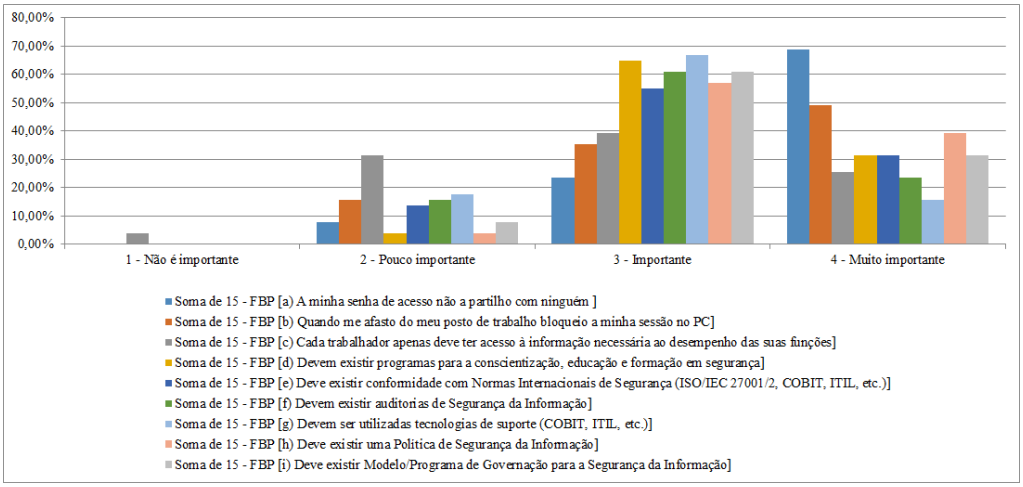


Gráfico 5.91- Factores de Boas Práticas: PP (Trabalhador)

5.3.3 – Resumo da Perspectiva do Próprio

Assim, seguindo a metodologia apresentada na figura seguinte (Figura 5.17) e resumindo, na tabela (Tabela 5.28) apresenta-se a ordenação pela categoria "Muito importante" e "Não é importante" dos elementos considerados para o estudo como Factores de Boas Práticas, segundo cada uma das vistas dadas pela função do respondente.

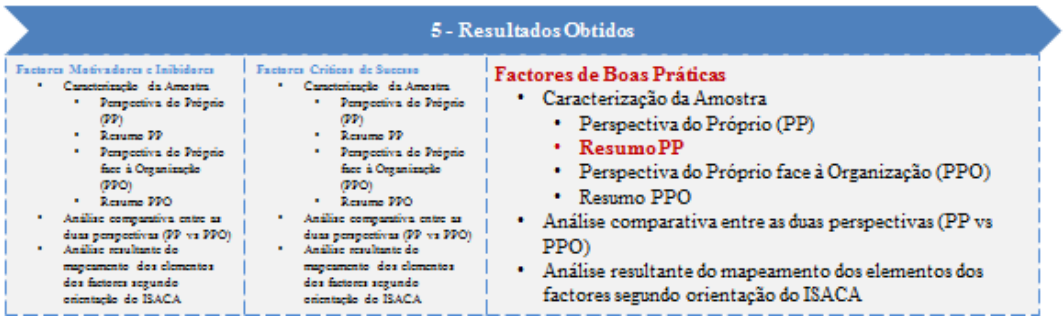


Figura 5.17- Modelo de Resultados Obtidos: FBP/Resumo da PP

Neste contexto, e conforme se pode visualizar (Tabela 5.28), o elemento de boas práticas "*A minha senha de acesso não a partilho com ninguém*" é o mais referido em primeiro lugar na categoria "Muito importante".

Contudo, o Gestor de Topo coloca-o em segundo lugar dando preferência ao elemento de boas práticas "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*".

Por outro lado, os Gestores Intermédios e das TI votam, neste último elemento, em sexto lugar dando a sua preferência ao primeiro elemento mencionado.

Relativamente à categoria "Não é importante" o Gestor de Topo e o Gestor/Funcionário de Segurança não indicam nenhum dos elementos. O Gestor Intermédio aponta quatro dos nove elementos: "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho*

das suas funções", "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*", "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*". Os outros tipos de respondentes apontam um elemento nesta categoria. O Consultor das TI e o Trabalhador indicam "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*". O Gestor das TI menciona o elemento considerado de boas práticas "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*".

Factores Boas Práticas - PP (- Elemento não é referido pelos respondentes)		15 - FBP [a] A minha senha de acesso não a partilho com ninguém]	15 - FBP [b] Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC]	15 - FBP [c] Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções]	15 - FBP [d] Devem existir programas para a conscientização, educação e formação em segurança]	15 - FBP [e] Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)]	15 - FBP [f] Devem existir auditorias de Segurança da Informação]	15 - FBP [g] Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)]	15 - FBP [h] Deve existir uma Política de Segurança da Informação]	15 - FBP [i] Deve existir Modelo/Programa de Governação para a Segurança da Informação]
Gestor de Topo	Muito importante	2	4	4	5	5	2	6	3	1
	Não é importante	-	-	-	-	-	-	-	-	-
Gestor Intermédio	Muito importante	1	3	6	2	5	4	7	2	6
	Não é importante	-	2	1	-	2	-	-	-	2
Gestor das TI	Muito importante	1	2	4	6	6	4	5	3	6
	Não é importante	-	1	-	-	-	-	-	-	-
Consultor das TI	Muito importante	1	2	3	5	5	4	5	3	5
	Não é importante	-	-	1	-	-	-	-	-	-
Gestor / Funcionário da Segurança	Muito importante	1	1	2	2	-	2	-	-	-
	Não é importante	-	-	-	-	-	-	-	-	-
Trabalhador	Muito importante	1	2	5	4	4	6	7	3	4
	Não é importante	-	-	1	-	-	-	-	-	-
Global	**Muito importante**	**1**	**2**	**6**	**5**	**8**	**4**	**9**	**3**	**7**
	Não é importante	**-**	**2**	**1**	**-**	**3**	**-**	**-**	**-**	**3**

Tabela 5.28- Factores de Boas Práticas - PP: Ordenação das preferências

5.3.4 – Perspectiva do Próprio face à Organização

Continuando na mesma linha de apresentação dos resultados obtidos (Figura 5.18), neste ponto mostram-se as preferências indicadas pelos respondentes, baseadas no tratamento dos dados efectuados às respostas obtidas à décima sexta questão do questionário elaborado (ver Anexo A).

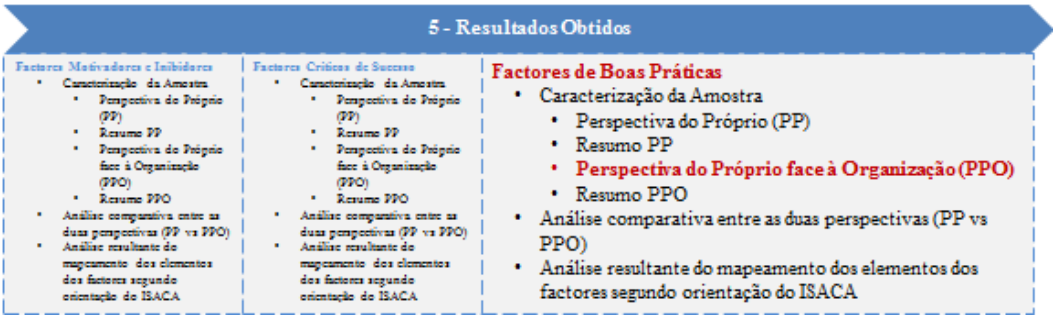


Figura 5.18- Modelo de Resultados Obtidos: FBP/PPO

Numa primeira fase, analisou-se também a totalidade das respostas, verificando-se que, para este factor, de uma forma global, os nove elementos considerados de boas práticas e atrás identificados, são classificados nas categorias "Muito importante" ou "Importante", com predominância da votação na categoria "Importante".

Assim, na categoria "Importante", cinco dos nove elementos considerados de boas práticas atingem valores maioritários (superiores a 50,00%), mas os três mais votados são: "*Devem existir programas para a conscientização, educação e formação em segurança*" (62,81%), "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" com igual votação (61,98%).

Os Factores de Boas Práticas mais votados, na categoria "Muito importante" na implementação/adopção dum Sistema de Gestão da Segurança da Informação são: "*A minha senha de acesso não a partilho com ninguém*" (66,12%) e "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" (50,41%).

Todos os elementos encontram-se populados na categoria "Pouco Importante", mas o elemento considerado de boas práticas "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" surge como o mais seleccionado pelos respondentes (19,83%). Nesta categoria o segundo e terceiro elemento mais votados são, respectivamente: "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" (19,01%) e "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" (15,70%).

Na categoria "Não é importante" são mencionados sete, dos nove elementos, com valores percentuais pouco significativos (inferiores a 5,00%). No gráfico (Gráfico 5.92) seguinte visualiza-se o pormenor do anteriormente indicado.

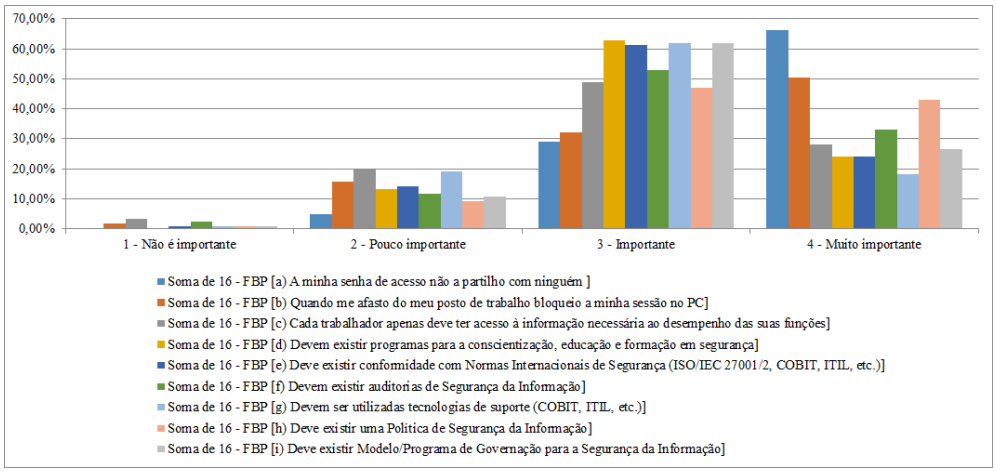


Gráfico 5.92- Factores de Boas Práticas: PPO (Global)

Numa segunda fase, foram analisadas as respostas dos participantes, tendo em conta a sua função, de forma a verificar se os elementos considerados como Factores de Boas Práticas na implementação/adopção de um SGSI diferiam ou não entre as classes seleccionadas: Gestor de Topo, Gestor Intermédio, Gestor das TI, Consultor das TI, Gestor / Funcionário da Segurança e Trabalhador. Investigou-se e obtiveram-se os seguintes resultados.

Do ponto de vista do Gestor de Topo - conforme gráfico (Gráfico 5.93) a seguir, constata-se que todos os elementos são considerados como Factores de Boas Práticas e classificados com percentagens acima da metade percentual (50,00%), quando somados nas categorias "Muito importante" ou "Importante, situando-se o enfoque da votação na categoria "Muito importante".

Assim, o elemento mais votado como Factores de Boas Práticas na categoria "Muito Importante" é: "*Deve existir uma Política de Segurança*" (70,00%). Porém, os elementos "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*", "*A minha senha de acesso não a partilho com ninguém*" e "*Devem existir auditorias de Segurança da Informação*" atingem, cada um, uma pontuação idêntica (60,00%).

Em relação à categoria "Importante", surgem como elementos de boas práticas de votação maioritária os seguintes: "*Devem existir programas para a conscientização, educação e formação em segurança*" e "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*", obtendo, cada um, igual percentagem (60,00%).

Note-se que a opinião deste tipo de respondente em relação ao elemento "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)"* encontra-se igualmente dividida pelas categorias "Muito importante" e "Importante" onde supera o um terço percentual (40,00%) cada, sendo o restante valor (20,00%) atribuído à categoria "Pouco importante".

Relativamente à categoria "Pouco importante", verifica-se que são mencionados seis dos nove elementos considerados de boas práticas, a saber: "*A minha senha de acesso não a partilho com ninguém*", "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" e "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" obtendo, cada um, classificação semelhante (20,00%).

Ainda para este grupo profissional, quatro dos nove elementos considerados são classificados na categoria "Não é importante": "*Devem existir auditorias de segurança*", "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*", "*Deve existir uma Política de Segurança*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" apresentando, cada um, valores percentuais idênticos (10,00%).

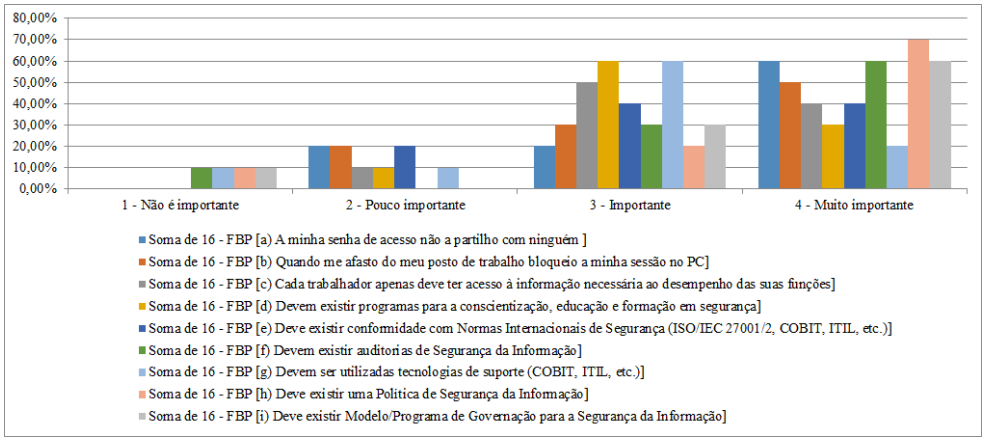


Gráfico 5.93- Factores de Boas Práticas: PPO (Gestor de Topo)

Do ponto de vista do Gestor Intermédio – já para este gestor, todos os elementos continuam a ser considerados como Factores de Boas Práticas e classificados com percentagens acima da metade percentual (50,00%), quando somados nas categorias "Muito importante" ou "Importante", verificando-se um enfoque maior na categoria "Importante".

Assim, na categoria "Muito importante" o elemento "*A minha senha de acesso não a partilho com ninguém*" é o único com uma votação maioritária (65,38%). Este elemento atinge a totalidade do valor percentual (100,00%), quando somados os valores desta categoria com a categoria "Importante".

Na categoria "Importante" cinco dos nove elementos atingem níveis maioritários de preferência (superiores a 50,00%), surgindo em primeiro lugar o elemento de boas práticas "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" (73,08%) seguido dos elementos "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" que obtêm, cada um, uma votação idêntica (65,38%). Em terceiro e quarto lugar mostram-

se, respectivamente, os seguintes elementos: "*Devem existir programas para a conscientização, educação e formação em segurança*" (57,69%) e "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" (53,85%).

No entanto, comprova-se que oito dos nove elementos considerados de boas práticas mostram-se populados na categoria "Pouco importante", sendo os elementos "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*", "*Devem existir auditorias de Segurança da Informação*" e "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" aqueles que atingem igual e maior votação (19,23%).

Na categoria "Não é importante" são apontados dois dos nove elementos considerados de boas práticas, revelando-se o elemento "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" como o mais votado (7,69%). O gráfico (Gráfico 5.94) seguinte retrata o anteriormente mencionado.

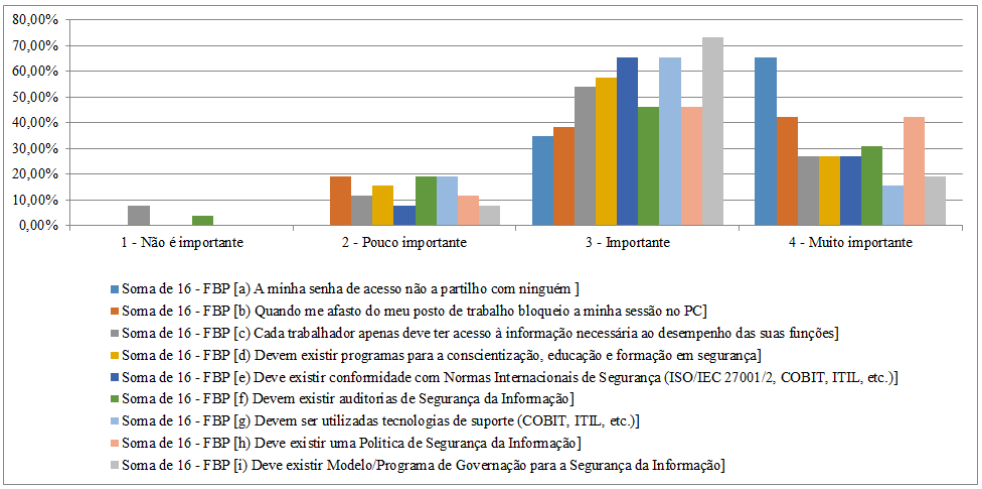


Gráfico 5.94- Factores de Boas Práticas: PPO (Gestor Intermédio)

Do ponto de vista do Gestor das TI – para este gestor, e conforme gráfico (Gráfico 5.95) abaixo, verifica-se que os elementos considerados de boas práticas "*A minha senha de acesso não a partilho com ninguém*" (76,47%) e "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no* PC" (64,71%) são os mais votados na categoria "Muito importante".

Porém, no primeiro elemento, o somatório das percentagens obtidas nas categorias "Muito importante" e "Importante" obtém a unanimidade (100,00%) das preferências dos respondentes. Os outros elementos que atingem esta mesma percentagem são: "*Devem existir programas para a conscientização, educação e formação em segurança*" e "*Devem existir auditorias de Segurança da Informação*". Mas aqui, as preferências vão para a categoria "Importante" com, respectivamente um valor maioritário (76,47%) para o primeiro e de um valor bastante significativo (70,59%) para o segundo elemento mencionados.

Também neste grupo profissional, os elementos considerados como Factores de Boas Práticas revelam-se sempre maioritariamente populados nas categorias "Muito importante" e "Importante", notando-se um enfoque na categoria "Importante", pois, seis dos nove elementos apresentam preferências na votação, atingindo valores superiores à metade percentual (50,00%). Assim, o elemento de boas práticas "*Devem existir programas para a conscientização, educação e formação em segurança*" mostra-se como o mais seleccionado nesta categoria (76,47%).

Na categoria "Pouco Importante", cinco dos nove elementos considerados de boas práticas surgem populados, destacando-se dois elementos: "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*", cada um, com uma votação igual (11,76%). Os restantes elementos mostram todos valores percentuais semelhantes (5,88%).

O elemento considerado de boas práticas "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" é o único elemento assinalado na categoria "Não é importante" com um valor pouco significativo (5,88%) das preferências.

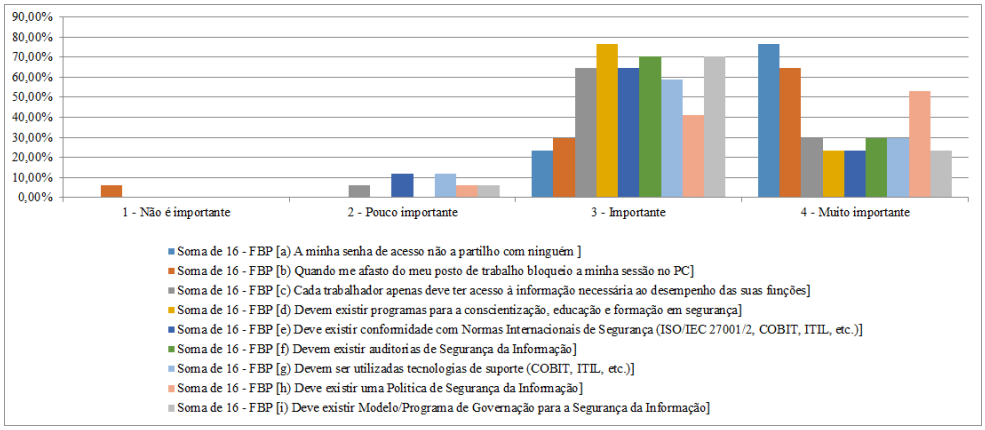


Gráfico 5.95- Factores de Boas Práticas: PPO (Gestor das TI)

Do ponto de vista do Consultor das TI – nesta perspectiva, continua a verificar-se a predominância da votação nas categorias "Muito importante" e "Importante", embora o enfoque esteja, mais uma vez, na categoria "Importante".

Na categoria "Muito importante" os dois elementos considerados de boas práticas mais votados são: "*A minha senha de acesso não a partilho com ninguém*" (78,57%) e "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" (57,14%).

Na categoria "Importante" revela-se, em primeiro lugar, o elemento "*Devem existir auditorias de Segurança da Informação*" (64,29%) e visualizam-se três elementos igualmente classificados em segundo lugar (57,14%), a saber: "*Devem existir programas para a conscientização,*

educação e formação em segurança", "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*".

Na categoria "Pouco importante" todos os elementos considerados de boas práticas aparecem populados, encontrando-se em primeiro lugar três dos nove elementos agrupando, cada um, valor análogo das preferências (35,71%): "*Devem existir programas para a conscientização, educação e formação em segurança*", "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*".

Na categoria "Não é importante" apenas é votado o elemento: "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" (7,14%). O gráfico (Gráfico 5.96) seguinte ilustra o acima mencionado.

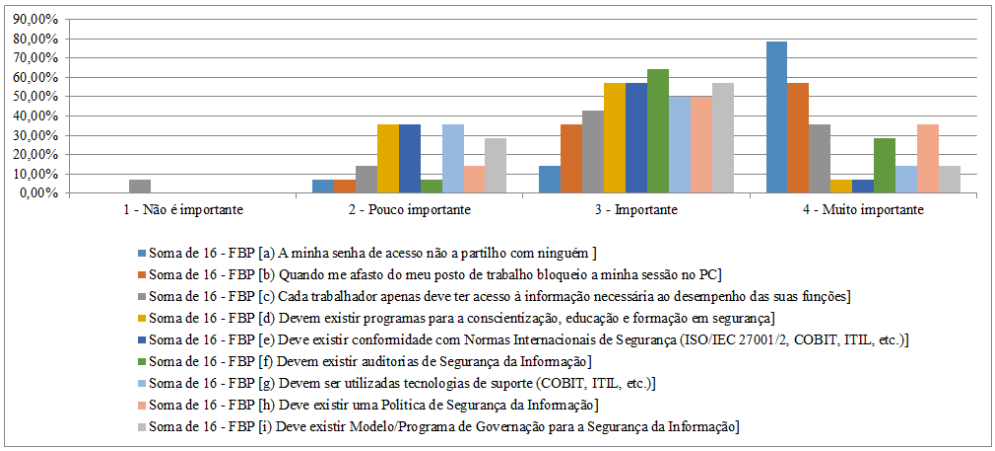


Gráfico 5.96- Factores de Boas Práticas: PPO (Consultor das TI)

Do ponto de vista do Gestor / Funcionário da Segurança – esta classe apresenta uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). Os elementos apresentam todos valores acima da metade percentual (50,00%), quando somados nas categorias "Muito importante" e "Importante", com prevalência nesta última.

Porém, o elemento "*A minha senha de acesso não a partilho com ninguém*" atinge a totalidade percentual (100,00%) na categoria "Muito importante" e os elementos "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" e "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" obtêm aquela pontuação (100,00%) na categoria "Importante".

Este grupo profissional aponta, ainda, como "Pouco importante" o elemento: "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" (33,33%).

Na categoria “Não é importante” não se encontra nenhuma votação. No gráfico (Gráfico 5.97) seguinte retrata o atrás exposto.

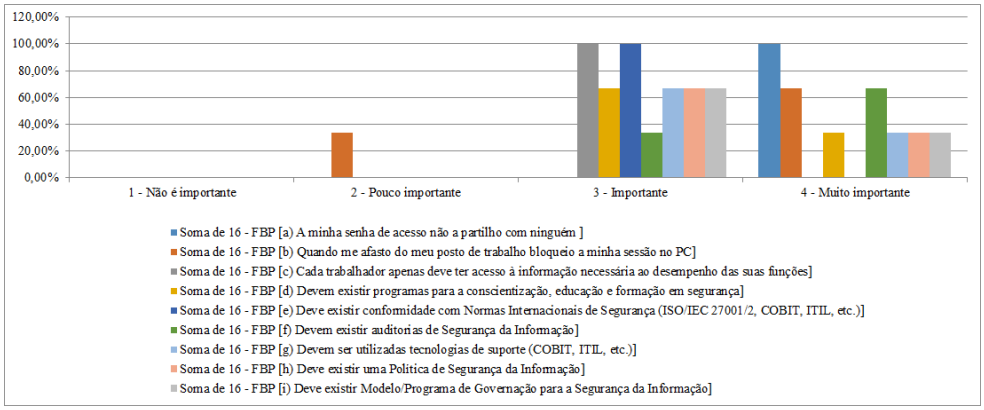


Gráfico 5.97- Factores de Boas Práticas: PPO (Gestor/Funcionário da Segurança)

Do ponto de vista do Trabalhador – também nesta vista, todos os elementos considerados, apresentam valores percentuais maioritários (superiores a 50,00%), quando somados nas categorias “Muito importante” e “Importante”, havendo uma primazia da votação nesta última categoria.

Assim, o elemento considerado de boas práticas mais votado na categoria “Importante” é “*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*” (64,71%), seguido do elemento “*Devem existir programas para a conscientização, educação e formação em segurança*” (62,75%).

Por outro lado, na categoria “Muito importante” vence o elemento considerado de boas práticas “*A minha senha de acesso não a partilho com ninguém*” (58,82%), seguido do elemento “*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*” (47,06%).

Relativamente à categoria “Pouco importante” todos os elementos são considerados, surgindo no topo o elemento “*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*” (33,33%).

Na categoria “Não é importante” revelam-se quatro dos nove elementos agrupando, cada um, valores percentuais semelhantes (1,96%). No gráfico (Gráfico 5.98) seguinte visualiza-se o atrás mencionado.

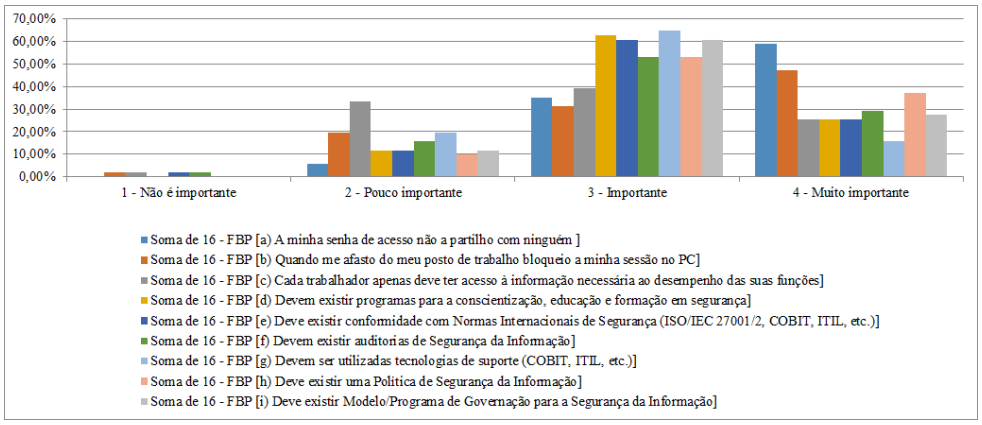


Gráfico 5.98- Factores de Boas Práticas: PPO (Trabalhador)

5.3.5 – Resumo da Perspectiva do Próprio face à Organização

Neste ponto, segue-se o referencial expositivo conforme mostrado na figura seguinte (Figura 5.19).

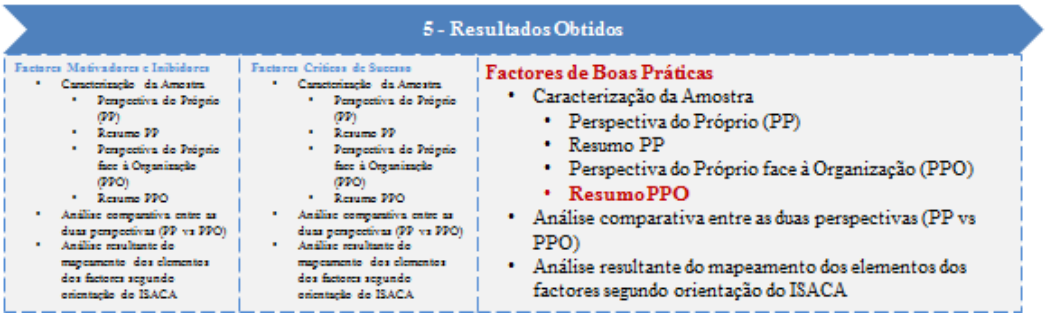


Figura 5.19- Modelo de Resultados Obtidos: FBP/Resumo da PPO

Resumindo, na tabela (Tabela 5.29) seguinte apresenta-se a ordenação pela categoria "Muito importante" e "Não é importante" dos elementos considerados para o estudo como Factores de Boas Práticas, segundo cada uma das vistas dadas pela função do respondente.

Factores Boas Práticas - PPO (- Elemento não é referido pelos respondentes)		16 - FBP [a) A minha senha de acesso não a partilho com ninguém]	16 - FBP [b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC]	16 - FBP [c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções]	16 - FBP [d) Devem existir programas para a consciencialização, educação e formação em segurança]	16 - FBP [e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)]	16 - FBP [f) Devem existir auditorias de Segurança da Informação]	16 - FBP [g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)]	16 - FBP [h) Deve existir uma Política de Segurança da Informação]	16 - FBP [i) Deve existir Modelo/Programa de Governação para a Segurança da Informação]
Gestor de Topo	Muito importante	2	3	4	5	4	2	6	1	2
	Não é importante	-	-	-	-	-	1	1	1	1
Gestor Intermédio	Muito importante	1	2	4	4	4	3	6	2	5
	Não é importante	-	-	1	-	-	2	-	-	-
Gestor das TI	Muito importante	1	2	4	5	5	4	4	3	5
	Não é importante	-	1	-	-	-	-	-	-	-
Consultor das TI	Muito importante	1	2	3	6	6	4	5	3	5
	Não é importante	-	-	1	-	-	-	-	-	-
Gestor / Funcionário da Segurança	Muito importante	1	2	-	3	-	2	3	3	3
	Não é importante	-	-	-	-	-	-	-	-	-
Trabalhador	Muito importante	1	2	6	6	6	4	7	3	5
	Não é importante	-	1	1	-	1	1	-	-	-
Global	**Muito importante**	**1**	**2**	**5**	**7**	**7**	**4**	**8**	**3**	**6**
	Não é importante	**-**	**3**	**1**	**-**	**4**	**2**	**4**	**4**	**4**

Tabela 5.29 - Factores de Boas Práticas - PPO: Ordenação das preferências

Conforme se pode constatar, o elemento considerado de boas práticas "*A minha senha de acesso não a partilho com ninguém*" obtém a primazia na categoria "Muito importante".

Contudo, o Gestor de Topo coloca-o em segundo lugar dando preferência ao elemento "*Deve existir uma Política de Segurança da Informação*". Por outro lado, o Gestor Intermédio coloca este elemento em segundo lugar e os restantes tipos de respondentes classificam, este elemento, em terceiro lugar.

Relativamente à categoria "Não é importante" o Gestor/Funcionário de Segurança não indica nenhum dos elementos. Porém, todos os outros tipos de respondentes referem elementos nesta categoria, a saber:

- O Gestor de Topo aponta quatro dos nove elementos considerados de boas práticas, todos com a mesma votação: "*Devem existir auditorias de Segurança da Informação*", "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*", "*Deve existir uma Política de Segurança da Informação*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*".
- O Gestor Intermédio indica dois dos nove elementos: "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" e "*Devem existir auditorias de Segurança da Informação*".
- O Gestor das TI e o Consultor das TI seleccionam, cada um, um elemento nesta categoria. O Gestor das TI menciona o elemento considerado de boas práticas "*Quando*

me afasto do meu posto de trabalho bloqueio a minha sessão no PC" e o Consultor das TI elege "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*".

- O Trabalhador designa quatro dos nove elementos: "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*", "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*", "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Devem existir auditorias de Segurança da Informação*".

5.3.6 - Análise Comparativa entre as duas Perspectivas (Próprio e Próprio face à Organização)

Neste ponto, tomando como modelo de resultados obtidos os referenciais apresentados na figura seguinte (Figura 5.20), seguidamente expõem-se os factos alcançados e comparativos das duas perspectivas dos respondentes (a do próprio e a do próprio face à organização/sector) relativamente aos factores considerados de boas práticas.

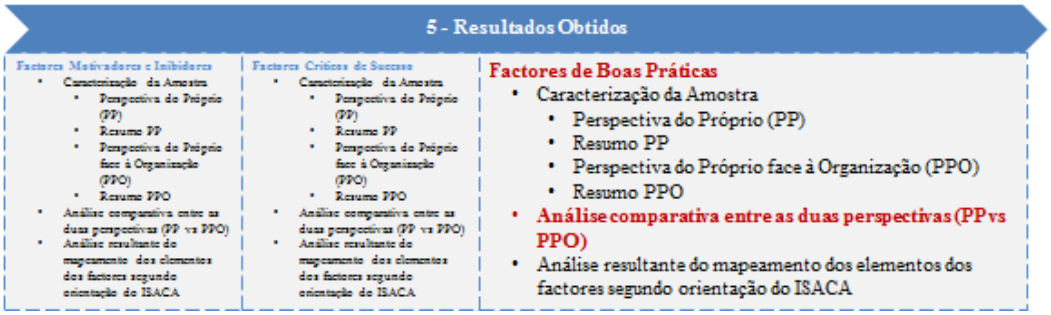


Figura 5.20- Modelo de Resultados Obtidos: FBP/Análise Comparativa

Assim, primeiramente efectuou-se o cálculo do nível médio de importância para cada elemento deste factor, através da seguinte fórmula:

$$\text{Nível médio de importância} = \frac{\sum_{c=1}^{4}(nº\ de\ referências\ ao\ elemento * c)}{n.º\ de\ respondentes}$$

em que a variável "c" corresponde ao valor da categoria de classificação (1-Não é importante; 2-Pouco importante; 3-Importante e 4-Muito importante) seleccionado pelo respondente para o elemento em causa.

Deste modo, na tabela (Tabela 5.30) seguinte apontam-se os valores médios encontrados para todos os elementos considerados como Factores de Boas Práticas, tendo em conta todas as respostas chegadas.

Factores de Boas Práticas	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
A minha senha de acesso não a partilho com ninguém	3,7	3,6	0,1
Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	3,4	3,5	-0,1
Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	3,0	3,5	-0,5
Devem existir programas para a conscientização, educação e formação em segurança	3,2	3,4	-0,2
Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	3,1	3,3	-0,2
Devem existir auditorias de Segurança da Informação	3,2	3,2	0,0
Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	3,0	3,2	-0,2
Deve existir uma Política de Segurança da Informação	3,4	3,0	0,4
Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,2	3,3	-0,1

Tabela 5.30- Factores de Boas Práticas: valores Nível Médio de Importância (Global)

Na tabela (Tabela 5.30) anterior, pode constatar-se que, em oito dos nove elementos considerados como Factores de Boas Práticas para a adopção/implementação de um SGSI numa organização do sector das águas/saneamento em Portugal, a perspectiva do próprio apresenta desvios na classificação dos mesmos relativamente à perspectiva do próprio face à organização.

Assim, o único elemento que mantém a mesma pontuação nas duas perspectivas é: "*Devem existir auditorias de Segurança da Informação*".

Pode, igualmente, verificar-se que o nível médio de importância - na perspectiva do próprio, é maior em dois dos nove elementos considerados, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, apresentando valores de desvio de (0,1) para o elemento "*A minha senha de acesso não a partilho com ninguém*" e de (0,4) para o elemento "*Deve existir uma Política de Segurança da Informação*".

Porém, nos restantes elementos considerados de boas práticas, a perspectiva do próprio apresenta níveis médios de importância inferiores aos níveis médios de importância na perspectiva do próprio face à organização, verificando-se valores para os desvios entre (0,1) e (0,5). Os elementos que agrupam menor valor absoluto do desvio (0,1) para o nível médio de importância são: "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*". O elemento que atinge maior valor absoluto de desvio (0,5) para o nível médio de importância é: "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*".

Para uma melhor visualização desses desvios apresenta-se o gráfico (Gráfico 5.99) "radar" seguinte:

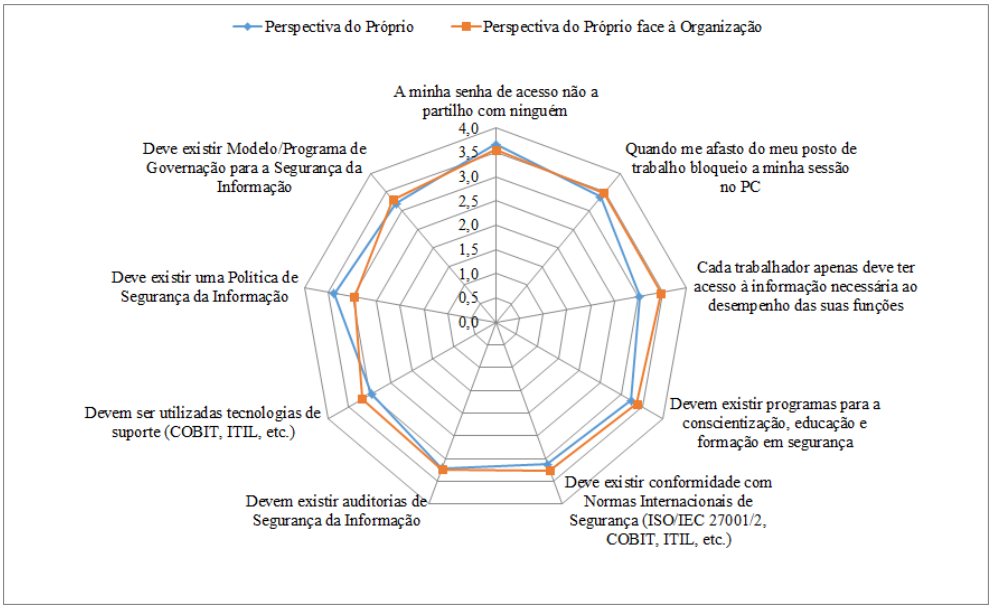


Gráfico 5.99- Factores de Boas Práticas: Comparação entre PP e PPO (Global)

Para uma melhor compreensão da origem dos desvios, isto é, para aferir que tipo de respondentes contribuíram para a apresentação destes desvios, elaborou-se também o cálculo do nível médio de importância, para cada elemento deste factor, cruzando-se o tipo de função do respondente, tendo-se chegado aos seguintes resultados:

Do ponto de vista do Gestor de Topo - a tabela (Tabela 5.31) a seguir mostra que as opiniões dos gestores de topo, que representam (8,26%) dos respondentes, apresentam desvios na classificação do nível de importância em todos os nove elementos considerados, quando comparada a perspectiva do próprio relativamente à perspectiva do próprio face à organização.

Assim, verifica-se que o nível médio de importância - na perspectiva do próprio, é maior em oito dos nove elementos considerados, quando comparado com o nível de importância – na perspectiva do próprio face à organização, apresentando valores de desvio de (0,1) para os elementos: "*A minha senha de acesso não a partilho com ninguém*", "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*", "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Deve existir uma Política de Segurança da Informação*" e de (0,4) para o elemento "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*".

Porém, no elemento "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" o valor do desvio é negativo e igual (-0,1) pois representa a existência de um maior nível médio de importância, quando comparado o elemento na perspectiva do próprio relativamente à perspectiva do próprio face à organização.

Factores de Boas Práticas	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
A minha senha de acesso não a partilho com ninguém	3,5	3,4	0,1
Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	3,2	3,3	-0,1
Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	3,4	3,3	0,1
Devem existir programas para a conscientização, educação e formação em segurança	3,4	3,2	0,2
Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	3,3	3,2	0,1
Devem existir auditorias de Segurança da Informação	3,6	3,4	0,2
Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	3,1	2,9	0,2
Deve existir uma Política de Segurança da Informação	3,6	3,5	0,1
Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,8	3,4	0,4

Tabela 5.31- Factores de Boas Práticas: valores Nível Médio de Importância (Gestor de Topo)

O gráfico (Gráfico 5.100) radar abaixo mostra as diferenças acima mencionadas.

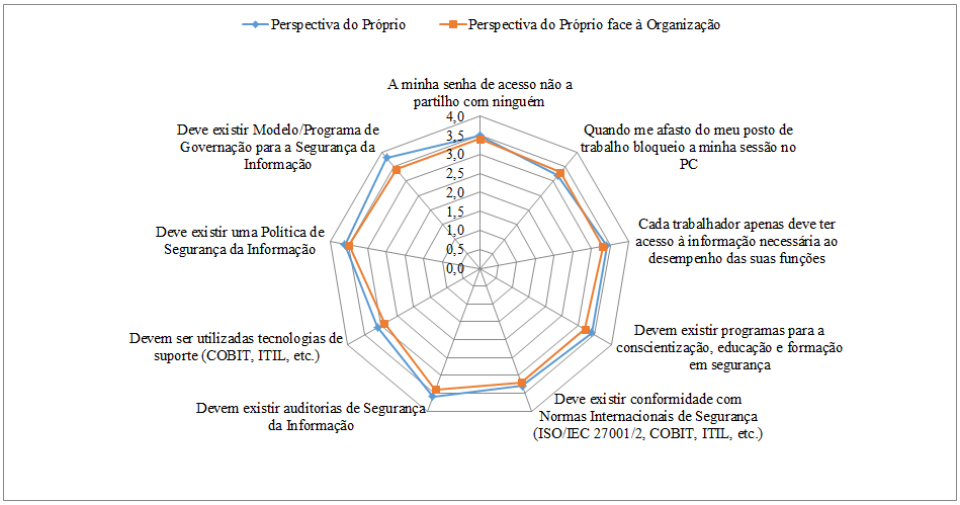


Gráfico 5.100- Factores de Boas Práticas: Comparação entre PP e PPO (Gestor de Topo)

Do ponto de vista do Gestor Intermédio - a tabela (Tabela 5.32) seguinte, mostra que as opiniões dos gestores intermédios, que representam (21,49%) dos respondentes, também apresentam desvios na classificação do nível médio de importância em cinco, dos nove elementos considerados, quando comparada a perspectiva do próprio relativamente à perspectiva do próprio face à organização.

Assim, comprova-se que o nível médio de importância - na perspectiva do próprio, é maior em dois dos nove elementos considerados de boas práticas, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, apresentando valores de desvio para o elemento "*Devem existir programas para a conscientização, educação e formação em segurança*" (0,2) e para o elemento "*Devem existir auditorias de Segurança da Informação*" (0,3).

Todavia, nos restantes elementos, a perspectiva do próprio apresenta níveis médios de importância inferiores ao nível médio de importância na perspectiva do próprio face à organização, verificando-se valor absoluto idêntico (0,1) para os desvios referentes aos seguintes elementos: "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*", "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" e "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*".

Factores de Boas Práticas	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
A minha senha de acesso não a partilho com ninguém	3,7	3,7	0,0
Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	3,2	3,2	0,0
Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	2,9	3,0	-0,1
Devem existir programas para a conscientização, educação e formação em segurança	3,3	3,1	0,2
Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	3,1	3,2	-0,1
Devem existir auditorias de Segurança da Informação	3,3	3,0	0,3
Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	2,9	3,0	-0,1
Deve existir uma Política de Segurança da Informação	3,3	3,3	0,0
Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,1	3,1	0,0

Tabela 5.32- Factores de Boas Práticas: valores Nível Médio de Importância (Gestor Intermédio)

O gráfico (Gráfico 5.101) radar abaixo ilustra as diferenças acima encontradas.

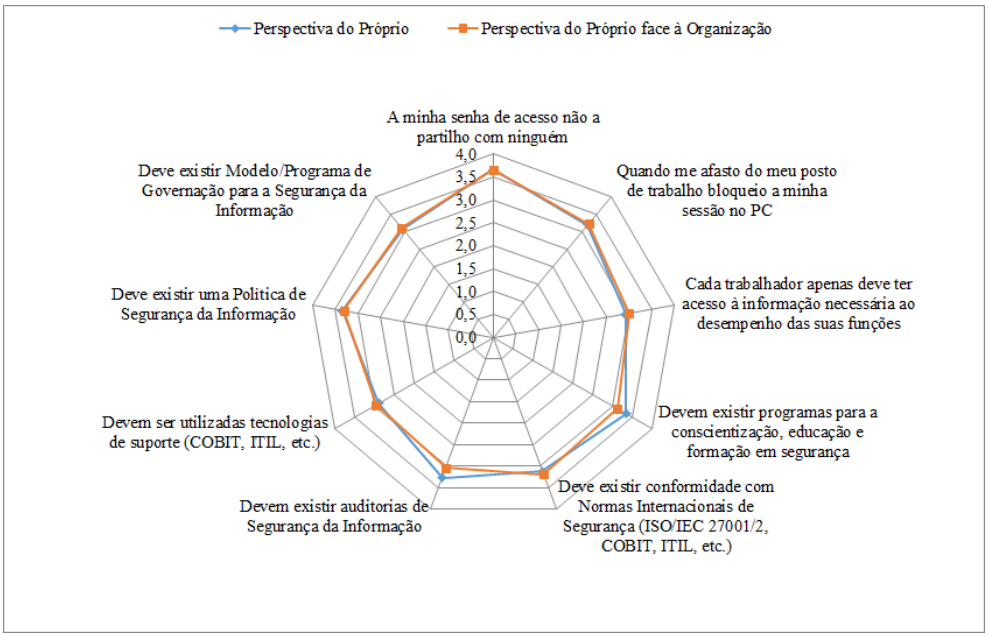


Gráfico 5.101- Factores de Boas Práticas: Comparação entre PP e PPO (Gestor Intermédio)

Do ponto de vista do Gestor das TI - a tabela (Tabela 5.33) seguinte, revela que as opiniões dos gestores das TI, que representam (14,05%) dos respondentes, apresentam desvios na

classificação do nível médio de importância em quatro, dos nove elementos considerados de boas práticas, quando comparada a perspectiva do próprio relativamente à perspectiva do próprio face à organização.

Pode pois verificar-se, que o nível médio de importância, na perspectiva do próprio, é maior no elemento considerado de boas práticas "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*", quando comparado com o nível médio de importância na perspectiva do próprio face à organização mostrando um desvio igual (0,1).

Para os restantes três elementos, acontece o contrário: o nível médio de importância na perspectiva do próprio é menor, quando comparado com o valor do nível médio de importância na perspectiva do próprio face à organização, apresentando valor absoluto de desvio igual (0,1), nos elementos: "*Devem existir programas para a conscientização, educação e formação em segurança*", "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*".

Factores de Boas Práticas	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
A minha senha de acesso não a partilho com ninguém	3,8	3,8	0,0
Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	3,6	3,5	0,1
Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	3,2	3,2	0,0
Devem existir programas para a conscientização, educação e formação em segurança	3,1	3,2	-0,1
Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	3,1	3,1	0,0
Devem existir auditorias de Segurança da Informação	3,3	3,3	0,0
Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	3,1	3,2	-0,1
Deve existir uma Política de Segurança da Informação	3,5	3,5	0,0
Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,1	3,2	-0,1

Tabela 5.33- Factores de Boas Práticas: valores Nível Médio de Importância (Gestor das TI)

O gráfico (Gráfico 5.102) radar abaixo reflecte as diferenças acima destacadas.

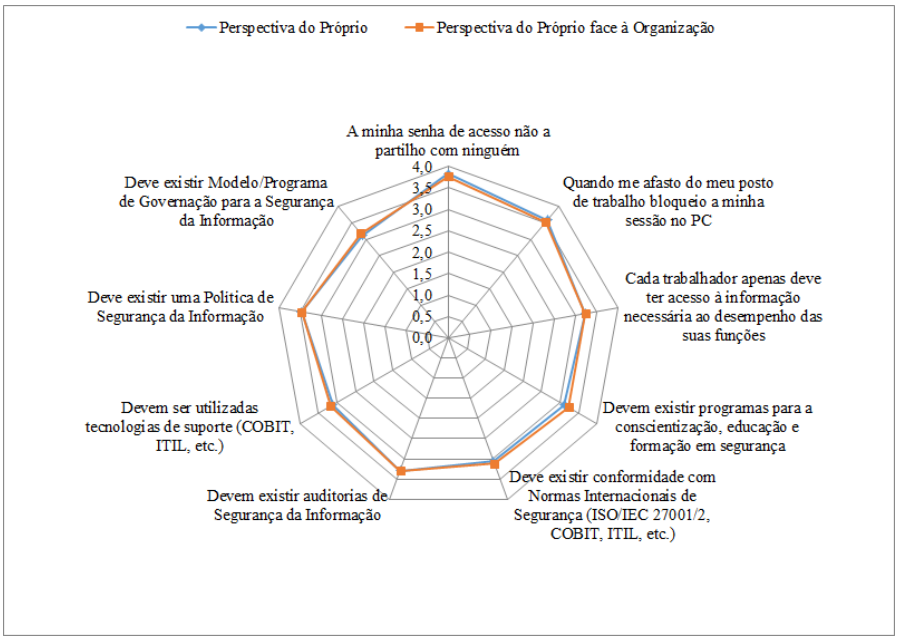


Gráfico 5.102- Factores de Boas Práticas: Comparação entre PP e PPO (Gestor das TI)

Do ponto de vista do Consultor das TI - a tabela (Tabela 5.34) a seguir, mostra que as opiniões dos consultores das TI, que representam (11,57%) dos respondentes, revelam desvios na classificação do nível médio de importância em oito dos nove elementos considerados de boas práticas, quando analisada a perspectiva do próprio relativamente à perspectiva do próprio face à organização. Apenas o elemento "*Devem existir auditorias de Segurança da Informação*" mantém a pontuação nas duas perspectivas.

O elemento considerado de boas práticas "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" surge com um valor do nível médio de importância menor na perspectiva do próprio, quando comparado com o valor do nível médio de importância na perspectiva do próprio face à organização, revelando um valor absoluto de desvio igual a (0,1).

Para os restantes elementos acontece o contrário, ou seja, o valor do nível médio de importância na perspectiva do próprio é maior quando comparado com o valor do nível médio de importância na perspectiva do próprio face à organização. Neste caso, os valores dos desvios variam entre (0,1) e (0,3), ocorrendo, respectivamente, nos seguintes elementos:

- "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" – cada um, com valor desvio igual (0,1);
- "*A minha senha de acesso não a partilho com ninguém*", "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*", "*Devem existir programas para a*

conscientização, educação e formação em segurança" e "*Deve existir uma Política de Segurança da Informação*" - cada um, com valor desvio igual (0,2);

- "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)*" - cada um, com valor desvio igual (0,3).

Factores de Boas Práticas	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
A minha senha de acesso não a partilho com ninguém	3,9	3,7	0,2
Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	3,7	3,5	0,2
Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	3,2	3,1	0,1
Devem existir programas para a conscientização, educação e formação em segurança	2,9	2,7	0,2
Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	3,0	2,7	0,3
Devem existir auditorias de Segurança da Informação	3,2	3,2	0,0
Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	2,7	2,8	-0,1
Deve existir uma Política de Segurança da Informação	3,4	3,2	0,2
Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,0	2,9	0,1

Tabela 5.34- Factores de Boas Práticas: valores Nível Médio de Importância (Consultor das TI)

O gráfico (Gráfico 5.103) radar abaixo mostra as diferenças acima descritas.

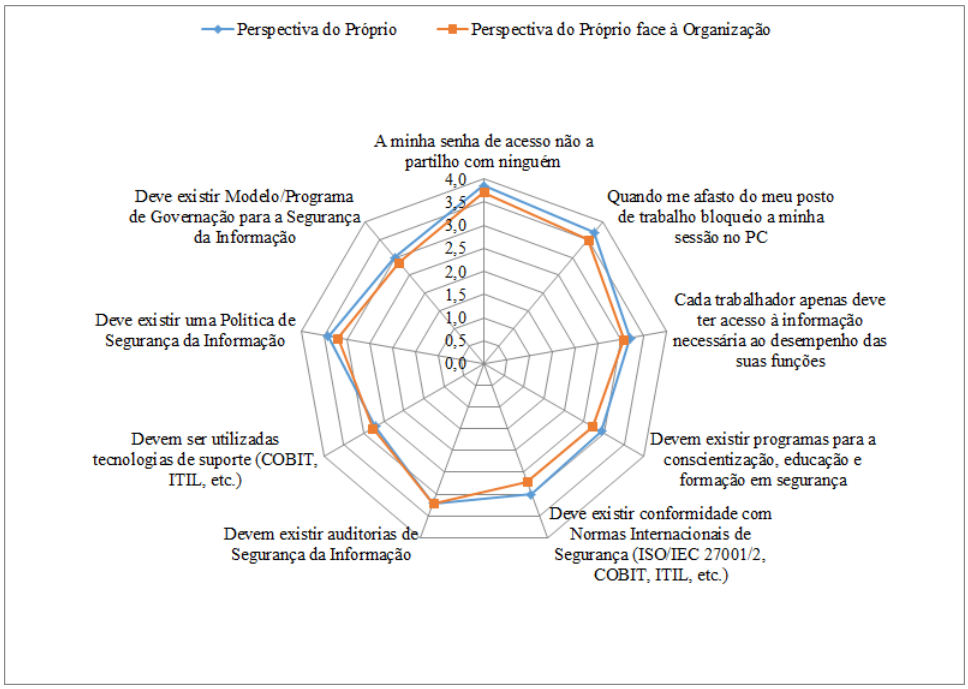


Gráfico 5.103- Factores de Boas Práticas: Comparação entre PP e PPO (Consultor das TI)

Do ponto de vista do Gestor/Funcionário de Segurança – esta classe apresenta uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). No entanto, ainda assim, é de referir os desvios na classificação do nível médio de importância em sete dos nove elementos

considerados de boas práticas, quando analisada a perspectiva do próprio em relação à perspectiva do próprio face à organização.

Deste modo, podemos verificar que o nível médio de importância na perspectiva do próprio para o elemento "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" é maior quando comparado com o valor do nível médio de importância na perspectiva do próprio face à organização, apresentando um desvio de (0,3).

Contudo, para os outros seis elementos acontece o contrário: o nível médio de importância na perspectiva do próprio é inferior quando comparado com o nível médio de importância na perspectiva do próprio face à organização atingindo os desvios valores entre (0,3) e (0,6).

Na tabela (Tabela 5.35) seguinte pode-se visualizar o já referido.

Factores de Boas Práticas	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
A minha senha de acesso não a partilho com ninguém	3,7	4,0	-0,3
Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	3,3	3,3	0,0
Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	3,3	3,0	0,3
Devem existir programas para a conscientização, educação e formação em segurança	3,3	3,3	0,0
Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	2,7	3,0	-0,3
Devem existir auditorias de Segurança da Informação	3,3	3,7	-0,4
Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	3,0	3,3	-0,3
Deve existir uma Política de Segurança da Informação	2,7	3,3	-0,6
Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,0	3,3	-0,3

Tabela 5.35- Factores de Boas Práticas: valores Nível Médio de Importância (Gestor/Funcionário da Segurança)

O gráfico (Gráfico 5.104) radar abaixo expõe as diferenças acima expostas.

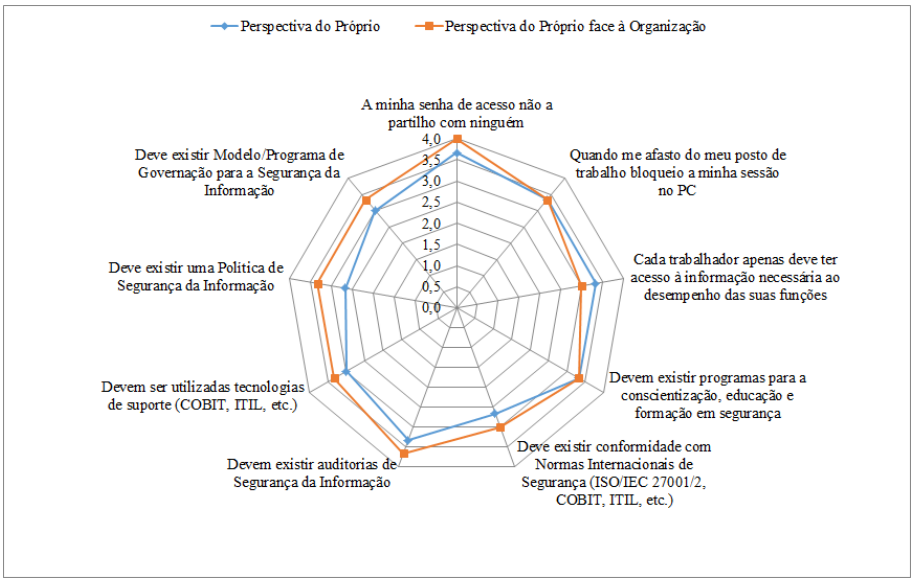


Gráfico 5.104- Factores de Boas Práticas: Comparação entre PP e PPO (Gestor/Funcionário da Segurança)

Do ponto de vista do Trabalhador - a tabela (Tabela 5.36) seguinte, mostra que as opiniões dos trabalhadores, que representam (42,15%) dos respondentes, apresentam desvios na classificação do nível médio de importância em cinco dos nove elementos considerados de boas práticas, quando analisada a perspectiva do próprio relativamente à perspectiva do próprio face à organização.

Assim, constata-se que o nível médio de importância - na perspectiva do próprio, é maior em cinco dos nove elementos considerados de boas práticas, quando comparado com o nível médio de importância – na perspectiva do próprio face à organização, apresentando valores idênticos de desvios (0,1) para quatro dos elementos, a saber: "*A minha senha de acesso não a partilho com ninguém*", "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*", "*Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.*)" e "*Deve existir uma Política de Segurança da Informação*". Para o elemento "*Devem existir programas para a conscientização, educação e formação em segurança*" o desvio apresenta um valor superior (0,2).

De referir, ainda, que, neste caso, quando existe desvio, na análise comparativa entre as duas perspectivas dos respondentes, os níveis médios de importância atribuídos, por estes, quando assinalam a perspectiva do próprio, são sempre maiores, do que quando indicam os níveis médios de importância, na perspectiva do próprio face à organização.

Factores de Boas Práticas	Perspectiva do Próprio	Perspectiva do Próprio face à Organização	Desvio
A minha senha de acesso não a partilho com ninguém	3,6	3,5	0,1
Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	3,3	3,2	0,1
Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	2,9	2,9	0,0
Devem existir programas para a conscientização, educação e formação em segurança	3,3	3,1	0,2
Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	3,2	3,1	0,1
Devem existir auditorias de Segurança da Informação	3,1	3,1	0,0
Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	3,0	3,0	0,0
Deve existir uma Política de Segurança da Informação	3,4	3,3	0,1
Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,2	3,2	0,0

Tabela 5.36- Factores de Boas Práticas: valores Nível Médio de Importância (Trabalhador)

O gráfico (Gráfico 5.105) radar seguinte mostra as diferenças acima mencionadas.

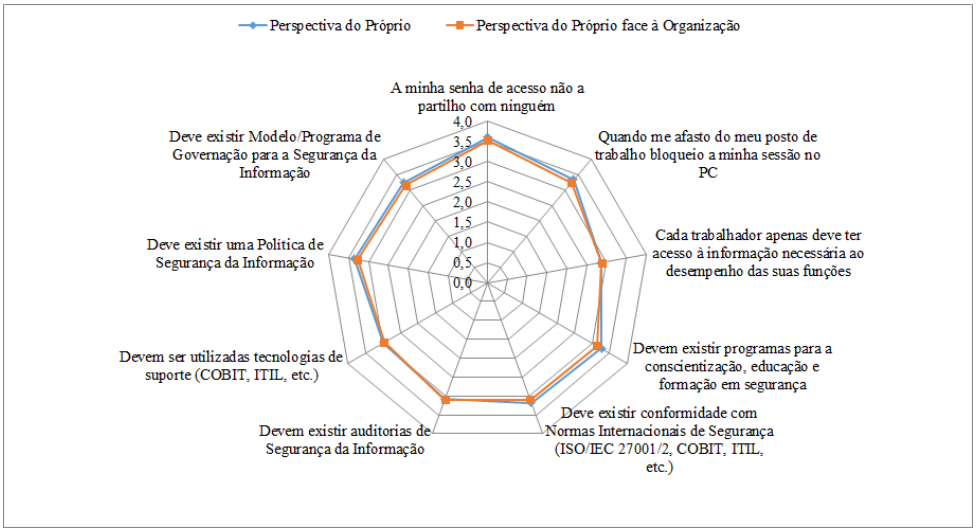


Gráfico 5.105- Factores de Boas Práticas: Comparação entre PP e PPO (Trabalhador)

5.3.7 – Análise resultante do mapeamento dos elementos do factor segundo a orientação do ISACA

Reavendo o referencial abaixo ilustrado (Figura 5.21), neste ponto apresentam-se os resultados alcançados por meio da análise efectuada ao cruzamento dos dados obtidos e o mapeamento dos elementos de boas práticas tendo em conta a orientação do ISACA [125] que refere: «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*» e conforme se mostra no ponto 4.2 deste documento.

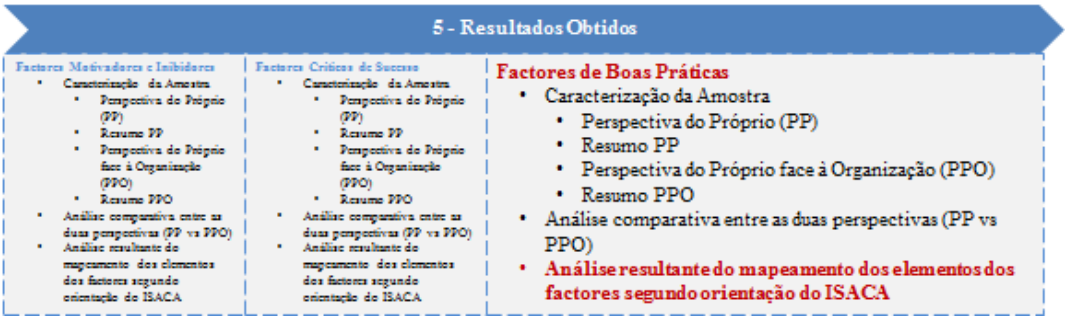


Figura 5.21- Modelo dos Resultados Obtidos: FBP/Análise Mapeamento ISACA

Deste modo, o estudo revela que, globalmente, os elementos considerados de boas práticas na adopção/implementação dum Sistema de Gestão da Segurança da Informação nas organizações centram-se no pilar de resultados: "*Gestão de Risco*" e apresentam pontuações de nível médio de importância, na ordem dos (3,3 – 3,5). A tabela/gráfico (Gráfico 5.106) seguinte mostra o acima referido.

Factores de Boas Práticas (Nível médio de importância - Global)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) A minha senha de acesso não a partilho com ninguém			3,7	3,6						
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC			3,4	3,5						
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções			3	3,5						
d) Devem existir programas para a conscientização, educação e formação em segurança			3,2	3,4						
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)							3,1	3,3		
f) Devem existir auditorias de Segurança da Informação									3,2	3,2
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)					3	3,2				
h) Deve existir uma Política de Segurança da Informação	3,4	3								
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,2	3,3								
Total (Valor médio)	3,3	3,15	3,33	3,5	3	3,2	3,1	3,3	3,2	3,2

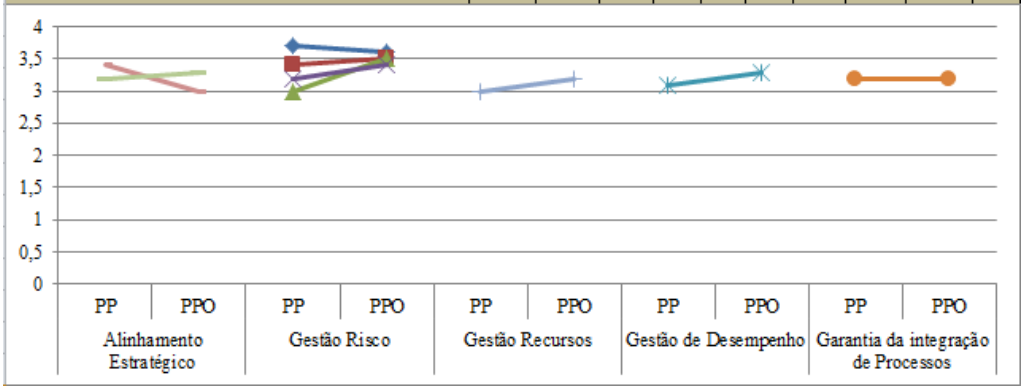


Gráfico 5.106- Factores de Boas Práticas: Mapeamento ISACA (Global)

Contudo, se se analisar os resultados tendo em conta a função do respondente, verifica-se que o enfoque do "pilar de resultados" muda com o grupo profissional.

De facto, o Gestor de Topo centra a sua percepção no pilar de resultados – "*Alinhamento Estratégico*" com valores de níveis médios de importância significativos (3,7 – 3,45). De realçar que esta diferença na pontuação traduz o desvio, respectivamente, entre a perspectiva do próprio (3,7) e a perspectiva do próprio face à organização (3,45), verificando-se que, do ponto de vista da organização, o respondente – Gestor de Topo apenas lhe atribui um valor médio de importância de valor inferior (3,45). A tabela/gráfico (Gráfico 5.107) seguinte mostra o acima referido.

Factores de Boas Práticas (Nivel médio de importância - Gestor de Topo)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) A minha senha de acesso não a partilho com ninguém			3,5	3,4						
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC			3,2	3,3						
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções			3,4	3,3						
d) Devem existir programas para a conscientização, educação e formação em segurança			3,4	3,2						
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)							3,3	3,2		
f) Devem existir auditorias de Segurança da Informação									3,6	3,4
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)					3,1	2,9				
h) Deve existir uma Politica de Segurança da Informação	3,6	3,5								
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,8	3,4								
Total (Valor médio)	3,7	3,45	3,38	3,3	3,1	2,9	3,3	3,2	3,6	3,4

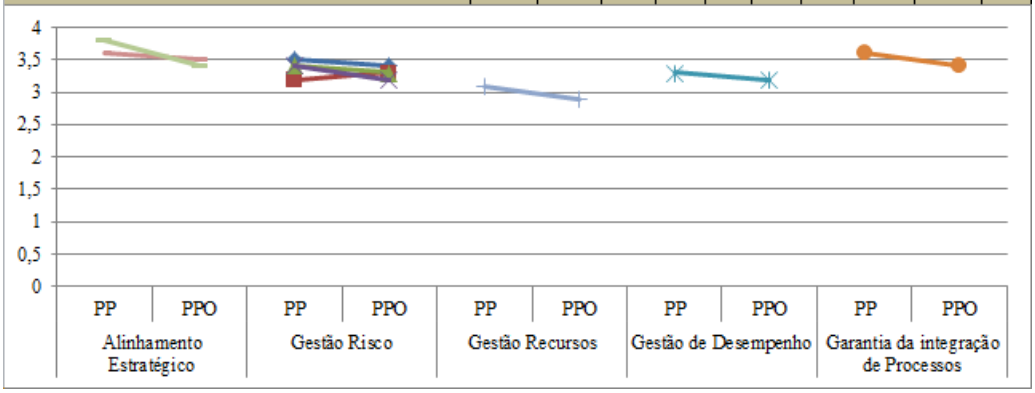


Gráfico 5.107- Factores de Boas Práticas: Mapeamento ISACA (Gestor de Topo)

Já o Gestor Intermédio segue a tendência global, centrando a sua preferência no pilar de resultados – "*Gestão de Risco*", apresentando valores de níveis médios de importância aproximados, quer na perspectiva do próprio (3,3), quer na perspectiva do próprio face à organização (3,25). A tabela/gráfico (Gráfico 5.108) seguinte mostra o acima referido.

Factores de Boas Práticas (Nível médio de importância - Gestor Intermédio)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) A minha senha de acesso não a partilho com ninguém			3,7	3,7						
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC			3,2	3,2						
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções			2,9	3						
d) Devem existir programas para a conscientização, educação e formação em segurança			3,3	3,1						
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)							3,1	3,2		
f) Devem existir auditorias de Segurança da Informação									3,3	3
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)					2,9	3				
h) Deve existir uma Politica de Segurança da Informação	3,3	3,3								
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,1	3,1								
Total (Valor médio)	3,2	3,2	3,28	3,25	2,9	3	3,1	3,2	3,3	3

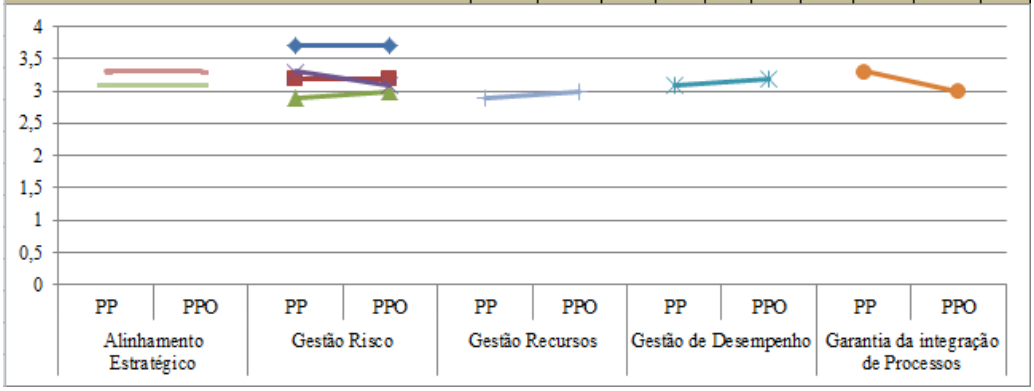


Gráfico 5.108- Factores de Boas Práticas: Mapeamento ISACA (Gestor Intermédio)

Também o Gestor das TI segue a tendência global, centrando a sua preferência no pilar de resultados – "*Gestão de Risco*", apresentando valores de níveis médios de importância, ligeiramente superiores aos do Gestor Intermédio - na perspectiva do próprio (3,4) e na perspectiva do próprio face à organização (3,43). Assim, de realçar que, neste grupo profissional e para este "pilar de resultados" a valorização na perspectiva do próprio é inferior, quando comparada com a valorização atribuída na perspectiva do próprio face à organização, significando que a percepção do respondente - Gestor das TI, adquire maior importância na perspectiva do próprio face à organização. A tabela/gráfico (Gráfico 5.109) seguinte mostra o acima referido.

Factores de Boas Práticas (Nivel médio de importância - Gestor das TI)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) A minha senha de acesso não a partilho com ninguém			3,8	3,8						
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC			3,6	3,5						
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções			3,2	3,2						
d) Devem existir programas para a conscientização, educação e formação em segurança			3,1	3,2						
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)							3,1	3,1		
f) Devem existir auditorias de Segurança da Informação									3,3	3,3
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)					3,1	3,2				
h) Deve existir uma Política de Segurança da Informação	3,5	3,5								
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,1	3,2								
Total (Valor médio)	3,3	3,35	3,43	3,43	3,1	3,2	3,1	3,1	3,3	3,3

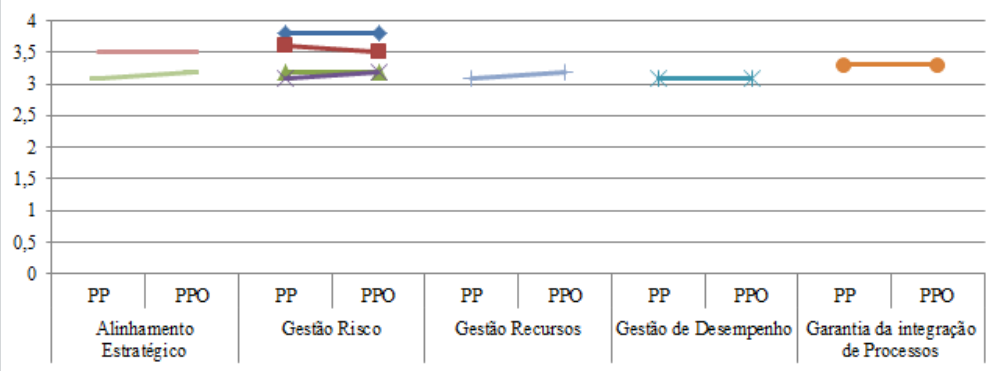


Gráfico 5.109- Factores de Boas Práticas: Mapeamento ISACA (Gestor das TI)

Todavia, o Consultor das TI segue a tendência global, centrando a sua preferência no pilar de resultados – "*Gestão de Risco*", apresentando valores de níveis médios de importância superiores, na perspectiva do próprio (3,4), comparado com os resultados na perspectiva do próprio face à organização (3,25). A tabela/gráfico (Gráfico 5.110) seguinte mostra o acima referido.

Factores de Boas Práticas (Nivel médio de importância - Consultor das TI)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) A minha senha de acesso não a partilho com ninguém			3,9	3,7						
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC			3,7	3,5						
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções			3,2	3,1						
d) Devem existir programas para a conscientização, educação e formação em segurança			2,9	2,7						
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)							3	2,7		
f) Devem existir auditorias de Segurança da Informação									3,2	3,2
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)					2,7	2,8				
h) Deve existir uma Politica de Segurança da Informação	3,4	3,2								
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	3	2,9								
Total (Valor médio)	3,2	3,05	3,4	3,25	2,7	2,8	3	2,7	3,2	3,2

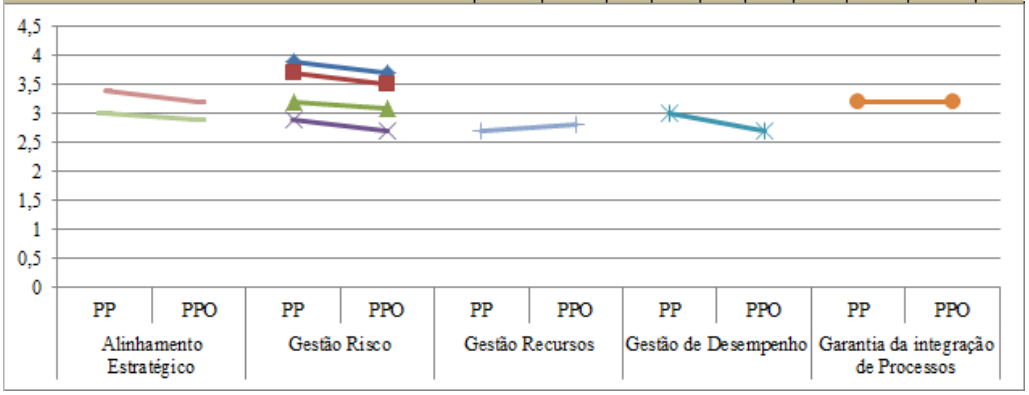


Gráfico 5.110- Factores de Boas Práticas: Mapeamento ISACA (Consultor das TI)

Porém, para o Gestor/Funcionário da Segurança" a percepção de preferência incide sobre dois pilares de resultados distintos, consoante se analisa a perspectiva do próprio – pilar de resultados – "*Gestão de Risco*" ou se examina a perspectiva do próprio face à organização – pilar de resultados – "*Garantia de integração de Processos*", apresentando, respectivamente, valores médios de importância de (3,4) e (3,7). A tabela/gráfico (Gráfico 5.111) seguinte mostra o acima referido.

Factores de Boas Práticas (Nivel médio de importância - Gestor/Funcionário da Segurança)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) A minha senha de acesso não a partilho com ninguém			3,7	4						
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC			3,3	3,3						
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções			3,3	3						
d) Devem existir programas para a conscientização, educação e formação em segurança			3,3	3,3						
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)							2,7	3		
f) Devem existir auditorias de Segurança da Informação									3,3	3,7
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)					3	3,3				
h) Deve existir uma Política de Segurança da Informação	2,7	3,3								
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	3	3,3								
Total (Valor médio)	2,85	3,3	3,4	3,4	3	3,3	2,7	3	3,3	3,7

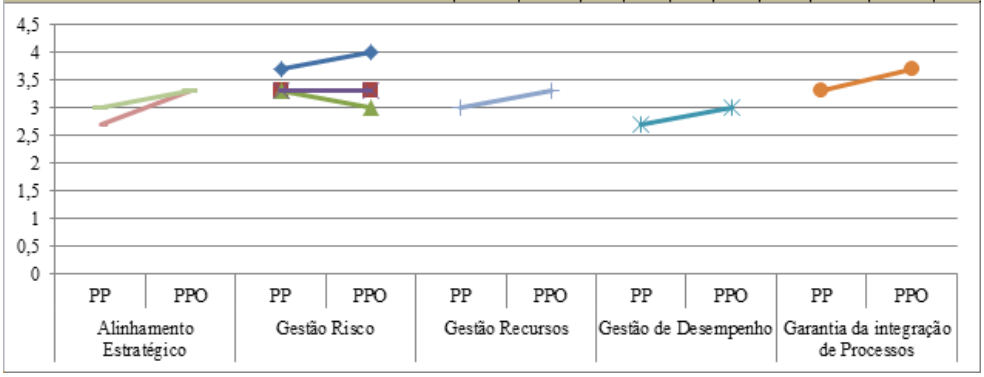


Gráfico 5.111- Factores de Boas Práticas: Mapeamento ISACA (Gestor/Funcionário da Segurança)

Já o Trabalhador segue a linha de percepção do Gestor de Topo, centra a sua percepção no pilar de resultados – "*Alinhamento Estratégico*", embora com valores de níveis médios de importância ligeiramente inferiores (3,3 – 3,25). De realçar que esta diferença na pontuação traduz o desvio, respectivamente, entre a perspectiva do próprio (3,3) e a perspectiva do próprio face à organização (3,25). A tabela/gráfico (Gráfico 5.112) seguinte mostra o acima referido.

Factores de Boas Práticas (Nível médio de importância - Trabalhador)	Alinhamento Estratégico		Gestão Risco		Gestão Recursos		Gestão de Desempenho		Garantia da integração de Processos	
	PP	PPO	PP	PPO	PP	PPO	PP	PPO	PP	PPO
a) A minha senha de acesso não a partilho com ninguém			3,6	3,5						
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC			3,3	3,2						
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções			2,9	2,9						
d) Devem existir programas para a conscientização, educação e formação em segurança			3,3	3,1						
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)							3,2	3,1		
f) Devem existir auditorias de Segurança da Informação									3,1	3,1
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)					3	3				
h) Deve existir uma Política de Segurança da Informação	3,4	3,3								
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,2	3,2								
Total (Valor médio)	3,3	3,25	3,28	3,18	3	3	3,2	3,1	3,1	3,1

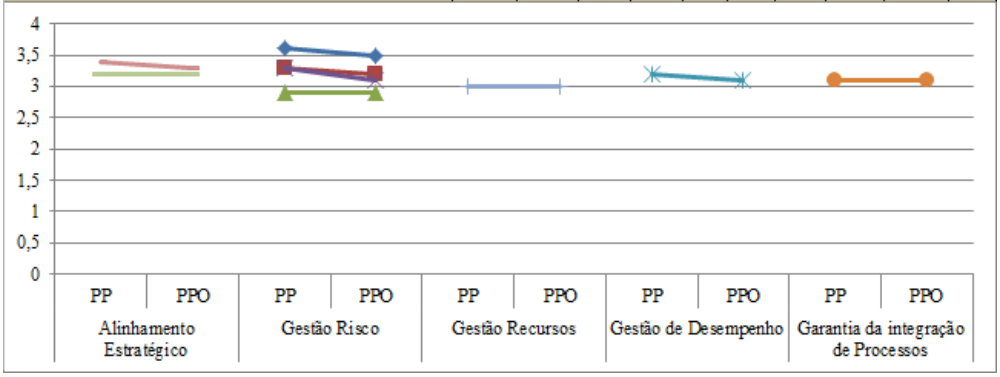


Gráfico 5.112- Factores de Boas Práticas: Mapeamento ISACA (Trabalhador)

6. CONCLUSÕES

O presente trabalho enquadra-se no sector das Águas/Saneamento em Portugal e tem como principais objectivos: a investigação de quais os Factores Motivadores (FM), Inibidores (FI), Críticos de Sucesso (FCS) e de Boas Práticas (FBP) que dão suporte à adopção/implementação de um Sistema de Gestão de Segurança da Informação (SGSI) nas organizações do sector, tendo em conta a perspectiva do próprio (PP) e a perspectiva do próprio face à organização (PPO), a comparação das duas perspectivas através do cálculo do nível médio de importância (NMI) para cada elemento dos factores acima referidos e a análise dos efeitos obtidos através do cruzamento do nível médio de importância dos elementos dos diferentes factores (FM, FI, FCS, FBP) com o mapeamento segundo a orientação do ISACA [126] que refere: «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*».

Deste modo, partiu-se para a revisão bibliográfica baseada em sete palavras-chave: Informação, Segurança da Informação, Governação Corporativa, Governação das TI, Governação da Segurança da Informação, Cultura Organizacional, Cultura de Segurança da Informação. Estendeu-se a pesquisa a temas fortemente relacionados, como a gestão de risco e controlo, bem como se evidencia a necessidade da aplicabilidade dos principais referenciais – modelos (BMIS), *frameworks* (COBIT), *standards* e normas (ISO/IEC série 27000 e NIST SP série 800) chegando-se ao modelo do racional teórico desenvolvido (Figura 4.1) como base de suporte à exposição do presente trabalho.

Assim, constata-se que actualmente, a aceitação da "Informação" como um recurso vital e estratégico para as organizações está na ordem do dia. Na literatura científica, segundo a ISO27000 [127] a protecção da "Informação" requer a «*preservação da confidencialidade, integridade e a disponibilidade da informação, podendo incluir outras propriedades como a autenticidade, a responsabilidade, o não-repúdio e a confiança*». Contudo, deve ter-se como ponto de partida a ideia básica de que não existe nenhum sistema totalmente seguro, pelo que se impõe a necessidade de gerir a segurança do recurso informação. Desta forma, Oliveira, Wilson [128] defende que «*a segurança da informação deve ser tratada como uma actividade contínua, pois existirão sempre novas técnicas de ataques da informação e consequentemente teremos de estar sempre atentos e prontos para o contra-ataque. A melhor arma para nossa defesa é estarmos sempre actualizados e nunca descurarmos a segurança …*».

De facto, a evolução tecnológica transpôs a "informação" do mundo do papel para o mundo electrónico e consequentemente os "sistemas de informação" tornam-se cada vez mais complexos, onde os riscos de violação adquirem maior dimensão e diversidade. Porém, Oliveira, Wilson [129] defende que «*A segurança da informação não é uma questão técnica, mas uma questão estratégica e humana*», verificando-se que - "o factor humano" é considerado, pela comunidade científica em geral, como o elo mais fraco da cadeia de segurança da informação.

Por outro lado, mostra-se também que a segurança é considerada, pelo Conselho da União Europeia [130] «*… em si mesma, um direito básico.… A segurança converteu-se portanto num factor-chave para garantir uma elevada qualidade de vida na sociedade europeia e para proteger as nossas infra-estruturas críticas através da prevenção e da luta contra as ameaças comuns*». Também no sector das Águas e Saneamento verifica-se que a 28 de Julho de 2010, a Assembleia Geral das Nações Unidas [131] declara, na sua Resolução n.º 64/292 «*A água e o saneamento como direitos humanos*», pelo que segundo Grey, David et al. [132] «*A escala do desafio sempre presente da sociedade de alcançar a sustentabilidade da segurança da água é determinada por muitos factores, entre os quais se destacam … o ambiente sócio-económico – a estrutura da economia e o comportamento dos seus actores – que reflectem legados naturais e culturais e escolhas políticas …*».

Logo, tendo como premissa a importância da segurança da informação nas organizações e como público-alvo os funcionários das organizações do sector das Águas e Saneamento em Portugal (incluindo a gestão de topo, gestão intermédia, gestão das TI, consultores das TI, gestor/funcionário da segurança e trabalhador), no presente estudo aprecia-se, através da elaboração e divulgação de questionário *on-line*, a "cultura individual" dos profissionais na cultura de segurança da informação nas organizações daquele sector, ou seja, que Factores Motivadores, Inibidores, Críticos de Sucesso e/ou de Boas Práticas estão presentes na adopção/implementação de Sistema de Gestão da Segurança da Informação, tendo em conta a perspectiva do próprio e a perspectiva do próprio face à organização.

A figura (Figura 6.1) seguinte esquematiza o raciocínio seguido na apresentação das principais conclusões.

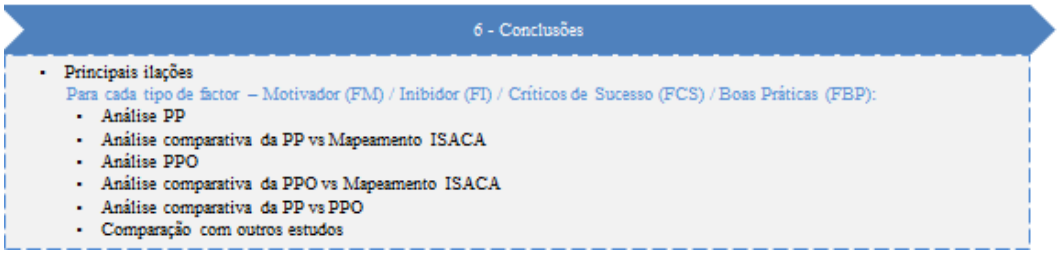


Figura 6.1- Modelo das Conclusões

6.1 - Factores Motivadores e Inibidores

Nesta parte apresenta-se uma resenha das principais observações referentes aos Factores Motivadores e Inibidores, decorrentes do estudo. Assim, de acordo com o modelo abaixo indicado (Figura 6.2) revelam-se as conclusões relativas aos elementos dos Factores Motivadores e Inibidores considerados para a pesquisa, tendo em conta as diferentes perspectivas, do próprio e do próprio face à organização, bem como as respectivas análises comparativas: entre as perspectivas, entre as perspectivas e o mapeamento com as orientações ISACA [133] (conforme ponto 4.2) e, ainda, com outros estudos encontrados na literatura científica.

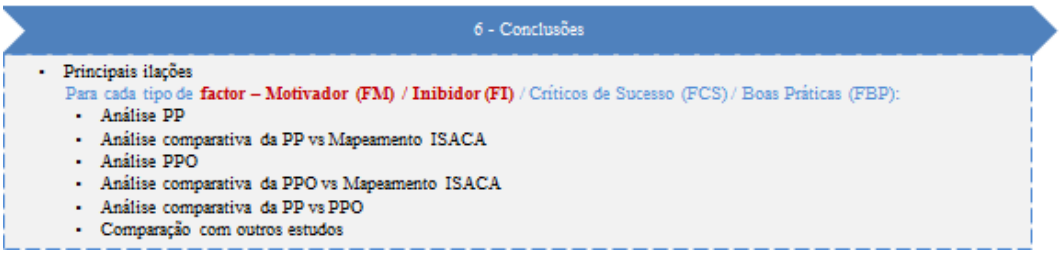


Figura 6.2- Modelo das Conclusões / Factores Motivadores e Inibidores

6.1.1- Perspectiva do Próprio

Face ao acima exposto, e seguindo o referencial explicativo da apresentação de resultados (Figura 6.3), neste ponto resume-se, primeiramente, os resultados observados para os elementos dos Factores Motivadores considerados na perspectiva do próprio.

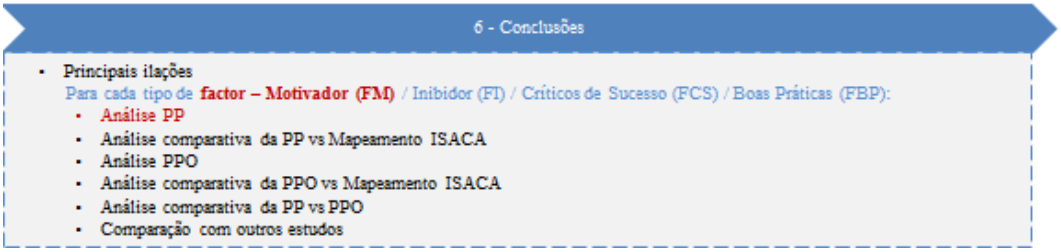


Figura 6.3- Modelo das Conclusões / Factores Motivadores - PP

Assim, os Factores Motivadores que, globalmente apresentam maior nível médio de importância na implementação/adopção dum Sistema de Gestão da Segurança da Informação são: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (3,8), seguido dos elementos "*Evitar perdas financeiras*" e "*Planear a segurança da informação antes da implementação de novas tecnologias*" com a mesma pontuação (3,6). O elemento "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" aparece na terceira posição em igualdade de pontuação com o elemento "*Emergência contínua de novos riscos*" (3,4).

Contudo, nesta perspectiva, o Gestor de Topo considera como mais motivador o elemento "*Evitar perdas financeiras*" (3,9). Os elementos "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (3,8) e "*Planear a segurança da informação antes da implementação de novas tecnologias*" (3,6), mostram-se, respectivamente, na segunda e terceira posição. Porém, o elemento "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" revela-se na quarta posição em igualdade de pontuação com o elemento "*Emergência contínua de novos riscos*" (3,4).

Já para o Gestor Intermédio o estudo revela que os três elementos mais indicados como Factores Motivadores são: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (3,8), "*Evitar perdas financeiras*" (3,7) e "*Emergência contínua de novos riscos*" (3,6), passando o elemento "*Planear a segurança da informação antes da implementação de novas tecnologias*" para o quarto lugar (3,5). O elemento "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" revela-se na última posição em igualdade de pontuação (3,2) com mais outros três elementos.

Todavia, para o Gestor das TI, mostra-se o elemento: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (3,9). Porém, os elementos "*Planear a segurança da informação antes da implementação de novas tecnologias*" e "*Evitar perdas financeiras*" atingem o mesmo nível médio de importância (3,6). Em terceiro lugar surge o elemento "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" (3,5).

Na opinião do Consultor das TI surgem os elementos "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (3,7) e "*Evitar perdas finance*iras" (3,5). O terceiro elemento mais votado é "*Planear a segurança da informação antes da implementação de novas tecnologias*" (3,4). Em quarto lugar revela-se o elemento "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" (3,3) com valor idêntico de nível médio de importância ao elemento "*Emergência contínua de novos riscos*".

Para o Gestor/Funcionário da Segurança obteve-se uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). No entanto, o elemento "*Garantir a disponibilidade, confidencialidade e integridade da informação*" obtém o nível médio de importância de valor (4,0). O elemento "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" surge na segunda posição mas, com outros três elementos de valor idêntico para o nível médio de importância (3,7).

Por último, do ponto de vista do Trabalhador os três primeiros elementos com maiores níveis médios de importância atribuídos pelos respondentes são: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (3,8), "*Planear a segurança da informação antes da implementação de novas tecnologias*" (3,6) e "*Evitar perdas financeiras*" (3,5). O elemento "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" surge na quarta posição mas, com outros dois elementos de valor idêntico para o nível médio de importância (3,4).

O gráfico abaixo (Gráfico 6.1) ilustra o acima mencionado.

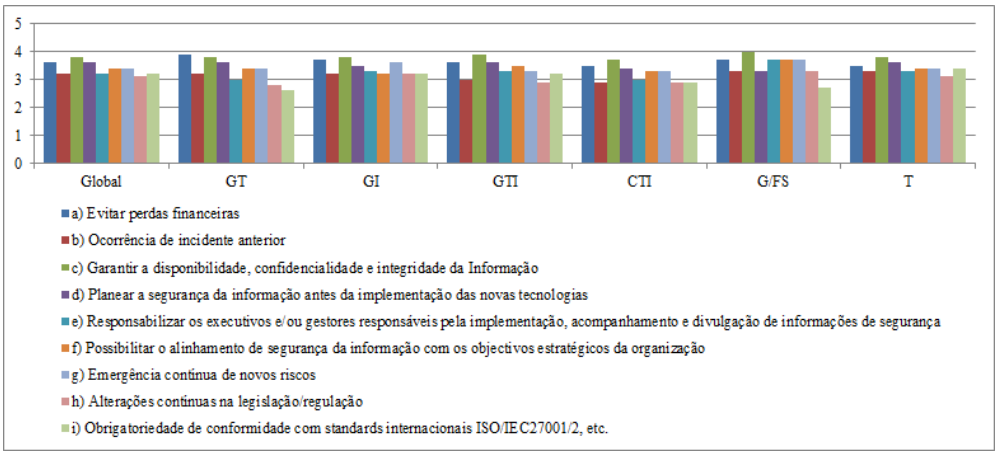


Gráfico 6.1- FM/PP: Comparação pelo Tipo Função e Nível Médio de Importância

Resumindo e conforme tabela seguinte (Tabela 6.1) o elemento motivador "*Garantir a disponibilidade, confidencialidade e integridade da Informação*" é o que apresenta maior nível médio de importância. De facto, só o Gestor de Topo é que o coloca em segundo lugar dando preferência ao elemento motivador "*Evitar perdas financeiras*". Porém, o elemento motivador "*Planear a segurança da informação antes da implementação de novas tecnologias*" é classificado em segundo lugar pelos "Gestor das TI" e "Trabalhador"; em terceiro pelos "Gestor de Topo", "Consultor das TI" e "Gestor/Funcionário da Segurança" e em quarto lugar pelo "Gestor intermédio". Por outro lado, o elemento motivador "*Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização*" é classificado em segundo lugar pelo Gestor/Funcionário da Segurança, mas é relegado para a terceira posição

pelo Gestor das TI e para a quarta posição pelos Gestores de Topo, Consultores das TI e Trabalhadores. O Gestor Intermédio atribui-lhe a sexta posição e globalmente o mesmo elemento surge na terceira posição.

Factores Motivadores (Nível médio de importância - PP)	Global	GT	GI	GTI	CTI	G/FS	T
a) Evitar perdas financeiras	3,6	3,9	3,7	3,6	3,5	3,7	3,5
b) Ocorrência de incidente anterior	3,2	3,2	3,2	3,0	2,9	3,3	3,3
c) Garantir a disponibilidade, confidencialidade e integridade da Informação	3,8	3,8	3,8	3,9	3,7	4,0	3,8
d) Planear a segurança da informação antes da implementação das novas tecnologias	3,6	3,6	3,5	3,6	3,4	3,3	3,6
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	3,2	3,0	3,3	3,3	3,0	3,7	3,3
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	3,4	3,4	3,2	3,5	3,3	3,7	3,4
g) Emergência contínua de novos riscos	3,4	3,4	3,6	3,3	3,3	3,7	3,4
h) Alterações contínuas na legislação/regulação	3,1	2,8	3,2	2,9	2,9	3,3	3,1
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.	3,2	2,6	3,2	3,2	2,9	2,7	3,4
Legenda							
Posição	1ª	2ª	3ª	4ª	5ª	6ª	

Tabela 6.1- FM/PP: Posicionamento dos elementos por Tipo de Função

Por outro lado, para a mesma perspectiva – a do próprio, segue-se a referência do raciocínio conforme figura abaixo (Figura 6.4).

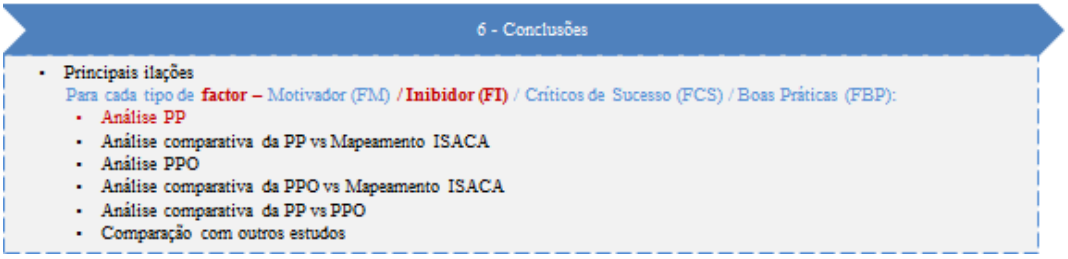


Figura 6.4- Modelo das Conclusões / Factores Inibidores - PP

Desta forma, os Factores Inibidores considerados que, globalmente apresentam maior nível médio de importância (3,3) na implementação/adopção dum Sistema de Gestão da Segurança da Informação (SGSI) são: "*Falta de conhecimento*", "*cultura organizacional*" e "*Dificuldade em medir o custo/benefício*". O elemento inibidor "*Acesso restrito à Gestão de Topo*" surge na última posição, com valor idêntico para o nível médio de importância (2,9), ao do elemento "*Emergência contínua de novos riscos*".

Contudo, nesta perspectiva, o Gestor de Topo e o Consultor das TI destacam o elemento "*Valor do investimento*", respectivamente (3,4) e (3,2), como o mais inibidor. Estes respondentes

também apresentam opinião semelhante para os elementos "*Falta de conhecimento*" e "*Dificuldade em medir o custo benefício*", os quais aparecem na segunda posição com a mesma pontuação para o nível médio de importância (3,3) para o Gestor de Topo e (3,1) para o Consultor das TI. Porém, os elementos inibidores "*Cultura organizacional*" e "*Acesso restrito à Gestão de Topo"* mostram-se, respectivamente, na quarta (2,9) e quinta (2,7) posição para o Gestor de Topo, enquanto, para o Consultor das TI, estes elementos surgem, respectivamente, na segunda posição (3,1) e terceira posição (2,5).

Já para o Gestor Intermédio o estudo revela que existem dois elementos mais indicados como Factores Inibidores: "*Falta de conhecimento*" e "*Dificuldade em medir o custo benefício*" mostrando um valor para o nível médio de importância igual (3,5). Todavia, os elementos "*Cultura organizacional*" e "*Acesso restrito à Gestão de Topo"* mostram-se, respectivamente, na segunda (3,4) e sexta (2,9) posição.

O Gestor das TI aponta o elemento: "*Cultura organizacional*" (3,4) como o mais inibidor, aparecendo o elemento "*Valor do investimento*" (3,2) na segunda posição seguido do elemento "*Falta de conhecimento*" (3,1). O elemento "*Acesso restrito à Gestão de Topo"* surge na quarta posição em igualdade com o elemento "*Dificuldade em medir o custo benefício*" mostrando o mesmo valor para o nível médio de importância (2,9).

Para o Gestor/Funcionário da Segurança obteve-se uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). No entanto, o elemento "*Dificuldade em medir o custo benefício*" obtém um nível médio de importância (3,7). O elemento "*Acesso restrito à Gestão de Topo*" surge na segunda posição em igualdade de pontuação com o elemento "*Emergência contínua de novos riscos*" (3,3). Os elementos inibidores "*Falta de conhecimento*" e "*Cultura organizacional*" mostram-se na terceira posição, com valor idêntico para o nível médio de importância (3,0).

Por último, o ponto de vista do Trabalhador apresenta uma opinião algo longe da do Gestor/Funcionário da Segurança ao classificar a "*Falta de conhecimento*" e a "*Cultura organizacional*" como os elementos inibidores de maior nível médio de importância (3,5). Para esta classe, o elemento "*Acesso restrito à Gestão de Topo*" declara-se na quarta posição com uma pontuação (3,0).

O gráfico a seguir (Gráfico 6.2) ilustra o acima mencionado.

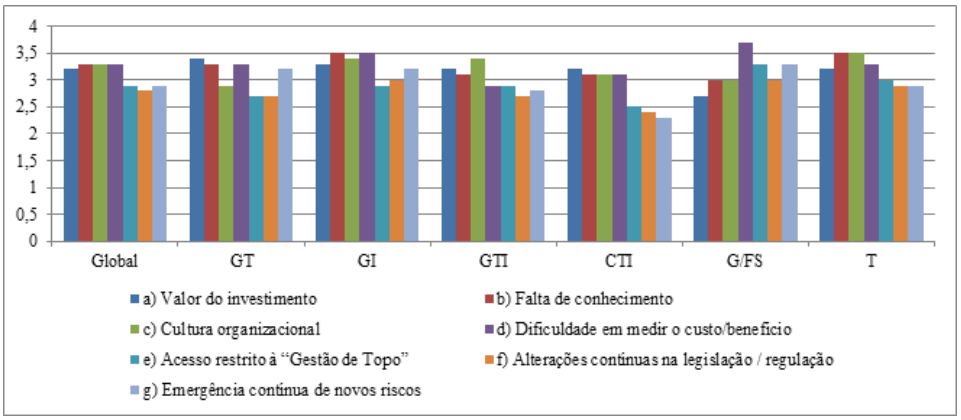


Gráfico 6.2- FI/PP: Comparação pelo Tipo de Função e Nível Médio de Importância

Resumindo e conforme tabela (Tabela 6.2) abaixo, na perspectiva do próprio, constata-se uma diversidade de opiniões na classificação do(s) elemento(s) mais, inibidor(es) na implementação/adopção dum Sistema de Gestão da Segurança da Informação.

Contudo, é de realçar que os elementos relacionados com o "Factor Humano" - "*Falta de conhecimento*" e "*Cultura organizacional*" encontram-se maioritariamente mencionados, pelos diferentes tipos de respondentes, nas três primeiras posições e, globalmente revelam-se na primeira posição com um valor para o nível médio de importância igual (3,3), o que indicia que, na perspectiva do próprio, os respondentes reconhecem a importância destes factores na implementação/adopção dum SGSI.

De notar também que o elemento "*Acesso restrito à Gestão de Topo*", com excepção do Gestor/Funcionário da Segurança (que o coloca na segunda posição), aparece classificado a partir da terceira posição, parecendo não se apresentar como um factor inibidor relevante, na perspectiva do próprio, para o sector em causa. De facto o Gestor das TI e o Trabalhador apontam-no para a quarta posição e o Gestor Intermédio para a sexta posição.

Factores Inibidores (Nivel médio de importância - PP)	Global	GT	GI	GTI	CTI	G/FS	T
a) Valor do investimento	3,2	3,4	3,3	3,2	3,2	2,7	3,2
b) Falta de conhecimento	3,3	3,3	3,5	3,1	3,1	3	3,5
c) Cultura organizacional	3,3	2,9	3,4	3,4	3,1	3	3,5
d) Dificuldade em medir o custo/beneficio	3,3	3,3	3,5	2,9	3,1	3,7	3,3
e) Acesso restrito à "Gestão de Topo"	2,9	2,7	2,9	2,9	2,5	3,3	3
f) Alterações contínuas na legislação / regulação	2,8	2,7	3	2,7	2,4	3	2,9
g) Emergência contínua de novos riscos	2,9	3,2	3,2	2,8	2,3	3,3	2,9
Legenda							
Posição	1ª	2ª	3ª	4ª	5ª	6ª	

Tabela 6.2- FI/PP: Posicionamento dos elementos por Tipo de Função

6.1.2 – Perspectiva do Próprio vs Mapeamento ISACA

Reavendo o quadro referencial seguido e conforme indicado na figura (Figura 6.5), neste ponto sintetizam-se as observações encontradas, através do cruzamento das perspectivas estudadas (próprio e do próprio face à organização) e o respectivo enquadramento representado no ponto 4.2 deste documento, referente às orientações propostas pelo ISACA [134] indicando que «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*».

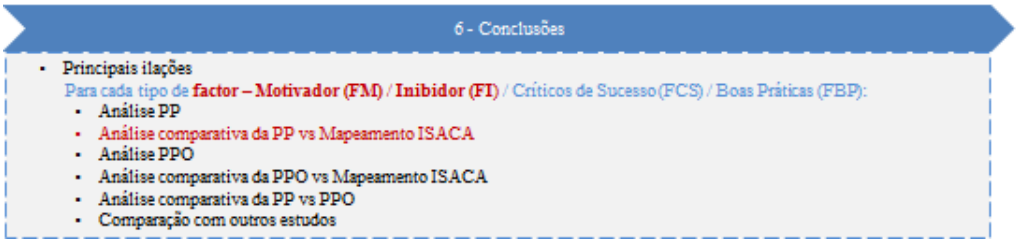


Figura 6.5- Modelo das Conclusões – FM/FI – PP vs Mapeamento ISACA

Assim, principiando-se pelos Factores Motivadores e face aos resultados dos valores médios de importância encontrados para os elementos considerados na caracterização dos Factores Motivadores verifica-se que, globalmente, os respondentes focam a sua preferência em elementos relacionados com o pilar de resultados – "*Gestão de Recursos*", indiciando que a motivação para a adopção/implementação do SGSI está centrada na "protecção de activos". De facto, o pilar de resultados – "*Alinhamento Estratégico*" aparece na terceira posição apresentando, globalmente, nível médio de importância (3,4), revelando-se na segunda posição para o Gestor/Funcionário da Segurança e em sexto lugar para os Gestores Intermédios. De notar que, para o Gestor de Topo, apesar de se manter o enfoque da motivação no pilar de resultados – "*Gestão de Recursos*", surge com maior nível médio de importância atribuído, o elemento motivador "*Evitar perdas financeiras*" pertencente ao pilar de resultados – "*Gestão de Risco*" e o pilar de resultados – "*Alinhamento Estratégico*" mostra-se na terceira posição. A tabela (Tabela 6.3) seguinte resume o acima mencionado.

Factores Motivadores (Nível médio de importância - PP)	Mapeamento ISACA	Global			GT			GI			GTI			CTI			G/FS			T		
		NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	Alinhamento Estratégico	3,4	3,40	3ª	3,4	3,40	3ª	3,2	3,20	5ª	3,5	3,50	3ª	3,3	3,30	3ª	3,7	3,70	2ª	3,4	3,40	3ª
a) Evitar perdas financeiras	Gestão Risco	3,6	3,33	4ª	3,9	3,33	4ª	3,7	3,43	3ª	3,6	3,20	5ª	3,5	3,15	4ª	3,7	3,50	3ª	3,5	3,33	4ª
b) Ocorrência de incidente anterior		3,2			3,2			3,2			3,0			2,9			3,3			3,3		
g) Emergência contínua de novos riscos		3,4			3,4			3,6			3,3			3,3			3,7			3,4		
h) Alterações contínuas na legislação/regulação		3,1			2,8			3,2			2,9			2,9			3,3			3,1		
d) Planear a segurança da informação antes da implementação das novas tecnologias	Garantia da integração de Processos	3,6	3,60	2ª	3,6	3,60	2ª	3,5	3,50	2ª	3,6	3,60	2ª	3,4	3,40	2ª	3,3	3,30	4ª	3,6	3,60	2ª
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	Gestão Desempenho	3,2	3,20	5ª	3,0	2,80	5ª	3,3	3,25	4ª	3,3	3,25	4ª	3,0	2,95	5ª	3,7	3,20	5ª	3,3	3,35	3ª
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.		3,2			2,6			3,2			3,2			2,9			2,7			3,4		
c) Garantir a disponibilidade, confidencialidade e integridade da Informação	Gestão Recursos	3,8	3,80	1ª	3,8	3,80	1ª	3,8	3,80	1ª	3,9	3,90	1ª	3,7	3,70	1ª	4,0	4,00	1ª	3,8	3,80	1ª

Tabela 6.3- FM/PP: Comparação pelo Mapeamento ISACA

Já para os Factores Inibidores verifica-se que, globalmente, os respondentes fazem incidir a sua preferência em elementos do pilar de resultados – "*Garantia da integração de Processos*", mantendo-se a incidência da inibição na adopção/implementação do SGSI centrada em elementos relacionados com o "Factor Humano" – "*Falta de conhecimento*" e " *Cultura organizacional*" e com igualdade de importância no pilar de resultados – "*Gestão de Desempenho*", mostrando-se o elemento inibidor "*Dificuldade em medir o custo/benefício*".

De facto, os pilares de resultados – "*Alinhamento Estratégico*" e "*Gestão de Risco*", pedras angulares na governação da segurança da informação, surgem globalmente e respectivamente na terceira e quarta posição.

A tabela (Tabela 6.4) seguinte resume o acima mencionado.

Factores Inibidores (Nível médio de importância - PP)	Mapeamento ISACA	Global			GT			GI			GTI			CTI			G/FS			T		
		NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição
a) Valor do investimento	Gestão Recursos	3,2	3,20	2ª	3,4	3,40	1ª	3,3	3,30	3ª	3,2	3,20	2ª	3,2	3,20	1ª	2,7	2,70	5ª	3,2	3,20	3ª
b) Falta de conhecimento	Garantia da integração de Processos	3,3	3,30	1ª	3,3	3,10	3ª	3,5	3,45	2ª	3,1	3,25	1ª	3,1	3,10	2ª	3	3,00	4ª	3,5	3,50	1ª
c) Cultura organizacional		3,3			2,9			3,4			3,4			3,1			3			3,5		
d) Dificuldade em medir o custo/benefício	Gestão Desempenho	3,3	3,30	1ª	3,3	3,30	2ª	3,5	3,50	1ª	2,9	2,90	3ª	3,1	3,10	2ª	3,7	3,70	1ª	3,3	3,30	2ª
e) Acesso restrito à "Gestão de Topo"	Alinhamento Estratégico	2,9	2,90	3ª	2,7	2,70	5ª	2,9	2,90	5ª	2,9	2,90	3ª	2,5	2,50	3ª	3,3	3,30	2ª	3	3,00	4ª
f) Alterações contínuas na legislação / regulação	Gestão Risco	2,8	2,85	4ª	2,7	2,95	4ª	3	3,10	4ª	2,7	2,75	4ª	2,4	2,35	4ª	3	3,15	3ª	2,9	2,90	5ª
g) Emergência contínua de novos riscos		2,9			3,2			3,2			2,8			2,3			3,3			2,9		

Tabela 6.4- FI/PP: Comparação pelo Mapeamento ISACA

6.1.3 – Perspectiva do Próprio face à Organização

De seguida, e acompanhando o mesmo quadro de referência expositivo (Figura 6.6), inicia-se este sub-capítulo com a apresentação resumida da perspectiva do próprio face à organização, para os Factores Motivadores considerados.

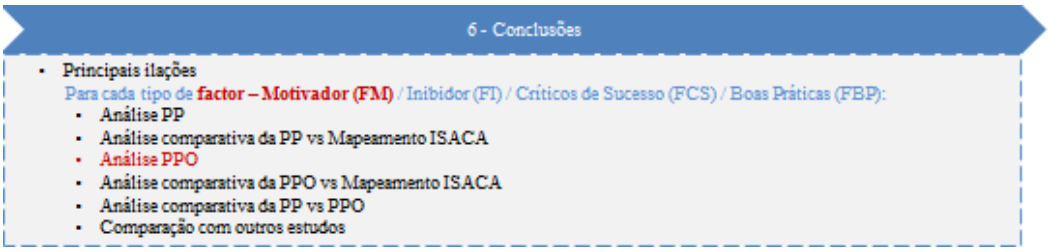


Figura 6.6- Modelo das Conclusões / Factores Motivadores - PPO

Deste modo, na perspectiva do próprio face à organização os Factores Motivadores que, globalmente apresentam maior nível médio de importância na implementação/adopção dum Sistema de Gestão da Segurança da Informação são os seguintes: "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (3,7), seguido dos elementos "*Evitar perdas financeiras*" e "*Planear a segurança da informação antes da implementação de novas tecnologias*" com valor idêntico (3,5). O elemento motivador "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" mostra-se na terceira posição (3,3).

No entanto, é de realçar o alinhamento de opinião face à organização, para o Gestor de Topo, o Gestor das TI e o Consultor das TI que consideram o elemento "*Garantir a disponibilidade, confidencialidade e integridade da informação*" como o mais motivador, respectivamente (3,8; 3,7; 3,6) seguindo-se o elemento "*Evitar perdas financeiras*" (3,7; 3,6; 3,5). O elemento "*Planear a segurança da informação antes da implementação de novas tecnologias*" surge na terceira posição (3,5; 3,5; 3,4) e o elemento "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" mostra-se na quarta posição (3,2; 3,4; 3,3).

Porém, do ponto de vista do Gestor Intermédio, o elemento "*Garantir a disponibilidade, confidencialidade e integridade da informação*" revela-se, também, como o mais motivador (3,7). Os elementos motivadores "*Evitar perdas financeiras*", "*Planear a segurança da informação antes da implementação de novas tecnologias*" e "*Emergência contínua de novos riscos*" apresentam-se na segunda posição (3,5). O elemento motivador "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" surge na última posição (3,2).

Por outro lado, do ponto de vista do Gestor/Funcionário da Segurança, os elementos "*Garantir a disponibilidade, confidencialidade e integridade da informação*" e "*Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança*" são apontados como os mais motivadores, apresentando um nível médio de importância igual (4,0). Os elementos motivadores "*Evitar perdas financeiras*",

"*Planear a segurança da informação antes da implementação de novas tecnologias*", "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" e "*Emergência contínua de novos riscos*" apresentam-se na segunda posição (3,7).

Já para o Trabalhador, o principal factor motivador continua a ser o elemento "*Garantir a disponibilidade, confidencialidade e integridade da informação*" (3,7). O elemento "*Planear a segurança da informação antes da implementação de novas tecnologias*" surge na segunda posição (3,6) e o elemento "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" revela-se na terceira posição em igualdade com o elemento "*Evitar perdas financeiras*" (3,4).

O gráfico (Gráfico 6.3) seguinte resume o acima mencionado.

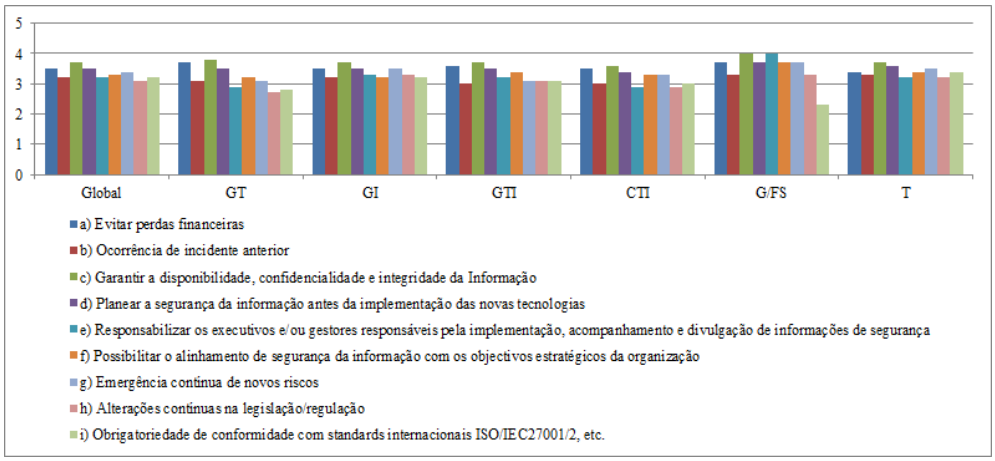


Gráfico 6.3- FM/PPO: Comparação pelo Tipo Função e Nível Médio de Importância

Resumindo e conforme tabela (Tabela 6.5) a seguir o elemento motivador "*Garantir a disponibilidade, confidencialidade e integridade da Informação*" surge como o mais referido, por todos os tipos de funções do respondente, variando, no entanto, os níveis médios de importância atribuídos (entre 3,6 a 4,0), sendo o valor médio global (3,5).

Em segundo lugar, também assinalado por todos os tipos de funções dos respondentes, com excepção do Trabalhador, revela-se o elemento motivador "*Evitar perdas financeiras*" com pontuações entre (3,5 a 3,7), sendo o valor global do nível médio de importância (3,5).

De sublinhar que o elemento motivador "*Planear a segurança da informação antes da implementação de novas tecnologias*" manifesta-se, respectivamente, na segunda posição para o Gestor Intermédio, o Gestor/Funcionário de Segurança e o Trabalhador, aparecendo na terceira posição para o Gestor de Topo, Gestor das TI e Consultor das TI, quando estes indicam o seu ponto de vista face à organização.

Constata-se, ainda, que o elemento motivador "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" é assinalado na quarta posição por todos os tipos de funções dos respondentes, com excepção do Gestor/Funcionário de Segurança que assinala o mesmo na segunda posição.

De referir que nesta perspectiva, do próprio face à organização, encontra-se uma maior semelhança de opiniões do que quando analisada a perspectiva do próprio.

Factores Motivadores (Nível médio de importância - PPO)	Global	GT	GI	GTI	CTI	G/FS	T
a) Evitar perdas financeiras	3,5	3,7	3,5	3,6	3,5	3,7	3,4
b) Ocorrência de incidente anterior	3,2	3,1	3,2	3,0	3	3,3	3,3
c) Garantir a disponibilidade, confidencialidade e integridade da Informação	3,7	3,8	3,7	3,7	3,6	4,0	3,7
d) Planear a segurança da informação antes da implementação das novas tecnologias	3,5	3,5	3,5	3,5	3,4	3,7	3,6
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	3,2	2,9	3,3	3,2	2,9	4,0	3,2
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	3,3	3,2	3,2	3,4	3,3	3,7	3,4
g) Emergência contínua de novos riscos	3,4	3,1	3,5	3,1	3,3	3,7	3,5
h) Alterações contínuas na legislação/regulação	3,1	2,7	3,3	3,1	2,9	3,3	3,2
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.	3,2	2,8	3,2	3,1	3	2,3	3,4
Legenda							
Posição	1ª	2ª	3ª	4ª	5ª	6ª	

Tabela 6.5- FM/PPO: Posicionamento dos elementos por Tipo de Função

Segue-se o mesmo referencial expositivo para a mesma perspectiva – a do próprio face à organização, conforme figura abaixo (Figura 6.7), tendo em conta, agora, os Factores Inibidores.

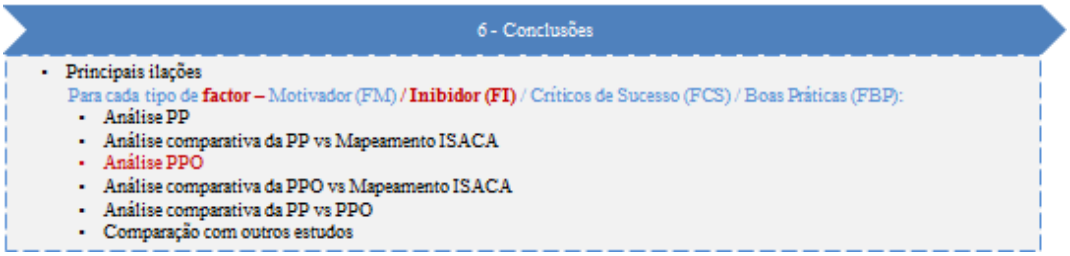


Figura 6.7- Modelo das Conclusões / Factores Inibidores - PPO

Desta forma, os Factores Inibidores que, globalmente apresentam maior nível médio de importância (3,3) na implementação/adopção dum Sistema de Gestão da Segurança da Informação (SGSI) são: "*Cultura organizacional*" e "*Valor do investimento*". O elemento "*Acesso restrito à Gestão de Topo*" surge na última posição, com valor idêntico para o nível

médio de importância (2,9), ao dos elementos "*Emergência contínua de novos riscos*" e "*Alterações contínuas na legislação/regulação*".

Contudo, nesta perspectiva, o Gestor de Topo, o Gestor Intermédio, o Gestor das TI e o Consultor das TI destacam o elemento "*Valor do investimento*" respectivamente (3,6), (3,5), (3,4) e (3,2), como o mais inibidor.

Todavia, o Gestor de Topo coloca na segunda posição, apresentando o mesmo nível médio de importância (3,1), quatro dos sete elementos inibidores considerados: "*Falta de conhecimento*", "*Cultura organizacional*", "*Dificuldade em medir o custo benefício*" e "*Emergência contínua de novos riscos*". Relativamente ao elemento "*Acesso restrito à Gestão de Topo"* mostra-se, na última posição em igualdade de pontuação (2,7) com o elemento "*Alterações contínuas na legislação/regulação*".

Já o Gestor Intermédio elege também para a primeira posição e com o mesmo nível médio de importância (3,5) o elemento inibidor "*Dificuldade em medir o custo benefício*". Os elementos relacionados com o "Factor Humano" são considerados, na segunda e terceira posição, respectivamente, "*Falta de conhecimento*" (3,4) e "*Cultura organizacional*" (3,3). O elemento inibidor "*Acesso restrito à Gestão de Topo"* surge na última posição, parecendo não ser um obstáculo na implementação/adopção dum SGSI.

O Gestor das TI menciona na segunda posição dois elementos inibidores com o mesmo nível médio de importância (3,2): "*Cultura organizacional*" e "*Dificuldade em medir o custo benefício*". O elemento "*Acesso restrito à Gestão de Topo"* surge na terceira posição em igualdade com o elemento "*Falta de conhecimento*", mostrando o mesmo valor para o nível médio de importância (3,0).

Porém, o Consultor das TI destaca na segunda posição o elemento relacionado com o "Factor Humano" - "*Cultura organizacional*", atribuindo-lhe o valor (3,0) para o nível médio de importância. O outro elemento relacionado com o "Factor Humano" – "*Falta de conhecimento*" surge na terceira posição, em igualdade de pontuação (2,9) com o elemento "*Dificuldade em medir o custo benefício*". Já o elemento inibidor "*Acesso restrito à Gestão de Topo"* revela-se na quarta posição.

Da parte do Gestor/Funcionário da Segurança obteve-se uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). No entanto, o elemento inibidor "*Dificuldade em medir o custo benefício*" obtém o maior nível médio de importância (3,7). Os elementos relacionados com o "Factor Humano" - "*Falta de conhecimento*" e "*Cultura organizacional*" mostram-se, respectivamente, na segunda (3,3) e terceira (3,0) posição. O elemento inibidor

"*Acesso restrito à Gestão de Topo*" surge na segunda posição em igualdade de pontuação com o elemento "*Falta de conhecimento*".

Por último, o Trabalhador declara o "Factor Humano" como o principal "*driver inibidor*" ao classificar os dois elementos "*Falta de conhecimento*" e "*Cultura organizacional*" como os elementos inibidores de maior nível médio de importância (3,4). Para esta classe, o elemento "*Acesso restrito à Gestão de Topo*" aparece na quinta posição (2,9).

O gráfico abaixo (Gráfico 6.4) ilustra o acima mencionado.

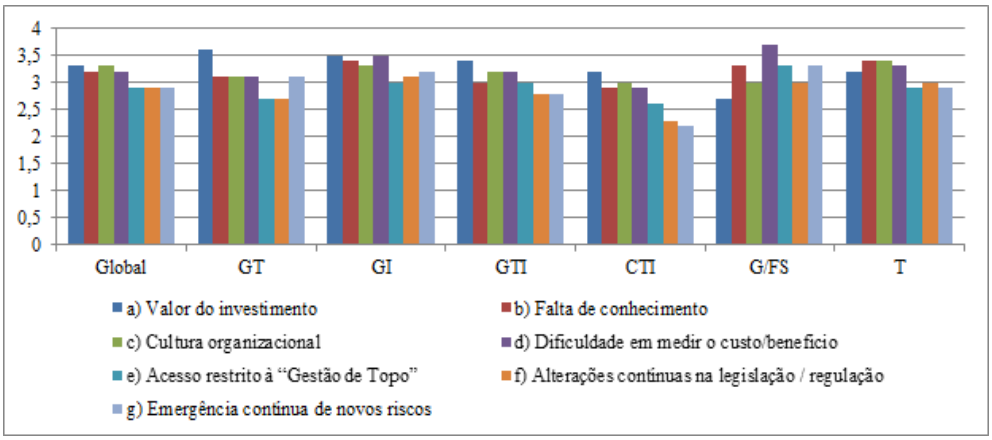


Gráfico 6.4- FI/PPO: Comparação pelo Tipo de Função e Nível Médio de Importância

Resumindo e conforme tabela (Tabela 6.6) a seguir, na perspectiva do próprio face à organização, constata-se um alinhamento de opinião na classificação do elemento mais inibidor – "*Valor do investimento*" na implementação/adopção dum Sistema de Gestão da Segurança da Informação (SGSI).

Contudo, é de realçar que os elementos relacionados com o "Factor Humano" - "*Falta de conhecimento*" e "*Cultura organizacional*" encontram-se maioritariamente mencionados, pelos diferentes tipos de respondentes, nas três primeiras posições e, globalmente revelam-se, respectivamente na segunda (3,2) e na primeira (3,3) posição, o que indicia que, na perspectiva do próprio face à organização, os respondentes reconhecem a importância destes factores na implementação/adopção dum Sistema de Gestão da Segurança da Informação.

De notar também que o elemento inibidor "*Acesso restrito à Gestão de Topo*", com excepção do Gestor/Funcionário da Segurança (que o coloca na segunda posição), aparece classificado a partir da terceira posição, parecendo não se apresentar como um factor inibidor relevante, na perspectiva do próprio face à organização, para o sector em causa. De facto o Gestor Intermédio coloca-o na sexta posição, o Gestor das TI coloca-o na quarta posição e o Trabalhador refere-o na quinta posição.

Factores Inibidores (Nivel médio de importância - PPO)	Global	GT	GI	GTI	CTI	G/FS	T
a) Valor do investimento	3,3	3,6	3,5	3,4	3,2	2,7	3,2
b) Falta de conhecimento	3,2	3,1	3,4	3	2,9	3,3	3,4
c) Cultura organizacional	3,3	3,1	3,3	3,2	3	3	3,4
d) Dificuldade em medir o custo/benefício	3,2	3,1	3,5	3,2	2,9	3,7	3,3
e) Acesso restrito à "Gestão de Topo"	2,9	2,7	3	3	2,6	3,3	2,9
f) Alterações contínuas na legislação / regulação	2,9	2,7	3,1	2,8	2,3	3	3
g) Emergência contínua de novos riscos	2,9	3,1	3,2	2,8	2,2	3,3	2,9
Legenda							
Posição	1ª	2ª	3ª	4ª	5ª	6ª	

Tabela 6.6- FI/PPO: Posicionamento dos elementos por Tipo de Função

6.1.4 – Perspectiva do Próprio face à Organização vs Mapeamento ISACA

Retomando o referencial expositivo indicado na figura seguinte (Figura 6.8) e recordando o mapeamento efectuado no ponto 4.2 deste documento – orientação segundo o ISACA [135] indicando que «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*», de seguida, apresentam-se as observações encontradas para os Factores Motivadores e Inibidores tendo em conta a perspectiva do próprio face à organização.

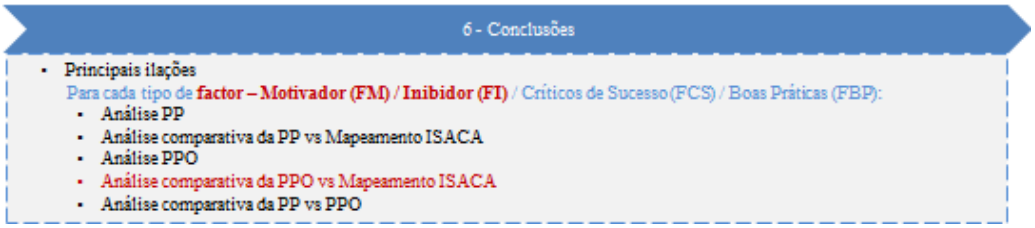


Figura 6.8- Modelo das Conclusões / Análise comparativa vs Mapeamento ISACA

Assim, perante os resultados dos valores médios de importância encontrados para os elementos considerados na caracterização dos Factores Motivadores verifica-se que, globalmente, os respondentes fazem incidir a sua preferência em elementos do pilar de resultados – "*Gestão de Recursos*", mantendo-se a incidência da motivação para a adopção/implementação do SGSI centrada na "protecção de activos".

De facto, o pilar de resultados – "*Alinhamento Estratégico*" aparece na terceira posição para o Gestor de Topo, o Gestor das TI, Consultor das TI e Trabalhador, apresentando, globalmente, nível médio de importância (3,3). Revela-se na segunda posição para o Gestor/Funcionário da Segurança e em quinto lugar para o Gestor Intermédio.

A tabela (Tabela 6.7) seguinte resume o acima mencionado.

Factores Motivadores (Nível médio de importância - PPO)	Mapeamento ISACA	Global			GT			GI			GTI			CTI			G/FS			T		
		NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	Alinhamento Estratégico	3,3	3,30	3ª	3,2	3,20	3ª	3,2	3,20	5ª	3,4	3,40	3ª	3,3	3,30	3ª	3,7	3,70	2ª	3,4	3,40	3ª
a) Evitar perdas financeiras	Gestão Risco	3,5	3,30	3ª	3,7	3,15	4ª	3,5	3,38	3ª	3,6	3,20	4ª	3,5	3,18	4ª	3,7	3,50	3ª	3,4	3,35	4ª
b) Ocorrência de incidente anterior		3,2			3,1			3,2			3,0			3,0			3,3			3,3		
g) Emergência contínua de novos riscos		3,4			3,1			3,5			3,1			3,3			3,7			3,5		
h) Alterações contínuas na legislação/regulação		3,1			2,7			3,3			3,1			2,9			3,3			3,2		
d) Planear a segurança da informação antes da implementação das novas tecnologias	Garantia da integração de Processos	3,5	3,50	2ª	3,5	3,50	2ª	3,5	3,50	2ª	3,5	3,50	2ª	3,4	3,40	2ª	3,7	3,70	2ª	3,6	3,60	2ª
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	Gestão Desempenho	3,2	3,20	4ª	2,9	2,85	5ª	3,3	3,25	4ª	3,2	3,15	5ª	2,9	2,95	5ª	4,0	3,15	4ª	3,2	3,30	5ª
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.		3,2			2,8			3,2			3,1			3,0			2,3			3,4		
c) Garantir a disponibilidade, confidencialidade e integridade da Informação	Gestão Recursos	3,7	3,70	1ª	3,8	3,80	1ª	3,7	3,70	1ª	3,7	3,70	1ª	3,6	3,60	1ª	4,0	4,00	1ª	3,7	3,70	1ª

Tabela 6.7- FM/PPO: Comparação pelo Mapeamento ISACA

Já para os Factores Inibidores os resultados dos valores médios de importância encontrados para os elementos considerados na sua caracterização, revelam que, globalmente, os respondentes incidem a sua preferência dos elementos inibidores no pilar de resultados – "*Gestão de Recursos*" – "*Valor do investimento*" (3,3).

Todavia, de notar que os elementos relacionados com o "Factor Humano" – "*Falta de conhecimento*" e "*Cultura organizacional*" e considerados como inibidores na adopção/implementação do SGSI surgem classificados na segunda posição, mostrando o elemento "*Cultura organizacional*" o mesmo valor (3,3) que o elemento considerado como o mais inibidor - "*Valor do investimento*" (3,3). Porém, o Trabalhador coloca-os na primeira posição, reflectindo a importância destes elementos na implementação/adopção dum Sistema de Gestão da Segurança da Informação. Por outro lado, os Gestores das TI e os Gestores/Funcionários da Segurança (talvez por serem os principais "promotores" da governação da segurança da informação) remetem os elementos relacionados com o "Factor Humano" para a terceira posição do nível médio de importância.

Os pilares de resultados – "*Alinhamento Estratégico*" e "*Gestão de Risco*", pedras angulares na governação da segurança da informação, surgem globalmente, em igualdade, na quarta posição.

A tabela (Tabela 6.8) seguinte resume o acima mencionado.

Factores Inibidores (Nível médio de importância - PPO)	Mapeamento ISACA	Global			GT			GI			GTI			CTI			G/FS			T		
		NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição
a) Valor do investimento	Gestão Recursos	3,3	3,30	1ª	3,6	3,60	1ª	3,5	3,50	1ª	3,4	3,40	1ª	3,2	3,20	1ª	2,7	2,70	4ª	3,2	3,20	3ª
b) Falta de conhecimento	Garantia da integração de Processos	3,2	3,25	2ª	3,1	3,10	2ª	3,4	3,35	2ª	3	3,10	3ª	2,9	2,95	2ª	3,3	3,15	3ª	3,4	3,40	1ª
c) Cultura organizacional		3,3			3,1			3,3			3,2			3			3			3,4		
d) Dificuldade em medir o custo/benefício	Gestão Desempenho	3,2	3,20	3ª	3,1	3,10	2ª	3,5	3,50	1ª	3,2	3,20	2ª	2,9	2,90	3ª	3,7	3,70	1ª	3,3	3,30	2ª
e) Acesso restrito à "Gestão de Topo"	Alinhamento Estratégico	2,9	2,90	4ª	2,7	2,70	4ª	3	3,00	3ª	3	3,00	4ª	2,6	2,60	4ª	3,3	3,30	2ª	2,9	2,90	5ª
f) Alterações contínuas na legislação / regulação	Gestão Risco	2,9	2,90	4ª	2,7	2,90	3ª	3,1	3,15	2ª	2,8	2,80	5ª	2,3	2,25	5ª	3	3,15	3ª	3	2,95	4ª
g) Emergência contínua de novos riscos		2,9			3,1			3,2			2,8			2,2			3,3			2,9		

Tabela 6.8- FI/PPO: Comparação pelo Mapeamento ISACA

6.1.5 – Perspectiva do Próprio vs Perspectiva do Próprio face à Organização

Relembrando o referencial de apresentação de acordo com o indicado na figura abaixo (Figura 6.9), e iniciando-se pelos Factores Motivadores, neste ponto descrevem-se as principais observações encontradas na análise comparativa efectuada entre as duas perspectivas.

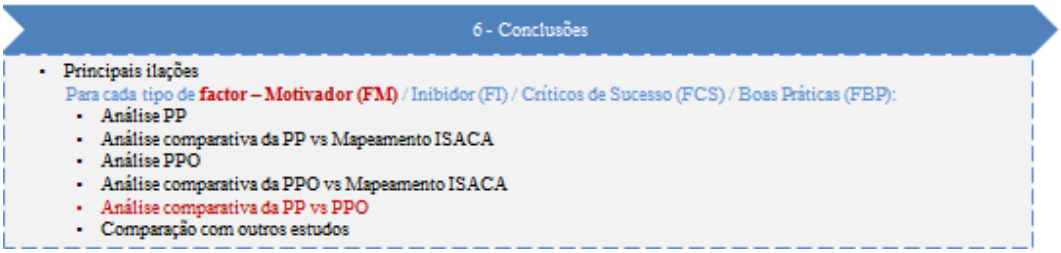


Figura 6.9- Modelo das Conclusões / Factores Motivadores – PP vs PPO

Assim, este estudo também permitiu identificar, para os elementos motivadores considerados, desvios existentes entre as duas perspectivas (PP e PPO) tendo-se destacado os seguintes:

- Os Gestores de Topo e os Gestores das TI apresentam desvios entre as duas perspectivas para todos os elementos motivadores, com excepção do elemento "*Garantir a disponibilidade, confidencialidade e integridade da Informação*", no caso do Gestor de Topo e dos elementos "*Evitar perdas financeiras*" e "*Ocorrência de incidente anterior*" no caso do Gestor das TI.

- Os desvios de maior valor absoluto também aparecem nas opiniões emitidas pelos Gestores de Topo e Gestores das TI, surgindo no elemento motivador "*Emergência contínua de novos riscos*" um desvio de (0,3), para o Gestor de Topo e de (0,2) para o Gestor das TI. A perspectiva do próprio apresenta sempre um nível médio de importância superior quando comparado com o nível médio de importância atribuído na perspectiva do próprio face à organização.

- O Gestor Intermédio assinala desvios em quatro dos nove elementos motivadores e o Trabalhador diferencia cinco dos nove elementos. De realçar o desvio (0,2) para o elemento motivador "*Evitar perdas financeiras*".
- O elemento motivador "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização*" só apresenta desvios nas perspectivas do Gestor de Topo (0,2) e do Gestor das TI (0,1).

A tabela (Tabela 6.9) seguinte resume o acima mencionado.

Factores Motivadores (Nível médio de importância - Desvios entre as PP e PPO)	Global	Global	Desvio	GT	GT	Desvio	GI	GI	Desvio	GTI	GTI	Desvio	CTI	CTI	Desvio	G/FS	G/FS	Desvio	T	T	Desvio
	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO
a) Evitar perdas financeiras	3,6	3,5	0,1	3,9	3,7	0,2	3,7	3,5	0,2	3,6	3,6	0,0	3,5	3,5	0,0	3,7	3,7	0,0	3,5	3,4	0,1
b) Ocorrência de incidente anterior	3,2	3,2	0,0	3,2	3,1	0,1	3,2	3,2	0,0	3,0	3,0	0,0	2,9	3,0	-0,1	3,3	3,3	0,0	3,3	3,3	0,0
c) Garantir a disponibilidade, confidencialidade e integridade da Informação	3,8	3,7	0,1	3,8	3,8	0,0	3,8	3,7	0,1	3,9	3,7	0,2	3,7	3,6	0,1	4,0	4,0	0,0	3,8	3,7	0,1
d) Planear a segurança da informação antes da implementação das novas tecnologias	3,6	3,5	0,1	3,6	3,5	0,1	3,5	3,5	0,0	3,6	3,5	0,1	3,4	3,4	0,0	3,3	3,7	-0,4	3,6	3,6	0,0
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	3,2	3,2	0,0	3,0	2,9	0,1	3,3	3,3	0,0	3,3	3,2	0,1	3,0	2,9	0,1	3,7	4,0	-0,3	3,3	3,2	0,1
f) Possibilitar o alinhamento de segurança da informação com os objectivos estratégicos da organização	3,4	3,3	0,1	3,4	3,2	0,2	3,2	3,2	0,0	3,5	3,4	0,1	3,3	3,3	0,0	3,7	3,7	0,0	3,4	3,4	0,0
g) Emergência contínua de novos riscos	3,4	3,4	0,0	3,4	3,1	0,3	3,6	3,5	0,1	3,3	3,1	0,2	3,3	3,3	0,0	3,7	3,7	0,0	3,4	3,5	-0,1
h) Alterações contínuas na legislação/regulação	3,1	3,1	0,0	2,8	2,7	0,1	3,2	3,3	-0,1	2,9	3,1	-0,2	2,9	2,9	0,0	3,3	3,3	0,0	3,1	3,2	-0,1
i) Obrigatoriedade de conformidade com *standards* internacionais ISO/IEC27001/2, etc.	3,2	3,2	0,0	2,6	2,8	-0,2	3,2	3,2	0,0	3,2	3,1	0,1	2,9	3,0	-0,1	2,7	2,3	0,4	3,4	3,4	0,0

Tabela 6.9- FM/Desvios PP-PPO: Comparação pelo Tipo Função e Nível Médio de Importância

De facto, cruzando esta informação com os mapeamentos ISACA [136] verifica-se que, nos Gestores de Topo, a incidência dos maiores desvios da opinião (PP vs PPO), sobre quais os Factores Motivadores na implementação/adopção dum Sistema de Gestão da Segurança da Informação, recaem sobre elementos dos pilares de resultados "*Gestão de Risco*" e do "*Alinhamento Estratégico*". Todavia, de realçar o desvio (0,2) apresentado pelo Gestor das TI para o elemento motivador "*Garantir a disponibilidade, confidencialidade e integridade da Informação*", o qual enquadra o pilar de resultados – "*Gestão de Recursos*".

Recuperando o referencial expositivo conforme figura (Figura 6.10) abaixo, nesta parte identificam-se os desvios encontrados, entre as duas perspectivas (PP e PPO), para os Factores Inibidores considerados.

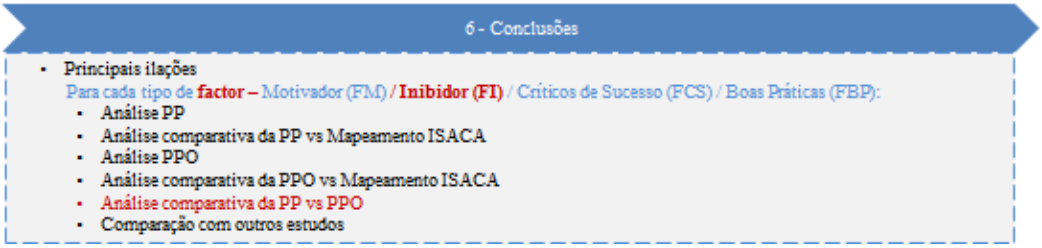


Figura 6.10- Modelo das Conclusões / Factores Inibidores – PP vs PPO

Assim, destacam-se os seguintes:

- Globalmente, os desvios entre as perspectivas aparecem em quatro dos sete elementos inibidores considerados, a saber: "*Valor do investimento*", "*Falta de conhecimento*", "*Dificuldade em medir o custo/benefício*" e "*Alterações contínuas na legislação/regulação*".

- O elemento considerado, na perspectiva do próprio face à organização, como o mais inibidor "*Valor do investimento*" apresenta desvio negativo (-0,2) segundo as opiniões dos Gestores de Topo, Gestores Intermédios e Gestores das TI. Deste modo, estes respondentes consideram que, na perspectiva do próprio, este elemento inibidor adquire menor valor de nível médio de importância do que quando indicada a perspectiva do próprio face à organização.

- O elemento inibidor "*Dificuldade em medir o custo/benefício*" é o que apresenta o maior valor absoluto do desvio (-0,3) e é referido pelo Gestor das TI. Assim, esta classe indica que na perspectiva do próprio este elemento não adquire tanta importância, como inibidor, do que quando comparado com a perspectiva do próprio face à organização.

- Relativamente aos elementos considerados inibidores e relacionados com o "Factor Humano" - "*Falta de conhecimento*" e "*Cultura organizacional*" constata-se que todas as classes de respondentes, com excepção dos Gestores/Funcionários da Segurança, apresentam desvios entre as perspectivas do próprio e do próprio face à organização. Estes desvios são maioritariamente positivos, ou seja, o nível médio de importância atribuído é maior quando se trata da perspectiva do próprio quando comparada com a perspectiva do próprio face à organização. Assim, estes elementos são considerados mais inibidores na perspectiva do próprio.

- O elemento inibidor "*Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização"* apresenta um desvio negativo (-0,1) nas perspectivas do Gestor Intermédio, do Gestor das TI e Consultor das TI, mostrando que na perspectiva do próprio o nível médio de importância é menor quando comparado com o nível médio de importância dada pelos respondentes na perspectiva do próprio face à organização. Contudo, embora de igual valor (0,1) este desvio passa a positivo na perspectiva do Trabalhador indicando que, na perspectiva do próprio, este elemento é mais importante como inibidor do que quando comparado com a perspectiva do próprio face à organização.

A tabela (Tabela 6.10) seguinte resume o acima mencionado.

Factores Inibidores (Nível médio de importância - Desvios entre as PP e PPO)	Global	Global	Desvio	GT	GT	Desvio	GI	GI	Desvio	GTI	GTI	Desvio	CTI	CTI	Desvio	G/FS	G/FS	Desvio	T	T	Desvio
	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO
a) Valor do investimento	3,2	3,3	-0,1	3,4	3,6	-0,2	3,3	3,5	-0,2	3,2	3,4	-0,2	3,2	3,2	0,0	2,7	2,7	0,0	3,2	3,2	0,0
b) Falta de conhecimento	3,3	3,2	0,1	3,3	3,1	0,2	3,5	3,4	0,1	3,1	3,0	0,1	3,1	2,9	0,2	3,0	3,3	-0,3	3,5	3,4	0,1
c) Cultura organizacional	3,3	3,3	0,0	2,9	3,1	-0,2	3,4	3,3	0,1	3,4	3,2	0,2	3,1	3,0	0,1	3,0	3,0	0,0	3,5	3,4	0,1
d) Dificuldade em medir o custo/benefício	3,3	3,2	0,1	3,3	3,1	0,2	3,5	3,5	0,0	2,9	3,2	-0,3	3,1	2,9	0,2	3,7	3,7	0,0	3,3	3,3	0,0
e) Acesso restrito à "Gestão de Topo"	2,9	2,9	0,0	2,7	2,7	0,0	2,9	3,0	-0,1	2,9	3,0	-0,1	2,5	2,6	-0,1	3,3	3,3	0,0	3,0	2,9	0,1
f) Alterações continuas na legislação / regulação	2,8	2,9	-0,1	2,7	2,7	0,0	3,0	3,1	-0,1	2,7	2,8	-0,1	2,4	2,3	0,1	3,0	3,0	0,0	2,9	3,0	-0,1
g) Emergência continua de novos riscos	2,9	2,9	0,0	3,2	3,1	0,1	3,2	3,2	0,0	2,8	2,8	0,0	2,3	2,2	0,1	3,3	3,3	0,0	2,9	2,9	0,0

Tabela 6.10- FI/Desvios PP-PPO: Comparação pelo Tipo Função e Nível Médio de Importância

De facto, cruzando esta informação com os mapeamentos ISACA [137] (conforme ponto 4.2) verifica-se que, globalmente, na perspectiva do próprio, a incidência da importância dos elementos inibidores recai no pilar de resultados – "*Garantia da integração de Processos*" que inclui os elementos relacionados com o "Factor Humano". Porém, na perspectiva do próprio face à organização, a indicação da importância manifesta-se no pilar de resultados – "*Gestão de Recursos*".

6.1.6 - Comparação com outros estudos

De acordo com o quadro de referência indicado na figura (Figura 6.11) seguinte, nesta parte relacionam-se as observações obtidas neste estudo com os resultados encontrados através da revisão bibliográfica realizada.

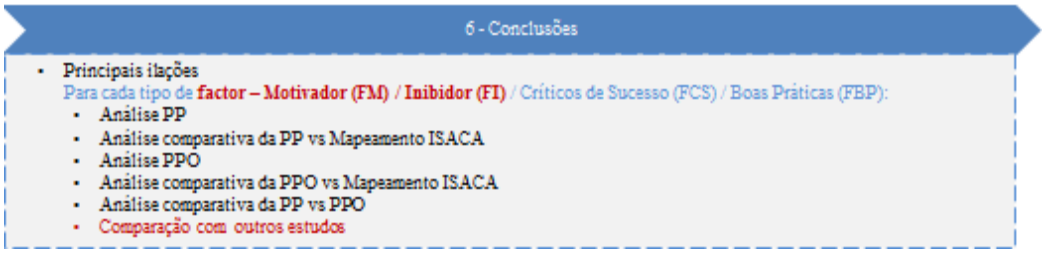


Figura 6.11- Modelo das Conclusões – FM/FI - Comparação com outros estudos

Pironti, John P. [138] refere que «*numa pesquisa realizada através da web, onde participaram cento e quarenta e oito Gestores de Segurança da Informação Certificados (CISMs), representando quarenta e um países e fornecendo uma visão sobre que factores motivam as organizações a implementar / adoptar uma iniciativa de governação de segurança da informação, foram indicados como:*

- *Factores motivadores mais mencionados: ´preocupação com a responsabilidade legal´; ´protecção da reputação da organização´ e o ´cumprimento da regulamentação´ – obtendo valores médios de importância maiores que quatro numa escala de cinco pontos.*
- *Factores motivadores menos mencionados: ´processos de melhoria´; ´optimização da utilização dos recursos de segurança´ e ´dependência de interacções com parceiros comerciais e fornecedores´».*

Todavia, segundo o mesmo autor e referindo-se ao mesmo estudo «*os factores motivadores considerados como mais significativos eram coerentes entre todos os participantes, mas foram detectadas diferenças nas prioridades entre os diferentes grupos. Assim, os executivos indicam respectivamente: ´preocupação com a responsabilidade legal´; ´protecção da reputação da organização´ e 'gestão de risco'; os gestores das TI referem quatro factores igualmente importantes: ´preocupação com a responsabilidade legal´; ´cumprimento da regulamentação'; 'assegurar à gestão de topo a garantia da conformidade com a política' e ´gestão de risco a um nível aceitável´. Porém, aqueles que tinham completado um projecto de governação da segurança da informação ou estavam a avançar na direcção da governação da segurança da informação indicavam como factores motivadores mais significativos os seguintes: ´protecção da reputação da organização´, ´preocupação com a responsabilidade legal e 'assegurar à gestão de topo a garantia da conformidade com a política'».*

Neste contexto, o presente estudo mostra divergências verificando-se que a *´preocupação com a responsabilidade legal´* representada no presente estudo pelo elemento *'Alterações contínuas da legislação/regulação´* é assinalada globalmente na última posição em ambas as perspectivas e, também, indicada pelos Gestor de Topo e o Gestor das TI nas últimas posições, verificando-se, contudo desvios entre as perspectivas do próprio e do próprio face à organização. Porém, a diferença entre as perspectivas, no Gestor de Topo, é positiva, ou seja, o próprio considera o elemento mais significativo quando comparada com a perspectiva do próprio face à organização. Todavia, para o Gestor das TI, o desvio é negativo, isto é, o próprio classifica este elemento como menos significativo do que quando comparado com a perspectiva do próprio face à organização.

Já para o elemento *'assegurar à gestão de topo a garantia da conformidade com a política'* que no presente trabalho se traduz no elemento *´Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização´* verifica-se que globalmente aparece na terceira posição, na perspectiva do próprio e na quarta posição, na perspectiva do próprio face à organização, seguindo esta tendência a opinião do Gestor das TI. Mas, para o Gestor de Topo revela-se na quarta posição em ambas as perspectivas. Contudo, ambos os grupos apresentam, desvios positivos (respectivamente: 0,1; 0,2) indicando que o próprio atribui-lhe mais importância do que quando comparada com a perspectiva do próprio face à organização.

Tomando como referencial de maturidade da cultura da governação da segurança da informação nas organizações aqueles elementos, nota-se que, no sector das Águas e Saneamento em Portugal, a motivação para a implementação/adopção dum Sistema de Gestão da Segurança da Informação (SGSI) demonstra um nível inicial de maturidade.

Também mencionando o ISACA [139], este refere que «*Para ser justo, os profissionais da segurança da informação têm realizado um trabalho louvável dado os poucos recursos disponíveis. Orçamentos baixos, recursos humanos limitados e acesso restrito à gestão de topo são obstáculos comuns que os profissionais da segurança da informação enfrentam enquanto tentam proteger os activos informacionais, minimizar o risco e proporcionar valor acrescentado ao negócio*». Contudo, no presente estudo verifica-se que os dois elementos considerados, globalmente, como mais inibidores, na perspectiva do próprio estão relacionados com o "factor humano" - "*Falta de conhecimento*", "*Cultura organizacional*", sendo este último elemento apontado também na perspectiva do próprio face à organização em paralelo com o elemento inibidor "*Dificuldade em medir o custo/benefício*". Todavia, o gestor de topo realça, em ambas as perspectivas, o elemento "*Valor do investimento*" como o mais inibidor, corroborando este facto o acima mencionado e indicado pelo ISACA. O Gestor das TI e o Gestor Intermédio consideram como mais inibidores, na perspectiva do próprio, os elementos relacionados com o "factor humano" – "*Falta de conhecimento*", "*Cultura organizacional*". Porém, na perspectiva do próprio face à organização apontam o elemento inibidor "*Valor do Investimento*". Já o Trabalhador escolhe, em ambas as perspectivas, como mais inibidores, os elementos relacionados com o "factor humano" - "*Falta de conhecimento*", "*Cultura organizacional*".

Este cenário pode indiciar o ponto de viragem para a consciencialização da importância da governação da segurança da informação no sector em estudo.

6.2- Factores Críticos de Sucesso

Um outro eixo de análise deste estudo foi a vertente dos Factores Críticos de Sucesso conforme se indica na figura (Figura 6.12) seguinte. Deste modo, este sub-capítulo trata as observações encontradas relativamente às perspectivas do próprio e do próprio face à organização, as comparações encontradas entre as mesmas, bem como o confronto existente, tendo por base o mapeamento com o referencial ISACA [140] (conforme ponto 4.2) e com outros estudos achados na revisão bibliográfica realizada.

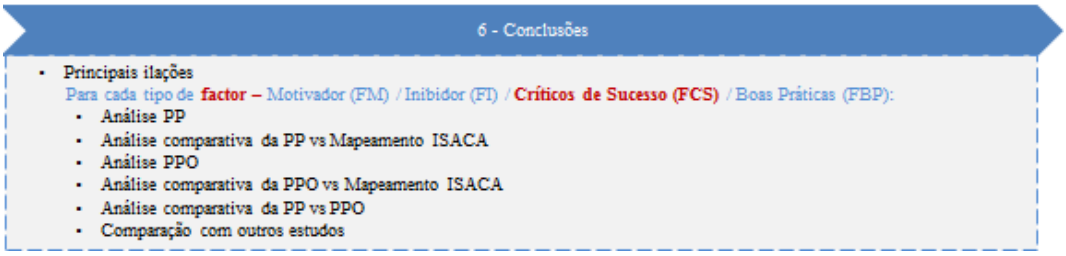


Figura 6.12- Modelo das Conclusões - FCS

6.2.1 – Perspectiva do Próprio

Assim, inicia-se esta apresentação dos resultados pela exposição da perspectiva do próprio, conforme indicado na figura abaixo (Figura 6.13).

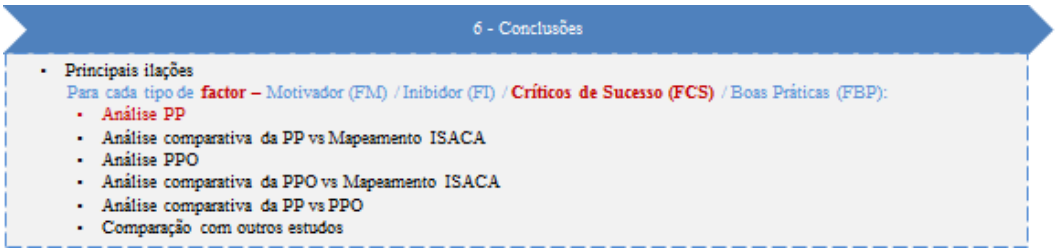


Figura 6.13- Modelo das Conclusões – FCS/Análise da PP

Nesta perspectiva os Factores Críticos de Sucesso que, globalmente apresentam maior nível médio de importância na implementação/adopção dum Sistema de Gestão da Segurança da Informação (SGSI) são: "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" (3,6), seguido dos elementos "*Suporte da Gestão de Topo*", "*Responsabilização pela Segurança da Informação*" e "*Motivação dos funcionários*" com o mesmo nível médio de importância (3,5). De realçar, ainda, que os elementos "*Programas para a conscientização, educação e formação em segurança em informação*" e "*Política de Segurança da Informação*" surgem na terceira posição (3,4) e o elemento "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)"* mostra-se na quarta posição com o valor de (3,3) para o nível médio de importância.

Deste modo, verifica-se que o enfoque dos Factores Críticos de Sucesso destaca-se em elementos relacionados com o "Factor Humano" e/ou com elementos ligados ao "*Alinhamento Estratégico*" da Governação Organizacional.

Porém, nesta perspectiva do próprio, o Gestor de Topo e o Consultor das TI seguem a tendência global e consideram, como factor crítico de sucesso de maior nível médio de importância, o elemento "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" (3,8; 3,7) vindo logo depois o elemento "*Suporte da Gestão de Topo*" (3,7; 3,5). Contudo, estas classes apontam na terceira posição os elementos críticos de sucesso "*Responsabilização pela*

Segurança da Informação" e "*Motivação dos funcionários*" com o mesmo nível médio de importância (3,6; 3,4).Todavia, o Gestor de Topo remete, respectivamente, para a quarta (3,4) e quinta (3,3) posição os elementos críticos de sucesso "*Política de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)"*, enquanto que o Consultor das TI assinala o elemento "*Política de Segurança da Informação*" na terceira (3,4) posição e coloca o elemento "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)"*, na sexta (2,7) posição.

Já o Gestor Intermédio e o Gestor das TI emergem com opiniões idênticas e indicam, como principais Factores Críticos de Sucesso, os seguintes elementos: "*Responsabilização pela Segurança da Informação*" (3,7), "*Suporte da Gestão de Topo*" (3,6) e "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" (3,5). Todavia, o elemento crítico de sucesso "*Motivação dos funcionários*" que se encontra relacionada com o "Factor Humano" revela-se na quarta (3,4) posição do nível médio de importância e os elementos relacionados com o "*Alinhamento Estratégico*" da Governação Organizacional aparecem, respectivamente, na quinta – "*Política de Segurança da Informação*" (3,3) e na sétima – "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)"* (3,1) posição.

Para o Gestor/Funcionário da Segurança obteve-se uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). No entanto, o elemento crítico de sucesso "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" obtém um nível médio de importância (3,7) em igualdade com os seguintes elementos: "*Responsabilização pela Segurança da Informação*", "*Programas para a conscientização, educação e formação em segurança em informação*" e "*Auditorias de Segurança da Informação*".

Por último, o Trabalhador aponta na primeira posição um elemento crítico de sucesso fortemente relacionado com o "Factor Humano" - "*Motivação dos funcionários*" atribuindo-lhe um nível médio de importância significativo (3,6). Seguidamente, na segunda posição (3,5) aparecem os elementos críticos de sucesso "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*", "*Responsabilização pela Segurança da Informação*" e "*Política de Segurança da Informação*". O elemento "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)"* surge na quinta posição (3,2).

O gráfico (Gráfico 6.5) abaixo ilustra o acima mencionado.

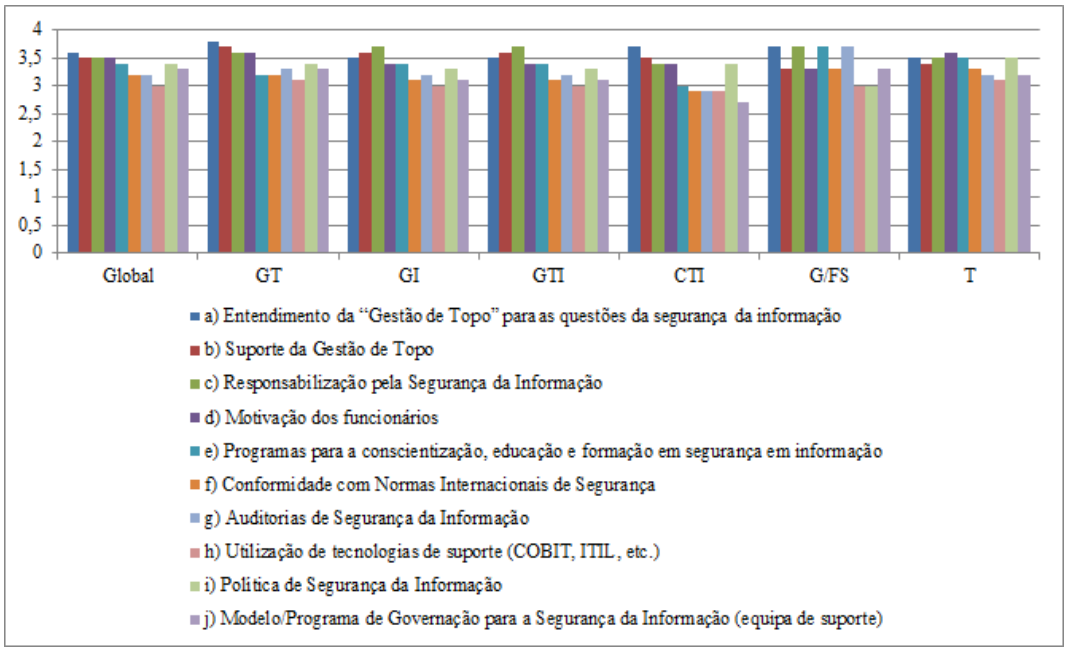


Gráfico 6.5- FCS/PP: Comparação pelo Tipo Função e Nível Médio de Importância

Resumindo e conforme tabela (Tabela 6.11) seguinte, globalmente, o elemento crítico de sucesso "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" é o que apresenta maior nível médio de importância. Todavia, os três elementos seguintes surgem com níveis médios de importância fortemente representativos, indiciando que a criticidade do sucesso na implementação/adopção dum Sistema de Gestão da Segurança da Informação assenta no "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*", no "*Suporte da Gestão de Topo*", na "*Responsabilização pela Segurança da Informação*" e na "*Motivação dos funcionários*" – todos estes elementos com um enfoque substancial no "Factor Humano".

Factores Críticos de Sucesso (Nível médio de importância - PP)	Global	GT	GI	GTI	CTI	G/FS	T
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,6	3,8	3,5	3,5	3,7	3,7	3,5
b) Suporte da Gestão de Topo	3,5	3,7	3,6	3,6	3,5	3,3	3,4
c) Responsabilização pela Segurança da Informação	3,5	3,6	3,7	3,7	3,4	3,7	3,5
d) Motivação dos funcionários	3,5	3,6	3,4	3,4	3,4	3,3	3,6
e) Programas para a conscientização, educação e formação em segurança em informação	3,4	3,2	3,4	3,4	3	3,7	3,5
f) Conformidade com Normas Internacionais de Segurança	3,2	3,2	3,1	3,1	2,9	3,3	3,3
g) Auditorias de Segurança da Informação	3,2	3,3	3,2	3,2	2,9	3,7	3,2
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	3	3,1	3,0	3,0	2,9	3	3,1
i) Política de Segurança da Informação	3,4	3,4	3,3	3,3	3,4	3	3,5
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,3	3,3	3,1	3,1	2,7	3,3	3,2
Legenda							
Posição	1ª	2ª	3ª	4ª	5ª	6ª	

Tabela 6.11- FCS/PP: Posicionamento dos elementos por Tipo de Função

6.2.2 – Perspectiva do Próprio vs Mapeamento ISACA

De seguida, retomando o referencial do discurso e, de acordo com o mostrado na figura (Figura 6.14) seguinte, surge a análise comparativa da perspectiva do próprio com o mapeamento ISACA [141] conforme referida no ponto 4.2 deste documento e tendo em conta os resultados dos valores dos níveis médios de importância encontrados para os elementos considerados na caracterização dos Factores Críticos de Sucesso.

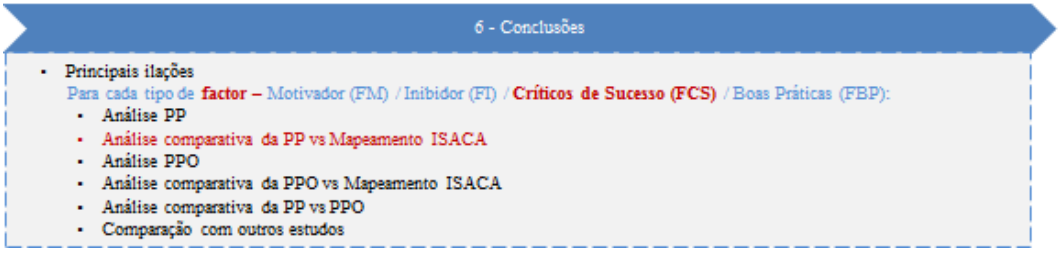


Figura 6.14- Modelo das Conclusões – FCS/PP vs Mapeamento ISACA

Assim, verifica-se que, globalmente, os respondentes focam a sua preferência em elementos críticos de sucesso relacionados com os pilares de resultados – "*Gestão de Desempenho*" e "*Alinhamento Estratégico*", indicando que a criticidade para a adopção/implementação do SGSI está centrada no "Factor Humano".

De facto, os elementos críticos de sucesso que agrupam maiores níveis médios de importância - "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*", "*Suporte*

da Gestão de Topo", "*Responsabilização pela Segurança da Informação*" e "*Motivação dos funcionários*" - mostram-se carregados de um "cariz humano" no enfoque do sucesso no compromisso da Segurança da Informação.

Contudo, de realçar que os elementos críticos de sucesso "*Política de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" atingem níveis médios de importância inferiores, manifestando-se níveis de baixa maturidade em matéria de Segurança da Informação.

A tabela (Tabela 6.12) seguinte resume o acima mencionado.

Factores Críticos de Sucesso (Nível médio de importância - PP)	Mapeamento ISACA	Global			GT			GI			GTI			CTI			G/FS			T		
		NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	Alinhamento Estratégico	3,6	3,45	2ª	3,8	3,55	2ª	3,5	3,38	2ª	3,5	3,38	2ª	3,7	3,33	2ª	3,7	3,33	3ª	3,5	3,40	2ª
b) Suporte da Gestão de Topo	Alinhamento Estratégico	3,5			3,7			3,6			3,6			3,5			3,3			3,4		
i) Política de Segurança da Informação	Alinhamento Estratégico	3,4			3,4			3,3			3,3			3,4			3			3,5		
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	Alinhamento Estratégico	3,3			3,3			3,1			3,1			2,7			3,3			3,2		
c) Responsabilização pela Segurança da Informação	Gestão de Desempenho	3,5	3,50	1ª	3,6	3,60	1ª	3,7	3,55	1ª	3,7	3,55	1ª	3,4	3,40	1ª	3,7	3,50	2ª	3,5	3,55	1ª
d) Motivação dos funcionários	Gestão de Desempenho	3,5			3,6			3,4			3,4			3,4			3,3			3,6		
e) Programas para a conscientização, educação e formação em segurança em informação	Gestão de Risco	3,4	3,30	3ª	3,2	3,20	4ª	3,4	3,25	3ª	3,4	3,25	3ª	3	2,95	3ª	3,7	3,50	2ª	3,5	3,40	2ª
f) Conformidade com Normas Internacionais de Segurança	Gestão de Risco	3,2			3,2			3,1			3,1			2,9			3,3			3,3		
g) Auditorias de Segurança da Informação	Garantia da integração de Processo	3,2	3,20	4ª	3,3	3,30	3ª	3,2	3,20	4ª	3,2	3,20	4ª	2,9	2,90	4ª	3,7	3,70	1ª	3,2	3,20	3ª
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	Gestão de Recursos	3,3	3,30	3ª	3,1	3,10	5ª	3	3,00	5ª	3	3,00	5ª	2,9	2,90	4ª	3	3,00	4ª	3,1	3,10	4ª

Tabela 6.12- FCS/PP: Comparação pelo Mapeamento ISACA

6.2.3 – Perspectiva do Próprio face à Organização

Neste ponto revela-se a perspectiva do próprio face à organização no eixo do estudo referente aos Factores Críticos de Sucesso conforme se indica na figura seguinte (Figura 6.15).

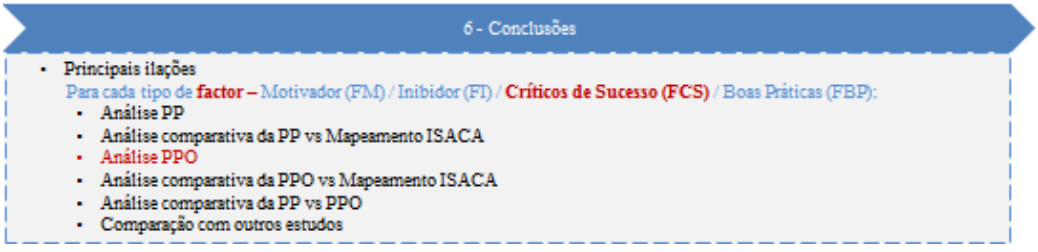


Figura 6.15- Modelo das Conclusões – FCS/PPO

Nesta perspectiva, os Factores Críticos de Sucesso que, globalmente apresentam maior nível médio de importância na implementação/adopção dum Sistema de Gestão da Segurança da Informação são: "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" (3,6), seguido dos elementos "*Suporte da Gestão de Topo*", "*Responsabilização*

pela Segurança da Informação" com o mesmo nível médio de importância (3,5), surgindo, nesta perspectiva, o elemento "*Motivação dos funcionários*" na terceira posição (3,4).

De realçar, ainda, que os elementos críticos de sucesso "*Programas para a conscientização, educação e formação em segurança em informação*" e "*Política de Segurança da Informação*" surgem na quarta posição (3,3) e o elemento "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" aparece na quinta posição com o valor de (3,2) para o nível médio de importância.

Deste modo, continua a verificar-se que o enfoque dos Factores Críticos de Sucesso destaca-se em elementos relacionados com o "Factor Humano" e/ou com elementos ligados ao "*Alinhamento Estratégico*" da Governação Organizacional.

Porém, nesta perspectiva do próprio face à organização, o Gestor de Topo e o Consultor das TI seguem a tendência global e consideram, como factor crítico de sucesso de maior nível médio de importância, o elemento "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" (3,6; 3,7) vindo logo depois o elemento "*Suporte da Gestão de Topo*" (3,5; 3,5). Contudo, o Gestor de Topo aponta, também, na segunda posição, o elemento "*Motivação dos funcionários*", enquanto o Consultor das TI revela este elemento na terceira posição. Ainda, na terceira posição, estas classes, apontam o elemento "*Responsabilização pela Segurança da Informação*" com o mesmo nível médio de importância (3,4).

Relativamente aos elementos "*Política de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)"*, o Gestor de Topo remete-os, respectivamente, para a quarta (3,3) e quinta (3,2) posições, enquanto que o Consultor das TI assinala-as, respectivamente, na quarta (3,3) e na sexta (3,0) posição.

Já o Gestor Intermédio e o Gestor das TI emergem com opiniões idênticas e indicam, como principais Factores Críticos de Sucesso, os seguintes elementos: "*Responsabilização pela Segurança da Informação*" (3,6), apresentando-se os elementos "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" e "*Suporte da Gestão de Topo*" na segunda posição com o valor (3,5) para o nível médio de importância. Todavia, o elemento "*Motivação dos funcionários*" que se encontra fortemente relacionado com o "Factor Humano" surge na terceira posição do nível médio de importância (3,3), subindo uma posição face às perspectivas dos próprios. Já os elementos relacionados com o "*Alinhamento Estratégico*" da Governação Organizacional – "*Política de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)"* aparecem, igualmente pontuados, na quarta posição (3,2), subindo, do mesmo modo um nível face às perspectivas dos próprios.

Para o Gestor/Funcionário da Segurança obteve-se uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). No entanto, o elemento "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" obtém um nível médio de importância em igualdade (3,7) com os seguintes elementos críticos de sucesso: "*Suporte da Gestão de Topo*", "*Responsabilização pela Segurança da Informação*" e "*Auditorias de Segurança da Informação*". Os elementos "*Motivação dos funcionários*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" mostram-se na segunda posição (3,3), enquanto que o elemento "*Política de Segurança da Informação*" é classificado na última posição (3,0).

Por último, o Trabalhador aponta na primeira posição o elemento crítico de sucesso "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" (3,5) embora, na perspectiva do próprio, o elemento "*Motivação dos funcionários*" - fortemente relacionado com o "Factor Humano" - tivesse obtido a primeira posição do nível médio de importância (3,6). Esta classe posiciona todos os outros elementos na segunda posição (3,4) com excepção, respectivamente, dos elementos "*Auditorias de Segurança da Informação*" e "*Utilização de tecnologias de suporte (COBIT, ITIL, etc.)*" que se encontram na terceira (3,2) e quarta (3,1) posições.

O gráfico (Gráfico 6.6) seguinte ilustra o acima mencionado.

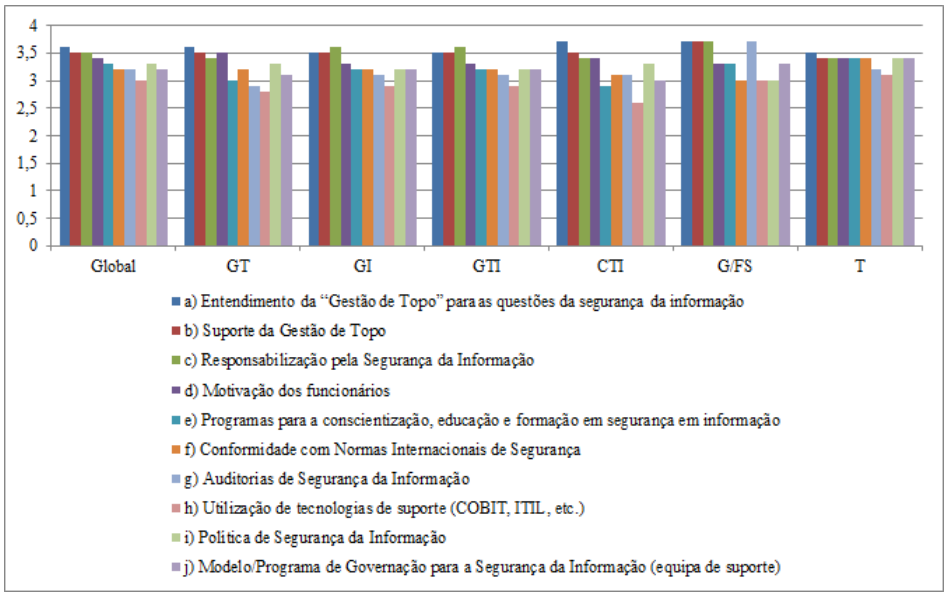


Gráfico 6.6-FCS/PPO: Comparação pelo Tipo Função e Nível Médio de Importância

Resumindo e conforme tabela (Tabela 6.13) abaixo, globalmente, o elemento crítico de sucesso "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" é o que apresenta maior nível médio de importância. Todavia, os três elementos seguintes surgem com

níveis médios de importância fortemente representativos, indiciando que, também nesta perspectiva – do próprio face à organização, os respondentes revelam que a criticidade do sucesso na implementação/adopção dum SGSI assenta no "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*", "*Suporte da Gestão de Topo*", *"Responsabilização pela Segurança da Informação" e "Motivação dos funcionários"* – todos estes elementos com um enfoque substancial no "Factor Humano".

Factores Críticos de Sucesso (Nivel médio de importância - PPO)	Global	GT	GI	GTI	CTI	G/FS	T
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,6	3,6	3,5	3,5	3,7	3,7	3,5
b) Suporte da Gestão de Topo	3,5	3,5	3,5	3,5	3,5	3,7	3,4
c) Responsabilização pela Segurança da Informação	3,5	3,4	3,6	3,6	3,4	3,7	3,4
d) Motivação dos funcionários	3,4	3,5	3,3	3,3	3,4	3,3	3,4
e) Programas para a conscientização, educação e formação em segurança em informação	3,3	3,0	3,2	3,2	2,9	3,3	3,4
f) Conformidade com Normas Internacionais de Segurança	3,2	3,2	3,2	3,2	3,1	3	3,4
g) Auditorias de Segurança da Informação	3,2	2,9	3,1	3,1	3,1	3,7	3,2
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	3	2,8	2,9	2,9	2,6	3	3,1
i) Política de Segurança da Informação	3,3	3,3	3,2	3,2	3,3	3	3,4
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,2	3,1	3,2	3,2	3	3,3	3,4
Legenda							
Posição	1ª	2ª	3ª	4ª	5ª	6ª	

Tabela 6.13- FCS/PPO: Posicionamento dos elementos por Tipo de Função

6.2.4 – Perspectiva do Próprio face à Organização vs Mapeamento ISACA

Seguidamente, conforme a figura (Figura 6.16) indica, apresenta-se a análise comparativa da perspectiva do próprio face à organização, tendo em conta os resultados dos valores dos níveis médios de importância encontrados para os elementos considerados na caracterização dos Factores Críticos de Sucesso e, enquadrando-os no referencial do ISACA [142] que refere: «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*» e representada no ponto 4.2 deste documento.

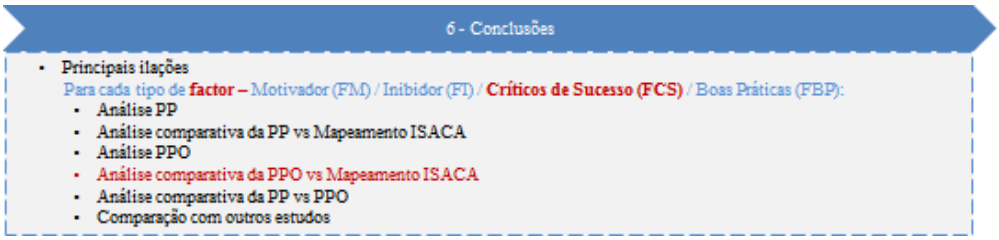


Figura 6.16- Modelo das Conclusões – FCS/Análise PPO vs Mapeamento ISACA

Assim, verifica-se que, globalmente, os respondentes focam a sua preferência em elementos relacionados com os pilares de resultados – "*Gestão de Desempenho*" e "*Alinhamento Estratégico*", indicando que a criticidade para a adopção/implementação do SGSI está centrada no "Factor Humano".

De facto, também nesta perspectiva – do próprio face à organização, os elementos que agrupam maiores níveis médios de importância - "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*", "*Suporte da Gestão de Topo*", "*Responsabilização pela Segurança da Informação*" *e* "*Motivação dos funcionários*" - mostram-se carregados de um "cariz humano" no enfoque do sucesso no compromisso da Governação da Segurança da Informação.

Contudo, de realçar que os elementos críticos de sucesso "*Política de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" atingem níveis médios de importância inferiores, respectivamente (3,3; 3,1), manifestando-se níveis de baixa maturidade em matéria da Governação da Segurança da Informação.

A tabela (Tabela 6.14) seguinte resume o acima mencionado.

Factores Críticos de Sucesso (Nível médio de importância - PPO)	Mapeamento ISACA	Global			GT			GI			GTI			CTI			G/FS			T		
		NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	Alinhamento Estratégico	3,6	3,40	2ª	3,6	3,38	2ª	3,5	3,35	2ª	3,5	3,35	2ª	3,7	3,38	2ª	3,7	3,43	3ª	3,5	3,43	1ª
b) Suporte da Gestão de Topo	Alinhamento Estratégico	3,5			3,5			3,5			3,5			3,5			3,7			3,4		
i) Política de Segurança da Informação	Alinhamento Estratégico	3,3			3,3			3,2			3,2			3,3			3			3,4		
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	Alinhamento Estratégico	3,2			3,1			3,2			3,2			3			3,3			3,4		
c) Responsabilização pela Segurança da Informação	Gestão de Desempenho	3,5	3,45	1ª	3,4	3,45	1ª	3,6	3,45	1ª	3,6	3,45	1ª	3,4	3,40	1ª	3,7	3,50	2ª	3,4	3,40	2ª
d) Motivação dos funcionários	Gestão de Desempenho	3,4			3,5			3,3			3,3			3,4			3,3			3,4		
e) Programas para a conscientização, educação e formação em segurança em informação	Gestão de Risco	3,3	3,25	3ª	3	3,10	3ª	3,2	3,20	3ª	3,2	3,20	3ª	2,9	3,00	3ª	3,3	3,15	4ª	3,4	3,40	2ª
f) Conformidade com Normas Internacionais de Segurança	Gestão de Risco	3,2			3,2			3,2			3,2			3,1			3			3,4		
g) Auditorias de Segurança da Informação	Garantia da integração de Processo	3,2	3,20	4ª	2,9	2,90	4ª	3,1	3,10	4ª	3,1	3,10	4ª	3,1	3,10	4ª	3,7	3,70	1ª	3,2	3,20	3ª
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	Gestão de Recursos	3	3,00	3ª	2,8	2,80	5ª	2,9	2,90	5ª	2,9	2,90	5ª	2,6	2,60	5ª	3	3,00	5ª	3,1	3,10	4ª

Tabela 6.14- FCS/PPO: Comparação pelo Mapeamento ISACA

6.2.5 - Perspectiva do Próprio vs Perspectiva do Próprio face à Organização

Este estudo também permitiu, conforme indicado na figura (Figura 6.17), identificar os desvios existentes entre as duas perspectivas do próprio (PP) e do próprio face à organização (PPO).

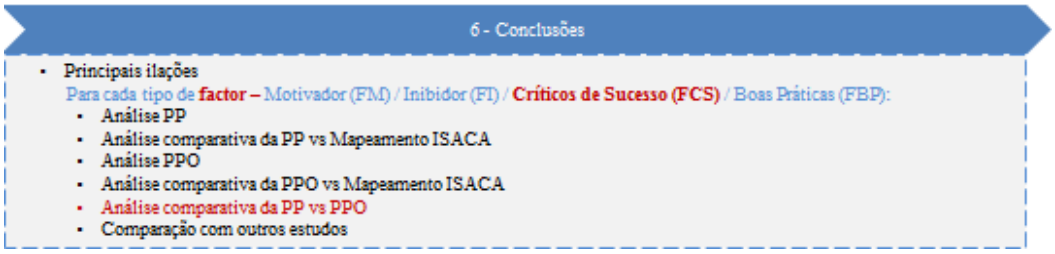


Figura 6.17- Modelo das Conclusões – FCS/Análise Comparativa entre perspectivas PP vs PPO

Deste modo destacam-se os seguintes:

- Globalmente, os desvios entre as perspectivas aparecem em quatro dos dez elementos críticos de sucesso, a saber: "*Motivação dos funcionários*", "*Programas para a conscientização, educação e formação em segurança em informação*", "*Política de Segurança da Informação*" e "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)*" revelando-se que, para todos eles, na perspectiva do próprio, os respondentes atribuem maior nível médio de importância do que quando mencionada a perspectiva do próprio face à organização.

- Todos os elementos considerados como Factores Críticos de Sucesso na implementação/adopção dum Sistema de Gestão da Segurança da Informação (SGSI) e relacionados com o pilar de resultados – "*Alinhamento Estratégico*" assinalam, por todos os tipos de respondentes, desvios entre as duas perspectivas, com excepção do elemento "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*". Neste, apenas o Gestor de Topo, expõe uma divergência positiva de (0,2), ou seja, a perspectiva do próprio adquire um maior nível médio de importância do que a perspectiva do próprio face à organização. Porém, para o elemento "*Política de Segurança da Informação*" verifica-se que os desvios apresentam igualmente o mesmo valor positivo (0,1) por todos os tipos de respondentes. Já o elemento "*Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)"* revela, para todos os tipos de respondentes, desvios entre as duas perspectivas. Todavia, apenas o Gestor de Topo considera, na perspectiva do próprio, maior nível médio de importância do que o que indica na perspectiva do próprio face à organização. Os outros tipos de respondentes mencionam o contrário: o nível médio de

importância adquire maior valor quando referida a perspectiva do próprio face à organização.

- O Gestor de Topo revela, para todos os elementos críticos de sucesso considerados, com excepção do elemento "*Conformidade com Normas Internacionais de Segurança*", desvios positivos entre as duas perspectivas, mostrando que, na perspectiva do próprio, o nível médio de importância é maior do que quando menciona a sua perspectiva face à organização. Aliás, para aquele elemento, os Gestores Intermédios, Gestores e Consultores das TI e Trabalhadores apresentam desvios negativos, indicando maiores níveis médios de importância quando citam as suas perspectivas face à organização. Contudo, o Gestor/Funcionário da Segurança manifesta um maior valor do nível médio de importância na perspectiva do próprio, surgindo um desvio significativo (0,3).
- Os elementos "*Auditorias da Segurança da Informação*" e "*Programas para a conscientização, educação e formação em segurança em informação*" são os que surgem com maior valor do desvio (0,4) entre as duas perspectivas – do próprio e do próprio face à organização, verificando que os mesmos são assinalados, respectivamente, pelo Gestor de Topo e pelo Gestor/Funcionário da Segurança.
- Relativamente aos elementos considerados críticos de sucesso e relacionados com o "Factor Humano" - "*Responsabilização pela Segurança da Informação*", "*Motivação dos funcionários*" e "*Programas para a conscientização, educação e formação em segurança em informação*" contam níveis médios de importância significativos, mas também apresentam desvios, sempre positivos (perspectiva do próprio agrupa níveis médios de importância maiores do que os indicados na perspectiva do próprio face à organização), entre as duas perspectivas, nomeadamente, pelos Gestores de Topo, Gestores Intermédios, Gestores das TI e Trabalhadores, revelando-se o "Factor Humano" como uma pedra basilar da criticidade na implementação/adopção dum SGSI. Verifica-se, ainda, que o elemento "*Programas para a conscientização, educação e formação em segurança em informação*" reúne desvios, de todos os tipos de respondentes, entre as duas perspectivas.

A tabela (Tabela 6.15) seguinte resume o acima mencionado.

Factores Criticos de Sucesso (Nível médio de importância - Desvios entre as PP e PPO)	Global	Global	Desvio	GT	GT	Desvio	GI	GI	Desvio	GTI	GTI	Desvio	CTI	CTI	Desvio	G/FS	G/FS	Desvio	T	T	Desvio
	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	3,6	3,6	0,0	3,8	3,6	0,2	3,5	3,5	0,0	3,5	3,5	0,0	3,7	3,7	0,0	3,7	3,7	0,0	3,5	3,5	0,0
b) Suporte da Gestão de Topo	3,5	3,5	0,0	3,7	3,5	0,2	3,6	3,5	0,1	3,6	3,5	0,1	3,5	3,5	0,0	3,3	3,7	-0,4	3,4	3,4	0,0
c) Responsabilização pela Segurança da Informação	3,5	3,5	0,0	3,6	3,4	0,2	3,7	3,6	0,1	3,7	3,6	0,1	3,4	3,4	0,0	3,7	3,7	0,0	3,5	3,4	0,1
d) Motivação dos funcionários	3,5	3,4	0,1	3,6	3,5	0,1	3,4	3,3	0,1	3,4	3,3	0,1	3,4	3,4	0,0	3,3	3,3	0,0	3,6	3,4	0,2
e) Programas para a conscientização, educação e formação em segurança em informação	3,4	3,3	0,1	3,2	3,0	0,2	3,4	3,2	0,2	3,4	3,2	0,2	3,0	2,9	0,1	3,7	3,3	0,4	3,5	3,4	0,1
f) Conformidade com Normas Internacionais de Segurança	3,2	3,2	0,0	3,2	3,2	0,0	3,1	3,2	-0,1	3,1	3,2	-0,1	2,9	3,1	-0,2	3,3	3,0	0,3	3,3	3,4	-0,1
g) Auditorias de Segurança da Informação	3,2	3,2	0,0	3,3	2,9	0,4	3,2	3,1	0,1	3,2	3,1	0,1	2,9	3,1	-0,2	3,7	3,7	0,0	3,2	3,2	0,0
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	3,0	3,0	0,0	3,1	2,8	0,3	3,0	2,9	0,1	3,0	2,9	0,1	2,9	2,6	0,3	3,0	3,0	0,0	3,1	3,1	0,0
i) Politica de Segurança da Informação	3,4	3,3	0,1	3,4	3,3	0,1	3,3	3,2	0,1	3,3	3,2	0,1	3,4	3,3	0,1	3,0	3,0	0,0	3,5	3,4	0,1
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	3,3	3,2	0,1	3,3	3,1	0,2	3,1	3,2	-0,1	3,1	3,2	-0,1	2,7	3,0	-0,3	3,3	3,3	0	3,2	3,4	-0,2

Tabela 6.15- FCS/Desvios PP-PPO: Comparação pelo Tipo Função e Nível Médio de Importância

6.2.6 - Comparação com outros estudos

A comparação deste vector de análise – Factores Críticos de Sucesso na implementação/adopção dum Sistema de Gestão da Segurança da Informação, com outros estudos revela-se significativa, pelo que, neste ponto e de acordo com o indicado na figura (Figura 6.18) seguinte, expõem-se os resultados obtidos.

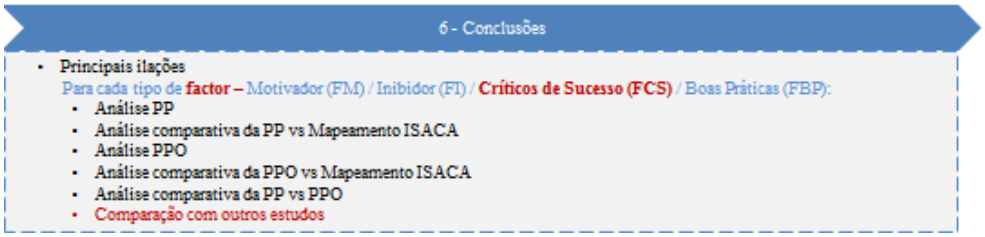


Figura 6.18- Modelo das Conclusões – FCS/Comparação co outros estudos

De facto, num estudo realizado, em Portugal, por Santos, Luís [143] sobre "Factores de Sucesso na Gestão de Segurança da Informação nas Empresas Portuguesas" concluiu-se que «*o factor ´Responsabilidades em Segurança da Informação´ foi o factor mais importante (3,69) no sucesso da Gestão da Segurança da Informação e o factor ´Aconselhamento Externo de Serviços em Segurança da Informação´ foi o de menor importância (2,69) comparados com os outros cinco factores: ´Suporte da Gestão de Topo´ (3,45), ´Politica de Segurança da Informação´ (3,38), ´Motivação dos Funcionários´ (3,45), ´Programas de Sensibilização e Formação´ (3,53) e ´Conformidade com Normas Internacionais de Segurança´ (3,35)*».

Comparando os resultados atrás mencionados com o presente estudo realizado no sector das Águas/Saneamento em Portugal, observa-se que o elemento "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*" foi o mais mencionado, obtendo, globalmente, o valor de (3,6) para o nível médio de importância – quer na perspectiva do próprio, quer na perspectiva do próprio face à organização, Contudo, o elemento "*Responsabilização pela Segurança da Informação*" posiciona-se em segundo lugar (3,5), também nas duas perspectivas.

De facto, no gráfico (Gráfico 6.7) seguinte podemos observar a semelhança/desvios nos resultados obtidos pelos dois estudos, verificando-se que o "Factor Humano" evidencia-se de forma significativa.

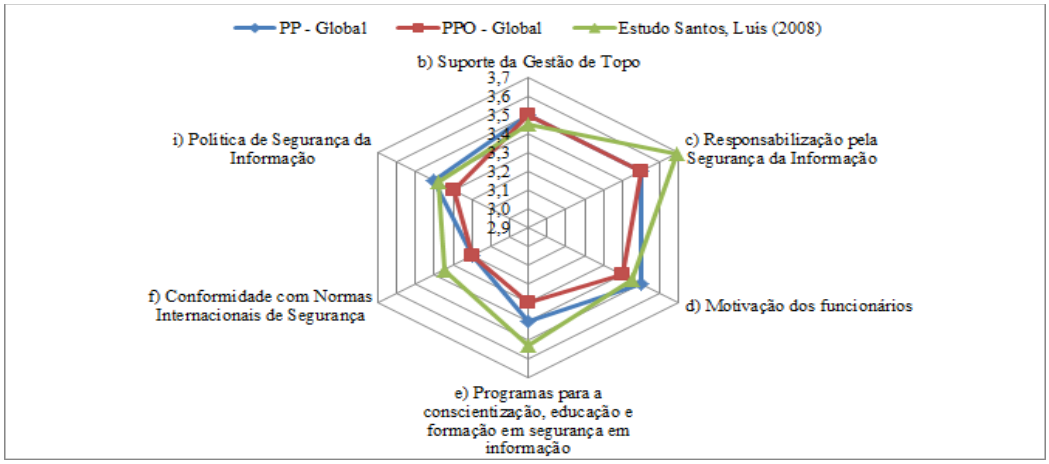


Gráfico 6.7- Factores Críticos de Sucesso: Comparação com o Estudo realizado por *Santos, Luís* (2008)

Na verdade, o referido estudo, infere que «*na generalidade as empresas portuguesas encontram-se numa maturidade inicial ou em desenvolvimento de uma cultura de Segurança da Informação e fortemente associada a processos tecnológicos, verificando, no entanto, alguma maturidade nas empresas dos sectores financeiros e de telecomunicações*». Acentua que «*é sentida a necessidade de desenvolver uma consciencialização em Segurança da Informação, através de políticas governamentais, de carácter obrigatório para os organismos públicos e recomendada para o sector privado de forma a sensibilizar a gestão das empresas portuguesas nesta matéria*».

No presente estudo, o elemento crítico de sucesso "*Motivação dos funcionários*" aparece, globalmente, na segunda posição, na perspectiva do próprio e na terceira posição, na perspectiva do próprio face à organização, revelando a importância que os respondentes dão a este factor.

A mesma pesquisa indica, ainda, que as «*empresas portuguesas demonstram possuírem menor maturidade na classificação dos factores essenciais ao sucesso da Gestão da Segurança da Informação do que as empresas da Finlândia e da Jordânia*», tendo em conta os níveis médios de importância obtidos nos elementos "*Suporte da Gestão de Topo*" e "*Política de Segurança da Informação*".

Assim, no presente estudo, os elementos "*Suporte da Gestão de Topo*" e "*Política de Segurança da Informação*" surgem com níveis médios de importância ligeiramente superiores aos apresentados no referido estudo, levando, eventualmente a considerar que o sector das "Águas e

Saneamento em Portugal" poderá apresentar uma maturidade ligeiramente superior na classificação dos factores indispensáveis na Governação da Segurança da Informação.

6.3- Factores de Boas Práticas (FBP)

Seguindo o referencial metodológico de apresentação dos resultados conforme ilustrado na figura (Figura 6.19), neste ponto revelam-se as observações referentes ao outro vector de análise considerado neste estudo - o das Boas Práticas.

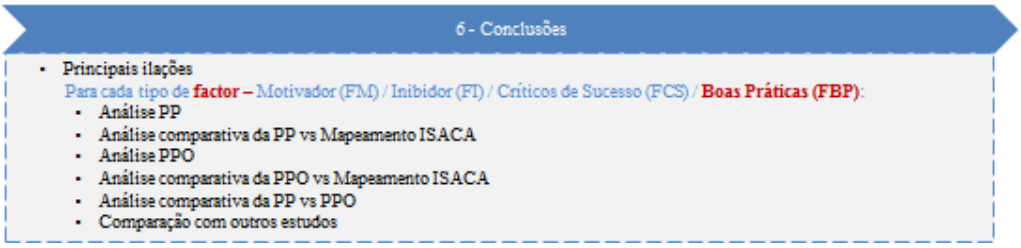


Figura 6.19- Modelo das Conclusões – FBP

6.3.1 - Perspectiva do Próprio

Neste contexto, inicia-se esta exposição pela perspectiva do próprio consoante o mencionado na figura (Figura 6.20) abaixo.

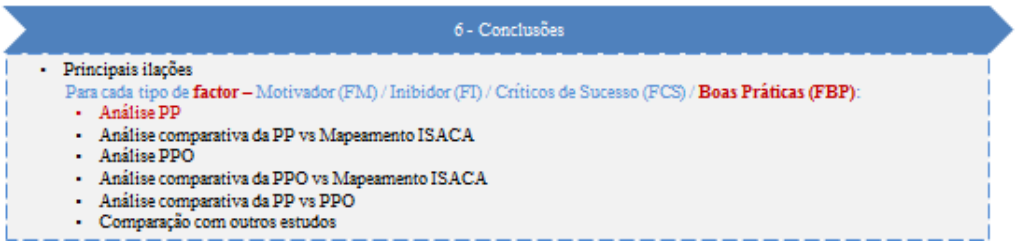


Figura 6.20- Modelo das Conclusões – FBP/Análise da PP

Assim, na sua visão, os Factores de Boas Práticas que, globalmente apresentam maior nível médio de importância na implementação/adopção dum Sistema de Gestão da Segurança da Informação (SGSI) são: "*A minha senha de acesso não a partilho com ninguém*" (3,7), seguido dos elementos "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*" e "*Deve existir uma Política de Segurança da Informação*" com o mesmo nível médio de importância (3,4). De realçar, ainda, que os elementos "*Devem existir programas para a conscientização, educação e formação em segurança*", "*Devem existir auditorias de Segurança da Informação*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" surgem na terceira posição (3,2).

Deste modo, verifica-se que o enfoque dos Factores de Boas Práticas destaca-se em elementos relacionados com o "Factor Humano" e/ou com elementos ligados ao "*Alinhamento Estratégico*" da Governação Organizacional.

Porém, nesta perspectiva do próprio, o Gestor de Topo não segue a tendência global e indica nas três primeiras posições os seguintes elementos: "*Deve existir Modelo/Programa de Governação para a Segurança da Informação"* (3,8), "*Devem existir auditorias de Segurança da Informação*" e "*Deve existir uma Política de Segurança da Informação*" com igualdade de pontuação (3,6), demonstrando um nível maduro de conhecimento sobre as boas práticas da governação da segurança da informação.

Todavia, todas as outras classes seguem a tendência global, indicando para a primeira posição do nível médio de importância, o elemento "*A minha senha de acesso não a partilho com ninguém*".

Contudo, o Gestor Intermédio assinala na segunda posição os três elementos seguintes: "*Devem existir programas para a conscientização, educação e formação em segurança*", "*Devem existir auditorias de Segurança da Informação*" e "*Deve existir uma Política de Segurança da Informação*" com igualdade de pontuação (3,3). O elemento "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" surge na quarta posição (3,1).

Já para o Gestor das TI e o Consultor das TI o elemento "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC"* aparece classificado na segunda posição (3,6; 3,7). De realçar que os elementos "*Deve existir uma Política de Segurança da Informação*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação"* declaram-se, respectivamente, na terceira (3,5; 3,4) e sexta/quinta (3,1; 3,0) posição, denunciando uma cultura de segurança da informação focada em questões técnicas e mostrando, também, um distanciamento face à perspectiva do Gestor de Topo, revelando um nível de maturidade inicial de conhecimento sobre as boas práticas da governação da segurança da informação.

Para o Gestor/Funcionário da Segurança obteve-se uma percentagem de resposta muito pouco significativa (2,48% - 3 respondentes). No entanto, esta classe segue a tendência global no posicionamento dos dois primeiros elementos, revelando-se também o enfoque da cultura da segurança da informação nas questões técnicas, surgindo os elementos "*Deve existir uma Política de Segurança da Informação*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação"*, respectivamente, na quarta (2,7) e terceira (3,0) posição.

Por último, o Trabalhador aponta na segunda posição o elemento "*Deve existir uma Política de Segurança da Informação*" (3,4) e o elemento "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" surge na quarta posição (3,2).

O gráfico (Gráfico 6.8) abaixo ilustra o acima mencionado.

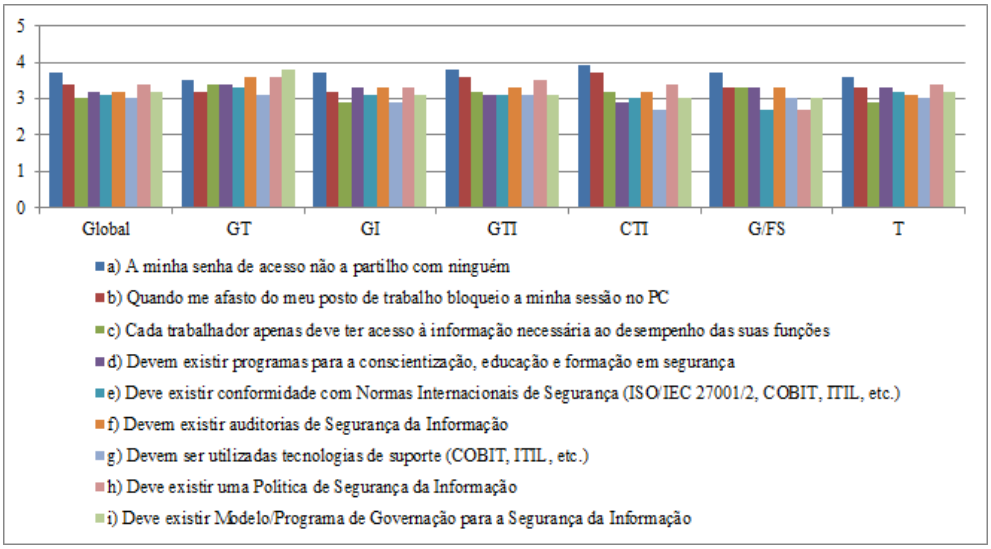


Gráfico 6.8- FBP/PP: Comparação pelo Tipo Função e Nível Médio de Importância

Resumindo e conforme tabela (Tabela 6.16) seguinte, globalmente, o elemento "*A minha senha de acesso não a partilho com ninguém*" é o que apresenta maior nível médio de importância (3,9). Exceptua-se a esta tendência global, o Gestor de Topo que indica, nas três primeiras posições, elementos relacionados com as boas práticas da governação da segurança da informação demonstrando um nível maduro de conhecimento sobre as mesmas. Por outro lado, o Gestor das TI e o Consultor das TI, seguindo a tendência global, mostram um distanciamento face à perspectiva do Gestor de Topo, denunciando uma cultura de segurança da informação focada em questões técnicas, revelando, assim, um nível de maturidade inicial de conhecimento sobre as boas práticas da governação da segurança da informação.

Factores de Boas Práticas (Nível médio de importância - PP)	Global	GT	GI	GTI	CTI	G/FS	T
a) A minha senha de acesso não a partilho com ninguém	3,7	3,5	3,7	3,8	3,9	3,7	3,6
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	3,4	3,2	3,2	3,6	3,7	3,3	3,3
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	3	3,4	2,9	3,2	3,2	3,3	2,9
d) Devem existir programas para a conscientização, educação e formação em segurança	3,2	3,4	3,3	3,1	2,9	3,3	3,3
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	3,1	3,3	3,1	3,1	3	2,7	3,2
f) Devem existir auditorias de Segurança da Informação	3,2	3,6	3,3	3,3	3,2	3,3	3,1
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	3	3,1	2,9	3,1	2,7	3	3
h) Deve existir uma Política de Segurança da Informação	3,4	3,6	3,3	3,5	3,4	2,7	3,4
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,2	3,8	3,1	3,1	3	3	3,2
Legenda							
Posição	1ª	2ª	3ª	4ª	5ª	6ª	

Tabela 6.16- FBP/PP: Posicionamento dos elementos por Tipo de Função

6.3.2 - Perspectiva do Próprio vs Mapeamento ISACA

Neste ponto e, conforme indicado na figura (Figura 6.21), apresenta-se a análise dos resultados obtidos no vector das boas práticas, na perspectiva do próprio, enquadrando-a no mapeamento das orientações do ISACA [144] que refere: «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*» e representada no ponto 4.2 deste documento.

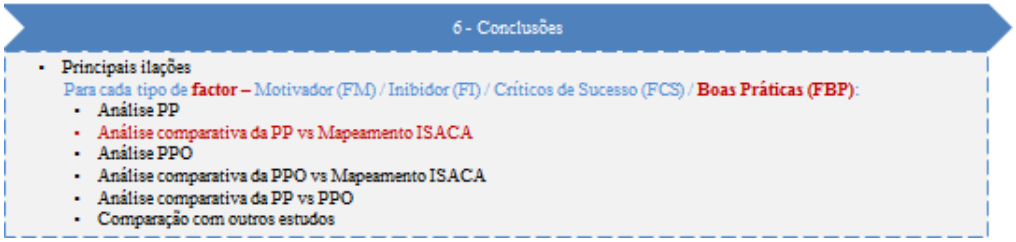


Figura 6.21- Modelo das Conclusões – FBP/PP vs Mapeamento ISACA

Assim, face aos resultados dos valores dos níveis médios de importância encontrados para os elementos considerados na caracterização dos Factores de Boas Práticas, verifica-se que, globalmente, o enfoque incide em elementos relacionados com o pilar de resultados – "*Gestão de Risco*". Porém, os elementos caracterizados no pilar de resultados – "*Alinhamento Estratégico*" surgem na segunda posição, conforme se pode visualizar na tabela (Tabela 6.17) seguinte.

Factores de Boas Práticas (Nível médio de importância - PP)	Mapeamento ISACA	Global			GT			GI			GTI			CTI			G/FS			T		
		NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição
a) A minha senha de acesso não a partilho com ninguém	Gestão de Risco	3,7			3,5			3,7			3,8			3,9			3,7			3,6		
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	Gestão de Risco	3,4			3,2			3,2			3,6			3,7			3,3			3,3		
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	Gestão de Risco	3	3,33	1ª	3,4	3,38	3ª	2,9	3,28	2ª	3,2	3,43	1ª	3,2	3,43	1ª	3,3	3,40	1ª	2,9	3,28	2ª
d) Devem existir programas para a conscientização, educação e formação em segurança	Gestão de Risco	3,2			3,4			3,3			3,1			2,9			3,3			3,3		
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	Gestão de Desempenho	3,1	3,10	4ª	3,3	3,30	4ª	3,1	3,10	4ª	3,1	3,10	5ª	3	3,00	3ª	2,7	2,70	5ª	3,2	3,20	3ª
f) Devem existir auditorias de Segurança da Informação	Garantia da integração de Processos	3,2	3,20	3ª	3,6	3,60	2ª	3,3	3,30	1ª	3,3	3,30	3ª	3,2	3,20	2ª	3,3	3,30	2ª	3,1	3,10	4ª
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	Gestão de Recursos	3	3,00	5ª	3,1	3,10	5ª	2,9	2,90	5ª	3,2	3,20	4ª	2,7	2,70	4ª	3	3,00	3ª	3	3,00	
h) Deve existir uma Política de Segurança da Informação	Alinhamento Estratégico	3,4	3,30	2ª	3,6	3,70	1ª	3,3	3,20	3ª	3,5	3,35	2ª	3,4	3,20	2ª	2,7	2,85	4ª	3,4	3,30	1ª
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	Alinhamento Estratégico	3,2			3,8			3,1			3,2			3			3			3,2		

Tabela 6.17- FBP/PP: Comparação pelo Mapeamento ISACA

6.3.3 - Perspectiva do Próprio face à Organização

Segue-se, neste item, a apresentação da perspectiva do próprio face à organização referente aos factores considerados de boas práticas, conforme se refere a figura (Figura 6.22) abaixo.

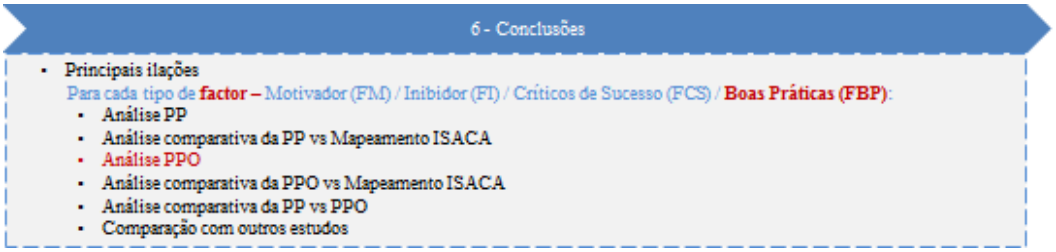


Figura 6.22- Modelo das Conclusões – FBP/Análise da PPO

Também, nesta visão e conforme se pode confirmar no gráfico (Gráfico 6.9) seguinte, o elemento considerado de boas práticas "*A minha senha de acesso não a partilho com ninguém*" obtém a primazia na categoria "Muito importante". Contudo, o Gestor de Topo coloca-o em segundo lugar dando preferência ao elemento "*Deve existir uma Política de Segurança da Informação*". Todavia, o Gestor Intermédio coloca este elemento em segundo lugar e os restantes tipos de respondentes classificam, este elemento, em terceiro lugar.

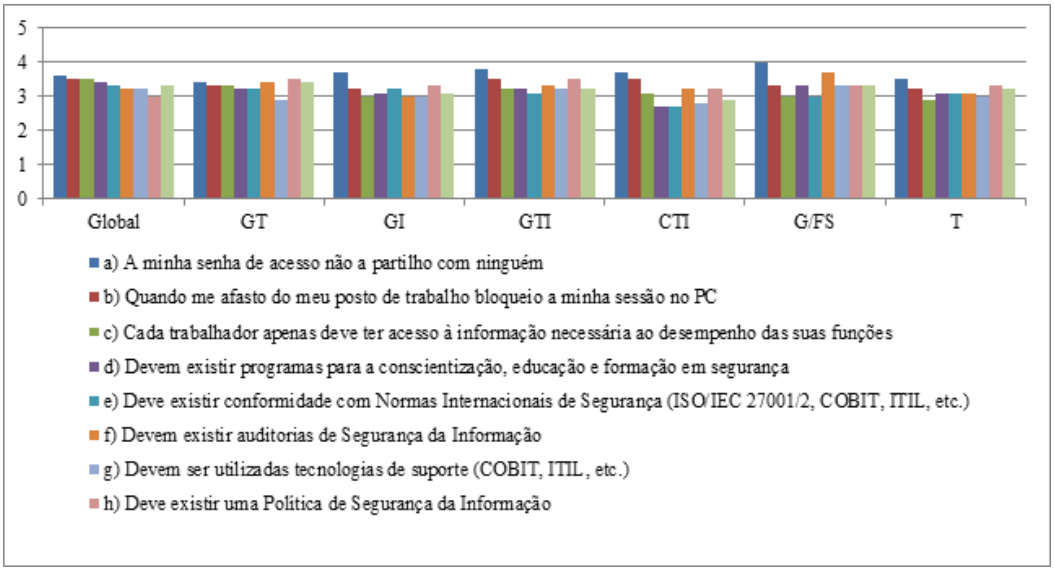


Gráfico 6.9- FBP/PPO: Comparação pelo Tipo Função e Nível Médio de Importância

A tabela (Tabela 6.18) reúne a comparação dos níveis médios de importância obtidos pelo tipo de função, mostrando que, também nesta perspectiva, se verifica uma cultura de segurança da informação focada em questões técnicas, revelando, assim, um nível de maturidade inicial de conhecimento sobre as boas práticas da governação da segurança da informação. Por outro lado, constata-se novamente o distanciamento do posicionamento dos Gestor das TI e Consultor das TI face ao Gestor de Topo.

Factores de Boas Práticas (Nível médio de importância - PPO)	Global	GT	GI	GTI	CTI	G/FS	T
a) A minha senha de acesso não a partilho com ninguém	3,6	3,4	3,7	3,8	3,7	4	3,5
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	3,5	3,3	3,2	3,5	3,5	3,3	3,2
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	3,5	3,3	3	3,2	3,1	3	2,9
d) Devem existir programas para a conscientização, educação e formação em segurança	3,4	3,2	3,1	3,2	2,7	3,3	3,1
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	3,3	3,2	3,2	3,1	2,7	3	3,1
f) Devem existir auditorias de Segurança da Informação	3,2	3,4	3	3,3	3,2	3,7	3,1
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	3,2	2,9	3	3,2	2,8	3,3	3
h) Deve existir uma Política de Segurança da Informação	3	3,5	3,3	3,5	3,2	3,3	3,3
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,3	3,4	3,1	3,2	2,9	3,3	3,2
Legenda							
Posição	1ª	2ª	3ª	4ª	5ª	6ª	

Tabela 6.18- FBP/PPO: Comparação pelo Tipo Função e Nível Médio de Importância

6.3.4 - Perspectiva do Próprio face à Organização vs Mapeamento ISACA

Neste ponto e, conforme indicado na figura (Figura 6.23), apresenta-se a análise dos resultados obtidos no vector das boas práticas, na perspectiva do próprio face à organização, enquadrando-a no mapeamento das orientações do ISACA [145] que refere: «*do ponto de vista da governação há seis principais resultados que o programa da segurança deverá trabalhar para atingir, a saber: 1) alinhamento estratégico; 2) gestão de risco; 3) entrega de valor; 4) gestão de recursos; 5) gestão de desempenho; e 6) garantia da integração de processos*» e representada no ponto 4.2 deste documento.

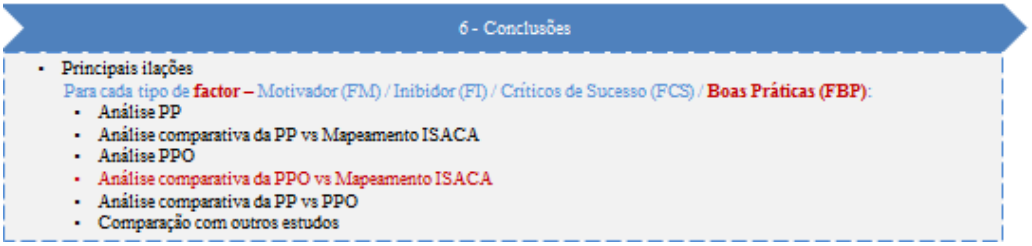


Figura 6.23- Modelo das Conclusões – FBP/PPO vs Mapeamento ISACA

Assim, também nesta visão do próprio face à organização, os resultados dos valores dos níveis médios de importância encontrados para os elementos considerados na caracterização dos Factores de Boas Práticas, mostram, globalmente, o enfoque em elementos relacionados com o pilar de resultados – "*Gestão de Risco*". Porém, os elementos caracterizados no pilar de resultados – "*Alinhamento Estratégico*" surgem na segunda posição, conforme se pode verificar na tabela (Tabela 6.19) seguinte, contribuindo para esta classificação o posicionamento dos Gestor de Topo e Trabalhador que, em média, atribuem maiores níveis médios de importância aos elementos que caracterizam aquele pilar.

Factores de Boas Práticas (Nível médio de importância - PPO)	Mapeamento ISACA	Global			GT			GI			GTI			CTI			G/FS			T		
		NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição	NMI	Valor Médio NMI	Posição
a) A minha senha de acesso não a partilho com ninguém	Gestão de Risco	3,6	3,50	1ª	3,4	3,30	3ª	3,7	3,25	1ª	3,8	3,43	1ª	3,7	3,25	1ª	4	3,40	2ª	3,5	3,18	2ª
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	Gestão de Risco	3,5			3,3			3,2			3,5			3,5			3,3			3,2		
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	Gestão de Risco	3,5			3,3			3			3,2			3,1			3			2,9		
d) Devem existir programas para a conscientização, educação e formação em segurança	Gestão de Risco	3,4			3,2			3,1			3,2			2,7			3,3			3,1		
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	Gestão de Desempenho	3,3	3,30	4ª	3,2	3,20	4ª	3,2	3,20	2ª	3,1	3,10	5ª	2,7	2,70	5ª	3	3,00	4ª	3,1	3,10	3ª
f) Devem existir auditorias de Segurança da Informação	Garantia da integração de Processos	3,2	3,20	3ª	3,4	3,40	2ª	3	3,00	3ª	3,3	3,30	3ª	3,2	3,20	2ª	3,7	3,70	1ª	3,1	3,10	3ª
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	Gestão de Recursos	3,2	3,20	5ª	2,9	2,90	5ª	3	3,00	3ª	3,2	3,20	4ª	2,8	2,80	4ª	3,3	3,30	3ª	3	3,00	4ª
h) Deve existir uma Política de Segurança da Informação	Alinhamento Estratégico	3	3,15	2ª	3,5	3,45	1ª	3,3	3,20	2ª	3,5	3,35	2ª	3,2	3,05	3ª	3,3	3,30	3ª	3,3	3,25	1ª
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	Alinhamento Estratégico	3,3			3,4			3,1			3,2			2,9			3,3			3,2		

Tabela 6.19- FBP/PPO: Comparação pelo Mapeamento ISACA

6.3.5 - Perspectiva do Próprio vs Perspectiva do Próprio face à Organização

Seguidamente e, conforme se visualiza na figura (Figura 6.24) seguinte, este item aborda a análise comparativa entre as duas perspectivas estudadas para o vector dos Factores de Boas Práticas.

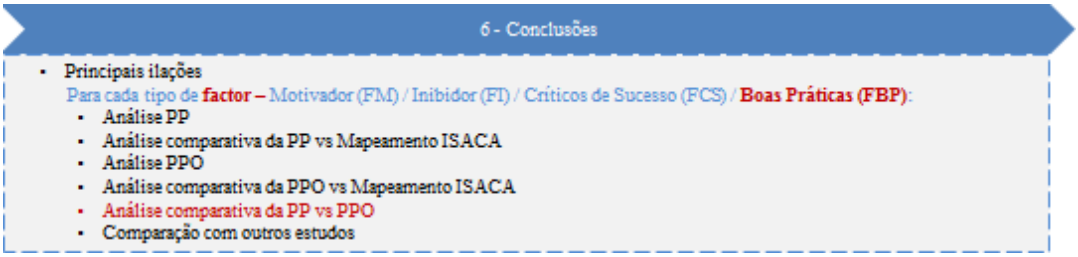


Figura 6.24- Modelo das Conclusões – FBP/Análise Comparativa entre perspectivas PP vs PPO

Assim, este estudo também permite identificar os desvios existentes entre as duas perspectivas (PP e PPO) tendo-se destacado, o seguinte:

- Globalmente, todos os elementos considerados como Factores de Boas Práticas apresentam desvios entre as duas perspectivas, com a excepção do elemento "*Devem existir Auditorias de Segurança da Informação*". Contudo, os elementos "*Deve existir uma Política de Segurança da Informação*" (0,4) e "*Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções*" (-0,5) surgem com os maiores desvios. Porém, no primeiro caso a perspectiva do próprio atribui-lhe maior nível médio de importância quando comparado com o nível médio de importância obtido na perspectiva do próprio face à organização. No segundo caso, verifica-se o contrário: a perspectiva do próprio face à organização atribui-lhe maior nível médio de importância.

- O Gestor de Topo mostra desvios em todos os elementos, evidenciando-se o elemento "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*". Este elemento aparece com um desvio significativo (0,4) entre as duas perspectivas, revelando que o Gestor de Topo atribui maior nível médio de importância a este elemento quando indica a sua perspectiva do que quando menciona a sua perspectiva face à organização.

- O Gestor das TI surge com desvios negativos para os elementos "*Devem existir programas para a conscientização, educação e formação em segurança*", "*Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)*" e "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*", indicando que

o nível médio de importância na perspectiva do próprio é menor, quando comparado com o valor do nível médio de importância na perspectiva do próprio face à organização, apresentando um valor absoluto de desvio igual (0,1).

- O elemento mais relacionado com o "Factor Humano" – "*Devem existir programas para a conscientização, educação e formação em segurança*" surge com desvios entre as duas perspectivas, globalmente e para todos os tipos de função com excepção do Gestor/Funcionário de Segurança.

A tabela (Tabela 6.20) seguinte ilustra o acima mencionado.

Factores de Boas Práticas (Nível médio de importância - Desvios entre as PP e PPO)	Global	Global	Desvio	GT	GT	Desvio	GI	GI	Desvio	GTI	GTI	Desvio	CTI	CTI	Desvio	G/FS	G/FS	Desvio	T	T	Desvio
	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO	PP	PPO	PP-PPO
a) A minha senha de acesso não a partilho com ninguém	3,7	3,6	0,1	3,5	3,4	0,1	3,7	3,7	0,0	3,8	3,8	0,0	3,9	3,7	0,2	3,7	4,0	-0,3	3,6	3,5	0,1
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	3,4	3,5	-0,1	3,2	3,3	-0,1	3,2	3,2	0,0	3,6	3,5	0,1	3,7	3,5	0,2	3,3	3,3	0,0	3,3	3,2	0,1
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	3,0	3,5	-0,5	3,4	3,3	0,1	2,9	3,0	-0,1	3,2	3,2	0,0	3,2	3,1	0,1	3,3	3,0	0,3	2,9	2,9	0,0
d) Devem existir programas para a conscientização, educação e formação em segurança	3,2	3,4	-0,2	3,4	3,2	0,2	3,3	3,1	0,2	3,1	3,2	-0,1	2,9	2,7	0,2	3,3	3,3	0,0	3,3	3,1	0,2
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	3,1	3,3	-0,2	3,3	3,2	0,1	3,1	3,2	-0,1	3,1	3,1	0,0	3,0	2,7	0,3	2,7	3,0	-0,3	3,2	3,1	0,1
f) Devem existir auditorias de Segurança da Informação	3,2	3,2	0,0	3,6	3,4	0,2	3,3	3,0	0,3	3,3	3,3	0,0	3,2	3,2	0,0	3,3	3,7	-0,4	3,1	3,1	0,0
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	3,0	3,2	-0,2	3,1	2,9	0,2	2,9	3,0	-0,1	3,1	3,2	-0,1	2,7	2,8	-0,1	3,0	3,3	-0,3	3,0	3,0	0,0
h) Deve existir uma Política de Segurança da Informação	3,4	3,0	0,4	3,6	3,5	0,1	3,3	3,3	0,0	3,5	3,5	0,0	3,4	3,2	0,2	2,7	3,3	-0,6	3,4	3,3	0,1
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	3,2	3,3	-0,1	3,8	3,4	0,4	3,1	3,1	0,0	3,1	3,2	-0,1	3,0	2,9	0,1	3,0	3,3	-0,3	3,2	3,2	0,0

Tabela 6.20- FBP/Desvios PP-PPO: Comparação pelo Tipo Função e Nível Médio de Importância

6.3.6 - Comparação com outros estudos

Neste ponto e seguindo o referencial expositivo conforme indicado na figura (Figura 6.25) seguinte faz-se referência a uma pesquisa citada por Pironti, John P. [146].

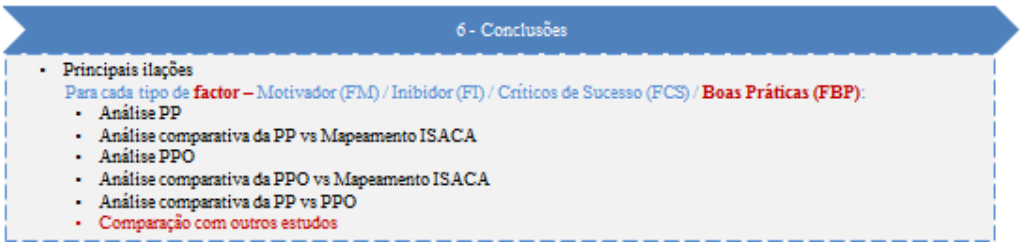


Figura 6.25- Modelo das Conclusões – FBP/Comparação co outros estudos

Assim, na investigação acima mencionada, os participantes revelaram as opiniões indicadas na figura (Figura 6.26) abaixo.

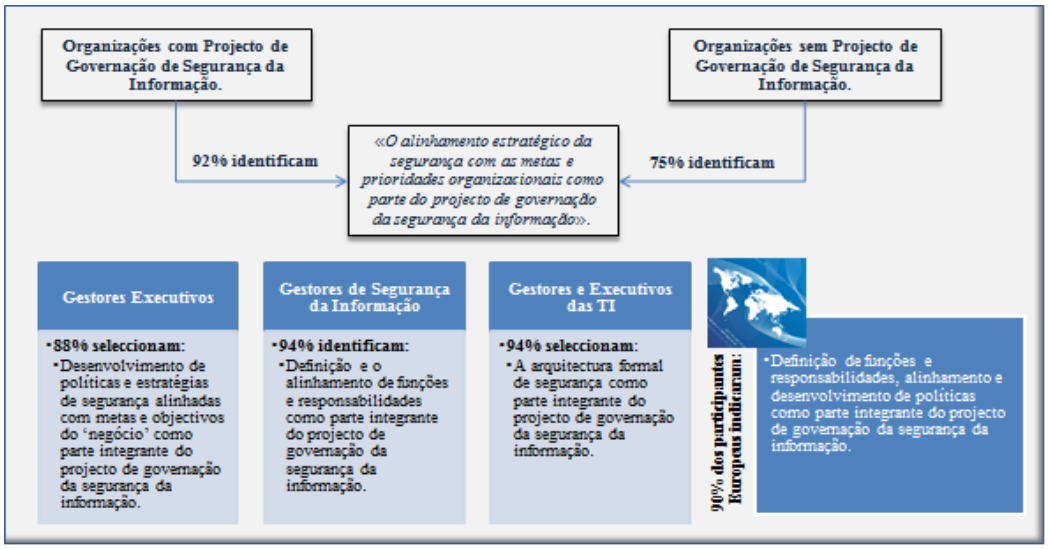


Figura 6.26- Componentes de um Projecto de Governação de Segurança da Informação. Adaptado de citação de Pironti, John P. [147]

Também no presente estudo, os gestores de topo dão primazia aos elementos dos Factores de Boas Práticas relacionados com o desenvolvimento de políticas e estratégias de segurança como sejam "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" e "*Deve existir uma Política de Segurança da Informação*". Contudo, o gestor/funcionário de segurança ao realçar o elemento "*Devem existir auditorias de Segurança de Informação*" redirecciona a prioridade, à semelhança dos seus pares na investigação acima citada, para a necessidade de definir e alinhar as funções e as responsabilidades como parte integrante da boa prática na implementação/adopção do programa de governação da segurança da informação. Já os gestores das TI, no presente estudo, apontam as questões técnicas como prioritárias, indiciando a necessidade da existência de uma arquitectura formal de segurança, conforme referência acima mencionada.

Neste contexto, verifica-se que os factores apontados como de boas práticas, no presente estudo, traduzem-se similares aos encontrados no estudo referenciado.

7. NOTAS FINAIS

Constata-se que actualmente, a aceitação da "Informação" como um recurso vital e estratégico para as organizações está na ordem do dia. Na literatura científica, segundo a ISO27000 [148] a protecção da "Informação" requer a «*preservação da confidencialidade, integridade e a disponibilidade da informação, podendo incluir outras propriedades como a autenticidade, a responsabilidade, o não-repúdio e a confiança*». Contudo, deve ter-se como ponto de partida a ideia básica de que não existe nenhum sistema totalmente seguro, pelo que se impõe a necessidade de gerir a segurança do recurso informação. Desta forma, Oliveira, Wilson [149] defende que «*a segurança da informação deve ser tratada como uma actividade contínua, pois existirão sempre novas técnicas de ataques da informação e consequentemente teremos de estar sempre atentos e prontos para o contra-ataque. A melhor arma para nossa defesa é estarmos sempre actualizados e nunca descurarmos a segurança …*».

Todavia, se, por um lado, a evolução tecnológica incita à passagem do mundo do papel para o mundo electrónico, também é certo que a mesma, associada à globalização, faz aumentar a probabilidade de ataques capazes de pôr em causa a continuidade da actividade das organizações. Neste contexto, torna-se necessário que as organizações desenvolvam mecanismos de protecção da informação, de forma a assegurar a continuidade do "negócio", a minimização dos riscos e a maximização do retorno do investimento e oportunidades de "negócio". Assim, vários são os autores que defendem que a governação da segurança da informação através da implementação dum SGSI, suportada na gestão do risco e partilhada/integrada na governação corporativa das organizações pode alavancar, não somente a protecção dos activos, como também possibilitar a criação de valor e a formação de vantagens competitivas. Contudo, também se mostrou que a cultura organizacional e consequentemente a cultura da segurança da informação constituem pilares-chave na implementação da segurança da informação nas organizações. De facto, verifica-se que o "factor humano" é o elo mais fraco na cadeia de segurança, pelo que actuar preventivamente sobre este componente, facilita a criação sustentada de uma cultura de segurança da informação, proporcionando a entrega de valor e a resiliência organizacional. Assim, de acordo com as pesquisas efectuadas, a implementação dum Sistema ou Plano/Programa de Gestão da Segurança da Informação tem sido um desafio para as organizações e muitas são as que ainda não aceitaram ou interiorizaram a importância e a mais-valia da aplicabilidade daqueles nas estruturas organizacionais.

Todavia, paralelamente também se verifica que esta não-aceitação por parte das organizações não se deve à falta de referenciais e/ou *guidelines*, uma vez que existe uma panóplia de modelos, *frameworks*, *standards* e normas disponíveis. Contudo, constata-se que a maioria

daqueles apenas proporciona “o que fazer”, sendo porém importante para as organizações, compreender e assimilar as razões do “para que fazer”, para além da necessidade do “como fazer”.

No presente estudo realizado no sector das Águas e Saneamento em Portugal verificaram-se os seguintes resultados globais (Tabela 7.1) referentes aos níveis médios de importância (NMI), atribuídos pelos respondentes e relativos aos diferentes Factores Motivadores, Inibidores, Críticos de Sucesso e de Boas Práticas que dão suporte à adopção/implementação de um Sistema de Gestão de Segurança da Informação, tendo em conta as perspectivas do próprio e a deste face à organização. Assim, o cálculo do NMI, para cada elemento daqueles factores, foi efectuado de acordo com a seguinte fórmula:

$$\text{Nível médio de importância} = \frac{\sum_{c=1}^{4}(n^{\underline{o}}\ de\ referências\ ao\ elemento * c)}{n.^{\underline{o}}\ de\ respondentes}$$

em que a variável “c” corresponde ao valor da categoria de classificação (1-Não é importante; 2-Pouco importante; 3-Importante e 4-Muito importante) seleccionado pelo respondente para o elemento em causa.

	Factores Inibidores	PP NMI	PPO NMI
(+)	“Valor do Investimento”	3,2	3,3
	“Falta de conhecimento”	3,3	3,2
	“Cultura Organizacional”	3,3	3,3
	“Dificuldade em medir o custo/benefício”	3,3	3,2
(-)	“Acesso restrito à Gestão de Topo”	2,9	2,9
	“Alterações continuas na legislação/regulação	2,8	2,9
	“Emergência Continua de novos riscos”	2,9	2,9

	Factores Motivadores	PP NMI	PPO NMI
(+)	“Garantir a disponibilidade, confidencialidade e integridade da Informação”	3,8	3,7
	“Evitar perdas financeiras”	3,6	3,5
	“Planear a segurança da informação antes da implementação de novas tecnologias	3,6	3,5
(-)	“Alterações continuas na legislação/regulação	3,1	3,1
	“Ocorrência de incidente anterior”	3,2	3,2
	“Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança”	3,2	3,2
	“Obrigatoriedade de conformidade com normas internacionais (ISSO/IEC 27001/2, etc.)	3,2	3,2

	Factores Críticos de Sucesso	PP NMI	PPO NMI
(+)	“Entendimento da ‘Gestão de topo’ para as questões da segurança da informação”	3,6	3,6
	“Suporte da Gestão de Topo”	3,5	3,5
	“Responsabilização pela Segurança da Informação”	3,5	3,5
	“Motivação dos funcionários”	3,5	3,4
(-)	“Utilização de tecnologias de suporte (COBIT, ITIL, etc.)”	3,0	3,0
	“Conformidade com normas internacionais de segurança”	3,2	3,2
	“Auditorias de Segurança da Informação”	3,2	3,2
	“Modelo/Programa de governação para a Segurança da Informação (equipa de suporte)	3,3	3,2

	Factores de Boas Práticas	PP NMI	PPO NMI
(+)	“A minha senha de acesso não a partilho com ninguém”	3,7	3,6
	“Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC”	3,4	3,5
	“Deve existir uma Politica de Segurança da Informação”	3,4	
	“Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções		3,5
(-)	“Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	3,0	
	Devem existir auditorias de Segurança da Informação	3,2	3,2
	Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	3,0	3,2
	“Deve existir uma Politica de Segurança da Informação”		3,0

Tabela 7.1- Resultados Globais obtidos: FM / FI / FCS / FBP

Uma análise mais detalhada dos dados deste estudo evidencia que:

- **O tipo de função é determinante para a visão sobre a segurança da informação -** encontram-se diferenças, quer na PP, quer na PPO, quer no resumo resultante da

análise realizada, tendo em conta os pilares de resultados propostos pelo ISACA [150] no posicionamento dos respondentes face aos elementos considerados, para os quatro vectores - FM, FI, FCS e FBP que dão suporte à adopção/implementação de um SGSI nas organizações do sector de Águas e Saneamento em Portugal.

- O valor da segurança da informação na perspectiva do próprio apresenta, globalmente, desvios face ao valor apurado na perspectiva profissional - quando existem, revelam-se sempre desvios positivos (NMI-PP > NMI-PPO) nos elementos considerados para os FM e FCS; surgem desvios positivos e desvios negativos (NMI-PP < NMI-PPO) nos itens referentes aos FI e FBP.

- **A motivação para a existência de uma cultura de segurança da informação surge, globalmente, focada na "protecção de activos",** uma vez que o valor do NMI nos FM manifestam-se em elementos relacionados com o pilar de resultados – "*Gestão de Recursos*". De facto, o pilar de resultados – "*Alinhamento Estratégico*" aparece na terceira posição (PP → NMI = 3,4; PPO →NMI = 3,3).

- A inibição para a existência de uma cultura de segurança da informação centra-se, globalmente, em itens relacionados com o "factor humano" - "*Falta de conhecimento*" e "*Cultura Organizacional*", revelando um nível médio de importância de dimensão paralela aos itens "*Valor do investimento*" e "*Dificuldade em medir o custo/benefício*". Neste contexto, pode aferir-se que o reconhecimento desta ´lacuna´ já é positivo para endereçar o caminho da mudança.

- **O sector em estudo apresenta um baixo nível de maturidade, em matéria de Segurança da Informação,** verificando que, globalmente, os elementos considerados críticos de sucesso para a adopção/implementação dum SGSI nas organizações centram-se nos pilares de resultados: "*Gestão de Desempenho*" e "*Alinhamento Estratégico*" e apresentam pontuações de nível médio de importância idênticas, na ordem dos (3,4 – 3,5). De notar o enfase do NMI nos elementos "*Entendimento da ´Gestão de Topo´ para as questões da segurança da informação*", "*Suporte da Gestão de Topo*" e "*Responsabilização pela Segurança da Informação*". De facto, estudos têm demonstrado que, quando as organizações apresentam níveis de maturidade elevados, nestas matérias, os factores críticos apontados centram-se mais nos processos do que nas estruturas.

- Os gestores de topo dão primazia aos elementos dos Factores de Boas Práticas relacionados com o desenvolvimento de políticas e estratégias de segurança, como

sejam "*Deve existir Modelo/Programa de Governação para a Segurança da Informação*" e "*Deve existir uma Política de Segurança da Informação*".

- O gestor/funcionário de segurança redirecciona a prioridade das boas práticas, para a necessidade de definir e alinhar as funções e as responsabilidades como parte integrante da boa prática na implementação/adopção do programa de governação da segurança da informação e realça o elemento "*Devem existir auditorias de Segurança de Informação*".
- Os gestores das TI apontam as questões técnicas como prioritárias, indiciando a necessidade da existência de uma arquitectura formal de segurança – os elementos seguintes, considerados de boas práticas, adquirem NMI significativos nas duas perspectivas (PP; PPO) "*A minha senha de acesso não a partilho com ninguém*" e "*Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC*".
- **O "factor humano" revela-se como um pilar basilar na cultura organizacional da segurança da informação –** surgindo a votação, em elementos relacionados com aquele factor, com valores significativos de NMI, como sejam: "*Falta de conhecimento*" e " *Cultura organizacional*" como Factores Inibidores e "*Motivação dos funcionários*", elemento crítico de sucesso na perspectiva do próprio.

Trabalhos Futuros

Seguindo a linha de orientação dos autores que defendem que um passo importante na promoção de uma cultura de segurança da informação é a avaliação do seu estado, podendo trazer benefícios à organização, nomeadamente na forma como a mesma encara a governação da segurança da informação e acompanhando o pensamento de Okere, Irene et al. [151] que apontam, entre outras, como razão para realizar a avaliação da cultura em segurança da informação, o facto de *«a mesma poder ainda servir como um ´wake-up´ para a forma como a gestão olha para estas questões ligadas à segurança da informação»* o presente estudo permitiu, no âmbito da temática da cultura organizacional em segurança da informação, caracterizar o sector empresarial das Águas e Saneamento em Portugal, segundo um dos pilares que é considerado de enorme relevância nas organizações – "o factor humano".

Assim, o trabalho realizado permitiu:

1. Desenvolver um modelo de trabalho que poderá ser aplicado a outros sectores da sociedade, permitindo a comparação entre os mesmos.

2. Aferir da relevância que o “factor humano” tem na temática da cultura organizacional em segurança da informação no sector das Águas e Saneamento em Portugal, possibilitando, no futuro, alargar o âmbito do impacto daquele factor às questões relacionadas com a segurança de outros activos relevantes para o sector.

REFERÊNCIAS

Resumo e Abstract

[1] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[2] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[3] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[4] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

Capítulo 1

[5] Oliveira, Wilson (2001) – "*Segurança da Informação – Técnicas e Soluções*" – Centro Atlântico, Lda., 1ª Ed., pp.17.

[6] Okere, Irene et al. (2012) – "Assessing Information Security Culture: A critical analysis of Current Approaches", *IEEE*, 987-1-4673-2159-**4/12.**

[7] Malcolmson, Jo (2009) – "What is Security Culture? Does it differ in content from general Organisational Culture?", *IEEE*, 978-1-4244-4170-**9/09**.

[8] Grey, David e et al. (2007) – "Sink or Swim? Water security for growth and development", *Water Policy 9*, The International Bank for Reconstruction and Development/The World Bank 2007, pp. 545-571.

[9] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[10] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

Capítulo 2

[11] Serra, J. Paulo (2007) - "*Manual de Teoria da Comunicação*", Covilhã: Livros Labcom, pp. 93-101.

[12] ISO/IEC 27000, First Edition, 1/5/2009.

[13] Adaptado Oliveira, Wilson (2001) – "*Segurança da Informação – Técnicas e Soluções*" – Centro Atlântico, Lda., 1ª Ed., pp.17,19.

[14] OCDE (1999) – "Principles of Corporate Governance" - citado por Gonçalves, Hélder (2011) - "*A Gestão do Risco Operacional e as TIC – O Contributo da Auditoria no Sector Financeiro*", Universidade Católica Editora 2011, pp.105.

[15] Wiander, Timo, et al. (2006) – "Holistic Information Security Management in Multi-Organization Environment", *IEEE*, VTT Technical Research Centre of Finland, 1-4244-0497-**5/06**.

[16] Sandrino-Arndt, Bop $^{CISA, PMP}$ (2008) – "People, Portfolios and Processes: The 3P Model IT Governance" - *Information System Control Jornal*, **volume 2**, pp.36-40.

[17] IT Governance Institute (2003) – "Board Briefing on IT Governance", 2nd Edition, USA.

[18] IT Governance Institute (2001) – citado por Grembergen, Wim Van et al. (2004) – "Structures, Processes and Mechanisms for IT Governance - Strategies for Information Technology Governance", *Idea Group Inc*., Chaper 1, pp. 5, ISBN 1-59140-284-0.

[19] Grembergen, Wim Van et al. (2004) – "Structures, Processes and Mechanisms for IT Governance - Strategies for Information Technology Governance", *Idea Group Inc*., Chaper 1, pp. 5, ISBN 1-59140-284-0.

[20] IT Governance Institute (2001) – "Cobit: Governance, Control and Audit for Information and Related Tecnology". Available online www.itgi.org, citado por Grembergen, Wim Van et al. (2004) – "Structures, Processes and Mechanisms for IT Governance - Strategies for Information Technology Governance", *Idea Group Inc.*, Chaper 1, pp. 6, ISBN 1-59140-284-0.

[21] ISO/IEC 27000, First Edition, 1/5/2009.

[22] Helokunnas, Tuija et al. (2003) – "Information Security Culture in a Value Net", *IEEE*, 0-7803-8150-**5/03**.

Capítulo 3.

[23] Le Coadic, Yves-Francois (1994) – "A Ciência da Informação", tradução de Gomes, Maria Yêda F.S. de Felgueiras, *Briquet de Lemos / Livros* (1996), Brasília, ISBN 85-85637-08-0.

[24] Barreto, Aldo de Albuquerque (1994) – "A Questão da Informação", *Revista São Paulo em Perspectiva*, Fundação Seade, **v 8**, n 4.

[25] Varajão, João Eduardo Quintela (1998) – "*A Arquitectura da Gestão de Sistemas de Informação*", FCA – Editora de Informática, 2ª Edição, ISBN: 972-722-140-8, pp.45.

[26] ISO/IEC 27000, First Edition, 1/5/2009.

[27] ISO/IEC 27000, First Edition, 1/5/2009.

[28] ISO/IEC 27000, First Edition, 1/5/2009.

[29] ISO/IEC 27000, First Edition, 1/5/2009.

[30] ISO/IEC 27000, First Edition, 1/5/2009.

[31] Oliveira, Wilson (2001) – "*Segurança da Informação – Técnicas e Soluções*", Centro Atlântico, Lda, 1ª Ed., 2001, pp.67.

[32] ISO/IEC 27000, First Edition, 1/5/2009.

[33] Gonçalves, Hélder (2011) - "*A Gestão do Risco Operacional e as TIC – O Contributo da Auditoria no Sector Financeiro*" - Universidade Católica Editora 2011, pp.173.

[34] Fernandes, Jorge Henrique Cabral (2009) – "Introdução à Gestão de Riscos de Segurança da Informação" – GSIC302, versão 1.2 – CEGSIC (2009-2011) pp. 17 e ISACA (2009) Figure 39—IT Risk Scenario Components, "*The Risk IT Practitioner Guide*", ISBN 978-1-60420-116-1, pp.55.

[35] Wiander, Timo, et al. (2006) – "Holistic Information Security Management in Multi-Organization Environment", *IEEE* – [1] ISO, [on-line], Available at: www.iso.org, [Ref. 14.12.2005], VTT Technical Research Centre of Finland, 1-4244-0497-**5/06**.

[36] ENISA (Agosto, 2012) - "Cyber Incident Reporting in the EU - An overview of security articles in EU legislation", Available online:

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu (consultado em 12/1/2013).

[37] Ponemon Institute© Research Report (August) 2011 – "Second Annual Cost of Cyber Crime Study - Benchmark Study of U.S. Companies". *Sponsored by ArcSight, an HP Company Independently conducted by Ponemon Institute* $_{LLC.}$ Available online:

http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf (consultado em 18/2/2013).

[38] Oliveira, Wilson (2001) – "*Segurança da Informação – Técnicas e Soluções*", Centro Atlântico, Lda, 1ª Ed., 2001, pp.20.

[39] Oliveira, Wilson (2001) – "*Segurança da Informação – Técnicas e Soluções*", Centro Atlântico, Lda, 1ª Ed., 2001, pp.173 e pp.66.

[40] Wiander, Timo, et al. (2006) – "Holistic Information Security Management in Multi-Organization Environment", *IEEE,* VTT Technical Research Centre of Finland, 1-4244-0497-**5/06**.

[41] Poole, Vernon, CISM® (2006) – "Why Information Security Governance - Is Critical to Wider Corporate Governance Demands—A European Perspective" – *Information System Control Jornal*, **Volume 1**.

[42] Hamaker Stacey CISA®, CIA® et al. (2005) – "Enterprise Governance and the Role of IT", *Information Systems Control Journal*, **Volume 6**.

[43] COBIT Foundation Course (2009) citado por Gonçalves, Hélder (2011) - "*A Gestão do Risco Operacional e as TIC – O Contributo da Auditoria no Sector Financeiro*", Universidade Católica Editora, 2011, pp.105.

[44] Tashi, Igli et al. (2009) – "A Security Management Assurance Model to holistically assess the Information Security posture", *IEEE,* DOI 10.1109/ARES.2009.28, 978-0-7695-3564-**7/09**.

[45] Shaun, Posthumus et al. (2004) – "A framework for the governance of information security". *Computers and Security*, 23(1):638-646 citado por Tashi, Igli et al. (2009) [44].

[46] Dodds, Rupert CISA®, CISM® (2005) – "How does Information Security Fit Into a Governance Framework?" – *Information Systems Audit and Control Associations*, JournalOnline, www.isaca.org.

[47] Malik, J. William (2006) – "Information Security Governance" – *Information Systems Control Journal*, IT Governance, **Volume 3**, pp.23.

[48] ISO/IEC 27000, First Edition, 1/5/2009.

[49] Gonçalves, Hélder (2011) - "*A Gestão do Risco Operacional e as TIC – O Contributo da Auditoria no Sector Financeiro*", Universidade Católica Editora 2011, pp.161.

[50] NIST (2012) – "*Guide for Conducting Risk Assessments – Information Security*" – NIST Especial Publication – Revision 1, September, Anexo B, pp.B-6.

[51] Brotby, Krag CISM® (2007) cita relatório do IT Governance Institute´s "IT Governance Global Status Report 2006*"* – *Information Systems Control Journal*, **Volume 2**, pp.14.

[52] Pironti, John P., CISA®, CISM®, CISSP®, ISSAP®, ISSMP® (2006) – "Information Security Governance: Motivations, Benefits and Outcomes" - *Information System Control Jornal*, **Volume 4**, pp.45-48.

[53] Malik, J. William (2006) – "Information Security Governance" – *Information Systems Control Journal*, IT Governance, **Volume 3**, pp.23.

[54] ISACA (2010) – "The Business Model for Information Security" – ISBN 978-1-60420-154-3, pp.12 citando *ISACA* (2008) – "Information Security Governance: Guidance for Information Security Managers", USA.

[55] Tashi, Igli et al. (2009) – "A Security Management Assurance Model to holistically assess the Information Security posture", *IEEE*, DOI 10.1109/ARES.2009.28, 978-0-7695-3564-**7/09.**

[56] ISO 27001:2005 (E) – "*Information technology – Security tecniques – Information security management systems – Requirements*", pp. vi.

[57] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.7, 9 e 13.

[58] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp. 13.

[59] Gonçalves, Hélder (2011) - "*A Gestão do Risco Operacional e as TIC – O Contributo da Auditoria no Sector Financeiro*", Universidade Católica Editora 2011, pp.107,110.

[60] ISACA (2012) – "COBIT5 - Executive Summary", Available online: http://www.isaca.org/cobit/pages/default.aspx (consultado em 3/11/2013).

[61] ISACA (2012) – "COBIT5 - Executive Summary", Available online: http://www.isaca.org/cobit/pages/default.aspx (consultado em 3/11/2013).

[62] Gonçalves, Hélder (2011) - "*A Gestão do Risco Operacional e as TIC – O Contributo da Auditoria no Sector Financeiro*", Universidade Católica Editora 2011, pp.112.

[63] Santos, Luís (2008) – "*Estudo sobre factores de sucesso na Gestão de Segurança da Informação nas Empresas Portuguesas*" – Dissertação de Mestrado em Gestão de Sistemas de Informação, ISCTE – Departamento de Ciências e Tecnologias de Informação.

[64] ISO 27000, First Edition, 1/5/2009, adaptado de Gonçalves, Hélder (2011) - "*A Gestão do Risco Operacional e as TIC – O Contributo da Auditoria no Sector Financeiro*", Universidade Católica Editora 2011, pp. 40-41.

[65] ISO (2013) - "Registo de empresas certificadas". Available online: http://www.iso27001certificates.com/ (consultado a 21/02/2013).

[66] NIST (2013) – "NIST General Information", 2º parágrafo. Available online: http://www.nist.gov/public_affairs/general_information.cfm (consultado em 26/05/2013).

[67] NIST/CSD - Computer Security Division (2013) – "CSD Mission Statement". Available online: http://csrc.nist.gov/mission/index.html (consultado em 26/05/2013).

[68] CSD/NIST (2013) – "Special Publications (800 Series)". Available online: http://csrc.nist.gov/publications/PubsSPs.html (consultado em 26/05/2013).

[69] NIST (2012) – "Information Security – Guide for Conducting Risk Assessments" – *NIST Special Publication 800-30*, Revision 1, September 2012.

[70] Gonçalves, Hélder (2011) - "*A Gestão do Risco Operacional e as TIC – O Contributo da Auditoria no Sector Financeiro*", Universidade Católica Editora 2011, pp. 21, 24.

[71] NIST (2012) – "Information Security – Guide for Conducting Risk Assessments" – *NIST Special Publication 800-30*, Revision 1, September, pp.4.

[72] NIST (2011) – "Managing Information - Security Risk Organization, Mission, and Information System View" – *NIST Special Publication 800-39*, Março 2011, pp.4.

[73] ENISA (2012) – "*National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace*", ENISA, Maio 2012.

[74] UE (2013) - "Estratégia digital para a União Europeia", *Sínteses da legislação da UE*, Available online: http://europa.eu/legislation_summaries/information_society/strategies/index_pt.htm (consultado em 21-02-2013).

[75] UE (2013) – "Estratégia digital para a União Europeia", *Sínteses da legislação da EU, Available online:* http://europa.eu/legislation_summaries/information_society/strategies/index_pt.htm (consultado em 21-02-2013).

[76] GNS (2013) – "Lei orgânica do Gabinete Nacional de Segurança", *Decreto-Lei n.º 3/2012, de 16 de Janeiro*, 6º parágrafo do preâmbulo, Available online: http://www.gns.gov.pt/lei-organica.aspx, (consultado a 09-02-2014).

[77] Presidência do Conselho de Ministros (2012), *GNS*, Available online: (http://www.gns.gov.pt/media/1247/PropostaEstratégiaNacionaldeCibersegurançaPortuguesa.pdf, (consultado a 10-11-2013).

[78] GNS - Resolução do Conselho de Ministros N.º 50/88, de 3/12, SEGNAC 1, ponto 1.2.2.5 – Importância do factor humano, Available online: http://www.gns.gov.pt/legislacao.aspx, (consultado a 09/02/2014).

[79] Pironti, John P., CISA®, CISM®, CISSP®, ISSAP®, ISSMP® (2006) – "Information Security Governance: Motivations, Benefits and Outcomes" - *Information System Control Jornal*, **Volume 4**, pp.45-48.

[80] Tavares, Fernanda Pereira (1996) - "A Cultura Organizacional como um instrumento de Poder", *Caderno de Pesquisas em Administração*, São Paulo, **V.1**, Nº 3, 2º SEM.

[81] Barbosa, Lívia Neves de Holanda (1996) – "Cultura Administrativa: Uma Nova Perspectiva das Relações entre Antropologia e Administração", *RAE - Revista de Administração de Empresas*, São Paulo, **V. 36**, n. 4, pp. 6-19 Out./Nov./Dez. 1996.

[82] Geertz, C. (1978) – "A interpretação das culturas". Rio de Janeiro: Zahar, 1978.

[83] Fleury, Maria Tereza Leme, et al. (1997) – "Entre a Antropologia e a Psicanálise: Dilemas Metodológicos dos Estudos sobre Cultura Organizacional", *Revista de Administração*, São Paulo **v.32**, n. 1, p. 23-37, Janeiro/Março.

[84] Malcolmson, Jo (2009) – "What is Security Culture? Does it differ in content from general Organisational Culture?", *IEEE* , 978-1-4244-4170-**9/09**.

[85] Santos, Maribel Yasmina et al. (2009) – "*Business Inteligence – Tecnologias da Informação na Gestão do Conhecimento*", FCA – Editora de Informática, 2ª Edição Actualizada e Aumentada, ISBN: 978-972-722-516-3, pp. 42.

[86] Malcolmson, Jo (2009) – "What is Security Culture? Does it differ in content from general Organisational Culture?" *IEEE* – 978-1-4244-4170-**9/09**.

[87] Okere, Irene et al. (2012) – "Assessing Information Security Culture: A critical analysis of Current Approaches", *IEEE* , 987-1-4673-2159-**4/12**,.

[88] Malcolmson, Jo (2009) – "What is Security Culture? Does it differ in content from general Organisational Culture?" *IEEE*, 978-1-4244-4170-**9/09**.

[89] ISACA (2010) – "The Business Model for Information Security (BMIS)", pp.27 refere Kiely, L. et al. ´Systemic Security Management', *Security & Privacy, IEEE*, vol. **4**, n. 6, 2006, pp. 74-77.

[90] ISACA (2010) – "The Business Model for Information Security (BMIS)", pp.23.

[91] Tashi, Igli et al. (2009) – "A Security Management Assurance Model to holistically assess the Information Security posture", *IEEE*, DOI 10.1109/ARES.2009.28, 978-0-7695-3564-**7/09**.

[92] Helokunnas, Tuija et al. (2003) – "Information Security Culture in a Value Net", *IEEE*, 0-7803-8150-**5/03**.

[93] Okere, Irene et al. (2012) – "Assessing Information Security Culture: A Critical Analysis of Current Approaches", *IEEE* , 978-1-4673-2159-**4/12**.

[94] Schlienger, Thomas et al. (2003) – "Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture" – Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03) – *IEEE Computer Society*.

[95] Ngo, Leanne et al. (2005) – "The Multifaceted and Ever-Changing Directions of Information Security – Australia Get Ready!" – Proceedings of the Third International Conference on Information Tecnology and Applications (ICITA´05), 0-7695-2316-1/05 – *IEEE Computer Society*.

[96] Helokunnas, Tuija et al. (2003) – "Information Security Culture in a Value Net", *IEEE*, 0-7803-8150-**5/03**.

[97] Schlienger, Thomas et al. (2003) – "Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture" – Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03) – *IEEE Computer Society*.

[98] Okere, Irene et al. (2012) – "Assessing Information Security Culture: A Critical Analysis of Current Approaches", *IEEE*, 978-1-4673-2159-**4/12**.

[99] Niekerk, Van et al. (2010) –"Information Security Culture: A management perspective", *Computers & Security*, **vol. 29**, Jun. 2010, pp. 476-486.

[100] Okere, Irene et al. (2012) – "Assessing Information Security Culture: A Critical Analysis of Current Approaches", *IEEE*, 978-1-4673-2159-**4/12**

[101] Jonch-Clausen, Torkil et al. (2001) – "Firming up the Conceptual Basis of Integrated Water Resources Management", *International Journal of Water Resources Development*, **17:4**, 501-510.

[102] Grey, David et al. (2007) – "Sink or Swim? Water security for growth and development", Water Policy 9 (2007) 545-571, The International Bank for Reconstruction and Development/The World Bank 2007.

[103] United Nations General Assembly (2011) – "The human right to safe drinking water and sanitation" cita a resolução 64/292 de 28/7/2010 da Assembleia Geral das Nações Unidas

Available online: http://www.ohchr.org/Documents/Issues/Water/A.HRC.18.L.1_en.pdf (consultado em 10-06-2013).

[104] Grey, David et al. (2007) – "Sink or Swim? Water security for growth and development", Water Policy 9 (2007) 545-571, *The International Bank for Reconstruction and Development/The World Bank 2007.*

[105] Jonch-Clausen, Torkil et al. (2001) – "Firming up the Conceptual Basis of Integrated Water Resources Management", *International Journal of Water Resources Development*, **17:4**, 501-510.

[106] Tortajada, Cecilia (2010) – "Water Governance: Some Critical Issues", *International Journal of Water Resources Development*, **26:2**, 297-307.

[107] Jonch-Clausen, Torkil et al. (2001) – "Firming up the Conceptual Basis of Integrated Water Resources Management", *International Journal of Water Resources Development*, **17:4**, 501-510.

[108] Biswas, Asit K. et al. (2008) – "Achieving Water Security for Asia", *International Journal of Water Resources Development*, **24:1**, 145-176.

[109] Conselho da União Europeia (2010) – "Projecto de Estratégia da segurança interna da União Europeia: Rumo a um modelo europeu de segurança" – 5842/2/10 VER 2, DG H 3A, AB/SR/jv.

[110] Águas de Portugal e APDA (2011) – "Planos de Segurança da Água em Portugal: Onde estamos, para onde vamos." Apresentação da sessão temática. Available online: http://www.apda.pt/pdfs/AdP_APDA_Planos_de_Seguranca_AguaPortugal.pdf, (consultado a 10-6-2013).

[111] Dodds, Rupert (2005) – "How does Information Security Fit Into a Governance Framework?" – *Information Systems Audit and Control Associations, JournalOnline.*

Capítulo 4

[112] Varajão, João Eduardo Quintela (1998) – "*A Arquitectura da Gestão de Sistemas de Informação"*, FCA – Editora de Informática, 2ª Edição, ISBN: 972-722-140-8, pp.45.

[113] Varajão, João Eduardo Quintela (1998) – "*A Arquitectura da Gestão de Sistemas de Informação*", FCA – Editora de Informática, 2ª Edição, ISBN: 972-722-140-8, pp.45.

[114] Okere, Irene et al. (2012) – "Assessing Information Security Culture: A Critical Analysis of Current Approaches", *IEEE*, 978-1-4673-2159-**4/12**.

[115] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[116] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers"*, USA.

[117] Okere, Irene et al. (2012) – "Assessing Information Security Culture: A Critical Analysis of Current Approaches", *IEEE*, 978-1-4673-2159-**4/12**.

[118] Santos, Luís (2008) – "*Estudo sobre Factores de Sucesso na Gestão de Segurança da Informação nas Empresas Portuguesas*", Dissertação de Mestrado em Gestão de Sistemas de Informação, ISCTE – Departamento de Ciências e Tecnologias de Informação.

[119] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[120] ISACA (2010) – "*The Business Model for Information Security*", ISBN 978-1-60420-154-3, pp. 9.

[121] ISACA (2010) – "*The Business Model for Information Security*", ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

Capítulo 5

[122] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[123] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[124] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[125] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

Capítulo 6

[126] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[127] ISO27000, First Edition, 1/5/2009.

[128] Oliveira, Wilson (2001) – "*Segurança da Informação – Técnicas e Soluções*", Centro Atlântico, Lda, 1ª Ed., pp.66 e 173.

[129] Oliveira, Wilson (2001) – "*Segurança da Informação – Técnicas e Soluções*" – Centro Atlântico, Lda., 1ª Ed., pp.17.

[130] Conselho da União Europeia (2010) – "Estratégia da segurança interna da União Europeia: Rumo a um modelo europeu de segurança", *Serviço das Publicações da União Europeia, 2010 Luxemburgo*, ISBN 978-92-824-2689-0, doi:10.2860/91465, pp. 11 e 19.

[131] United Nations General Assembly (2011) – "The human right to safe drinking water and sanitation" cita a resolução 64/292 de 28/7/2010 da Assembleia Geral das Nações Unidas Available online:

http://www.ohchr.org/Documents/Issues/Water/A.HRC.18.L.1_en.pdf (consultado em 10-06-2013).

[132] Grey, David et al. (2007) – "Sink or Swim? Water security for growth and development", Water Policy 9 (2007) 545-571, The International Bank for Reconstruction and Development/The World Bank 2007.

[133] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[134] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[135] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[136] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[137] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[138] Pironti, John P., CISA®, CISM®, CISSP®, ISSAP®, ISSMP® (2006) – "Information Security Governance: Motivations, Benefits and Outcomes" - *Information System Control Jornal*, **volume 4**, pp.45-48.

[139] ISACA (2010) – "*The Business Model for Information Security*", ISBN 978-1-60420-154-3, pp.9.

[140] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[141] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[142] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[143] Santos, Luís (2008) – "*Estudo sobre factores de sucesso na Gestão de Segurança da Informação nas Empresas Portuguesas*" – Dissertação de Mestrado em Gestão de Sistemas de Informação, ISCTE – Departamento de Ciências e Tecnologias de Informação.

[144] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[145] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[146] Pironti, John P., CISA®, CISM®, CISSP®, ISSAP®, ISSMP® (2006) – "Information Security Governance: Motivations, Benefits and Outcomes" - *Information System Control Jornal*, **volume 4**, pp.45-48.

[147] Pironti, John P., CISA®, CISM®, CISSP®, ISSAP®, ISSMP® (2006) – "Information Security Governance: Motivations, Benefits and Outcomes" - *Information System Control Jornal*, **volume 4**, pp.45-48.

Capítulo 7

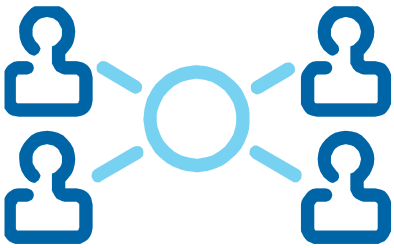
[148] ISO27000, First Edition, 1/5/2009.

[149] Oliveira, Wilson (2001) – "*Segurança da Informação – Técnicas e Soluções*", Centro Atlântico, Lda, 1ª Ed., pp.66 e pp.173.

[150] ISACA (2010) – "*The Business Model for Information Security*" – ISBN 978-1-60420-154-3, pp.12 citando ISACA (2008) – "*Information Security Governance: Guidance for Information Security Managers*", USA.

[151] Okere, Irene et al. (2012) – "Assessing Information Security Culture: A Critical Analysis of Current Approaches", *IEEE*, 978-1-4673-2159-**4/12**.

Universidade Católica Portuguesa
Faculdade de Engenharia



O Impacto das Crenças Individuais dos Profissionais na Cultura de Segurança da Informação nas Organizações

– Estudo no sector da Água / Saneamento em Portugal

Maria Helena Ferreira da Cruz e Silva

Dissertação para obtenção do Grau de Mestre em Segurança em Sistemas de Informação
Anexos

Júri

Prof. Doutor Manuel José Martinho Barata Marques (Presidente)
Prof. Doutor Rui Jorge Correia Mendes Alves Pires
Prof. Doutor Tito Santos Silva (Orientador)

Setembro de 2014

Universidade Católica Portuguesa
Faculdade de Engenharia

O Impacto das Crenças Individuais dos Profissionais na Cultura de Segurança da Informação nas Organizações

– Estudo no sector da Água / Saneamento em Portugal

Maria Helena Ferreira da Cruz e Silva

Dissertação para obtenção do Grau de Mestre em Segurança em Sistemas de Informação
Anexo A

Júri

Prof. Doutor Manuel José Martinho Barata Marques (Presidente)
Prof. Doutor Rui Jorge Correia Mendes Alves Pires
Prof. Doutor Tito Santos Silva (Orientador)

Setembro de 2014

1. MINUTA DO E-MAIL ENVIADO

No âmbito do trabalho realizado foi enviado e-mail aos Conselhos de Administração das Entidades Gestoras. A minuta do e-mail enviado encontra-se de seguida.

«Exmo. Conselho de Administração

Encontro-me a realizar uma Tese de Mestrado em Segurança em Sistemas de Informação pela Faculdade de Engenharia da Universidade Católica Portuguesa.

Neste contexto, elaborei um Questionário sobre a importância dos FACTORES MOTIVADORES, INIBIDORES, CRÍTICOS DE SUCESSO e BOAS PRÁTICAS na adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização.

*Para a recolha de dados/informação venho por este meio solicitar a divulgação deste e-mail pelos trabalhadores da vossa organização (para que possam também colaborar/participar) e a vossa colaboração/participação através da resposta ao questionário on-line (**até 25/2/2013),** que se encontra neste endereço:*

https://docs.google.com/spreadsheet/viewform?formkey=dDFENi1Nd1hvVXY5M1F4em9PYTJtYnc6MA#gid=0

Para uma melhor compreensão das diversas questões, envio, ainda, em anexo um ficheiro pdf, com uma explicação resumida do tema e o mote para a realização deste trabalho. No questionário, os temas em questão encontram-se organizados de modo a que possam ser respondidos segundo duas perspectivas:

- *a vossa opinião: o que pensa/faz*
- *o vosso ponto de vista no vosso sector de actividade/organização: o que a organização efectivamente pensa/faz.*

A vossa opinião é importante. Desde já, agradeço a vossa participação. A apresentação da Tese de Mestrado e respectivos resultados será pública. Para qualquer esclarecimento adicional por favor contacte por este endereço de mail.»

2. LISTA DAS ENTIDADES

Seguidamente apresenta-se a listas das Entidades Gestoras conforme retiradas do site da APDA – www.apda.pt (consultado em Dezembro e Janeiro de 2013).

2.1 - Região Norte

Nome da Entidade	Enviados	Observações
AGERE - Empresa de Águas, Efluentes e Resíduos de Braga, EM Praça Conde Agrolongo, 115 4700-312 Braga Tel. + 351 253 205 000 Fax. + 351 253 205 075		

Nome da Entidade	Enviados	Observações
Email: agere@agere.pt **AGS - Paços de Ferreira, SA** Rua Dr. Leão Meireles, 94 4590-586 Paços de Ferreira Tel. + 351 255 860 560 Fax. + 351 255 860 569	1	
Email: geral@agspacosferreira.pt **Águas de Barcelos, SA** Rua Rosa Ramalho, LT 25 4750-331 Tel. + 351 253 813 814 Fax. + 351 253 813 815	1	
Email: geral@aguasdebarcelos.pt **Águas de Carrazeda, SA** Rua Vitor Guilhar, 90 - 92 5140-103 Carrezeda de Ansiães Tel. + 351 278 617 736 Fax. + 351 278 616 730	1	
Email: aguasdecarrazeda@gmail.com **Águas de Gondomar, SA** Rua 5 de Outubro, 112 4420-086 Gondomar Tel. + 351 224 660 200 Fax. + 351 224 640 349	1	
Email: geral@aguasdegondomar.pt **Águas de Paredes, SA** Rua de Timor, 27 4580-015 Paredes Tel. + 351 255 788 530 Fax. + 351 255 788 539	1	
Email: aguas.paredes@veoliaagua.com.pt. **Águas de São João, EM, SA** Avenida da Liberdade 3701-956 S.João da Madeira Tel. + 351 256 100 700 Fax. + 351 256 100 709	1	
Email: geral@aguasdesjoao.pt **Águas de Valongo, SA** Rua 5 de Outubro, 306 4440-503 Valongo Tel. + 351 224 227 390 Fax. + 351 224 222 644	1	
Email: aguas.valongo@veoliaagua.com.pt	1	? resposta mail automática
Águas do Marco, SA Alameda Dr. Miranda da Rocha 4630-220 Marco de Canavesses Tel. + 351 255 538 350 Fax. + 351 255 538 359		
Email: geral@aguasdomarco.pt **32 - CMPEA - Empresa de Águas do Município do Porto, EEM** Rua Barão de Nova Sintra, 285 4300-367 Porto Tel. + 351 225 190 800 Fax. + 351 225 190 828	1	
Email: geral@aguasdoporto.pt **Águas e Parque Biológico de Gaia, EEM** Rua 14 de Outubro, 343 Apartado 35	1	

Nome da Entidade	Enviados	Observações
4431-954 Vila Nova de Gaia Tel. + 351 223 770 460 Fax. + 351 223 796 369 Email: info@aguasgaia.pt	1	
Câmara Municipal de Alfândega da Fé Praça do Município 5350-017 Alfandega da Fé Tel. + 351 279 468 120 Fax. + 351 279 462 619 Email: cmaf@mail.telepac.pt; gabinetepresidencia.cmaf@gmail.com	1	
Câmara Municipal de Alijó Rua General Alves Pedrosa, 13 5070-051 Alijó Tel. + 351 259 957 100 Fax. + 351 259 959 738 Email: geral@cm-alijo.pt	1	
Câmara Municipal de Amarante Alameda Teixeira Pascoães 4600-011 Amarante Tel. + 351 255 420 200 Fax. + 351 255 420 201 Email: cma.gabimprensa@mail.telepac.pt; amarante@cm-amarante.pt	1	0
Câmara Municipal de Amares Largo Município 4720-057 Amares Tel. + 351 253 991 330 Fax. + 351 253 992 643 Email: cmamares.pij@mail.telepac.pt; cm.amares@mail.telepac.pt	1	
Câmara Municipal de Arcos de Valdevez Praça Municipal 4974-003 Arcos de Valdevez Tel. + 351 258 520 500 Fax. + 351 258 520 509 Email: secretaria@cm-arcos-valdevez.org; geral@cmav.pt	1	Msg entregue
Câmara Municipal de Armamar Praça da República 5110-127 Armamar Tel. + 351 254 850 800 Fax. + 351 254 850 802 Email: camaraarmamar@mail.telepac.pt; geral@cm-armamar.pt	1	
Câmara Municipal de Arouca Praça do Município 4544-001 Arouca Tel. + 351 256 940 220 Fax. + 351 256 943 045 Email: arouca@cm-arouca.pt	0	erro envio mail
Câmara Municipal de Baião Rua Heróis do Ultramar 4640-158 Baião Tel. + 351 255 540 500 Fax. + 351 255 540 510 Email: camarabaiao@mail.telepac.pt; geral@cm-baiao.pt	1	
Câmara Municipal de Boticas Praceta do Município		

Nome da Entidade	Enviados	Observações
5460-304 Boticas Tel. + 351 276 410 200 Fax. + 351 276 410 201 Email: cmboticas@cm-boticas.pt	1	
Câmara Municipal de Bragança Forte S. João de Deus 5301-902 Bragança Tel. + 351 273 304 200 Fax. + 351 273 304 298 Email: cmb@cm-braganca.pt	1	
Câmara Municipal de Cabeceiras de Basto Praça da República 4860-355 Cabeceiras de Basto Tel. + 351 253 669 100 Fax. + 351 253 662 726 Email: geral-cmcbasto@mail.telepac.pt	1	
Câmara Municipal de Caminha Praça Conselheiro Silva Torres 4910-122 Caminha Tel. + 351 258 710 300 Fax. + 351 258 710 319 Email: c.caminha@mail.telepac.pt; geral@cm-caminha.pt	1	
Câmara Municipal de Castelo de Paiva Largo do Conde Sobrado 4550-102 Castelo de Paiva Tel. + 351 255 689 500 Fax. + 351 255 699 282 Email: cpaiva@cm-castelo-paiva.pt	0	erro envio mail
Câmara Municipal de Celorico de Basto Praça Cardeal D. António Ribeiro 4890-220 Celorico de Basto Tel. + 351 255 320 300 Fax. + 351 255 321 937 Email: geral@cm-celoricobasto.pt	1	
Câmara Municipal de Chaves Praça de Camões 5400-150 Chaves Tel. + 351 276 340 500 Fax. + 351 276 327 724 Email: cmc@mail.telepac.pt; municipio@cm-chaves.pt	0	erro envio mail
Câmara Municipal de Cinfães Largo dos Paços do Concelho 4690-030 Cinfães Tel. + 351 255 560 560 Fax. + 351 255 561 501 Email: cmcinfaes@hotmail.com; apoio.presidente@cm-cinfaes.pt	1	
Municipio de Espinho Praça Dr. José Salvador 4501-901 Espinho Tel. + 351 227 335 800 Fax. + 351 227 335 852 Email: cme@cm-espinho.pt	0	erro envio mail
Câmara Municipal de Fafe Av. 5 de Outubro 4820-501 Fafe Tel. + 351 253 700 400 Fax. + 351 253 700 409 Email: geral@cm-fafe.pt	1	

Nome da Entidade	Enviados	Observações
Câmara Municipal de Felgueiras Praça da República 4610-116 Felgueiras Tel. + 351 255 318 000 Fax. + 351 255 318 170 Email: cmfelgueiras@mail.telepac.pt; geral@cm-felgueiras.pt	1	
Câmara Municipal de Freixo de Espada à Cinta Av. Guerra Junqueiro 5180-104 Freixo de Espada À Cinta Tel. + 351 279 658 160 Fax. + 351 279 658 165 Email: geral@cm-freixoespadacinta.pt	1	
Câmara Municipal de Lamego Rua Padre Alfredo Pinto Teixeira 5100-150 Lamego Tel. + 351 254 609 600 Fax. + 351 254 609 601 Email: del.adn@cm.lamego.pt	0	erro envio mail
Câmara Municipal de Lousada Praça Dr. Francisco Sá Carneiro 4624-909 Lousada Tel. + 351 255 820 500 Fax. + 351 255 820 550 Email: cm-lousada@cm-lousada.pt	1	
Câmara Municipal de Macedo de Cavaleiros Jardim 1º de Maio 5340-218 Macedo de Cavaleiros Tel. + 351 234 915 230 Fax. + 351 278 426 243 Email: cmacedocavaleiros@mail.telepac.pt	1	
Câmara Municipal de Melgaço Largo Hermenegildo Solheiro 4960-551 Melgaço Tel. + 351 251 410 100 Fax. + 351 251 402 429 Email: geral@cm-melgaco.pt	1	
Câmara Municipal de Mesão Frio Av. Conselheiro José M. Alpoim, 432 5040-310 Mesão Frio Tel. + 351 254 890 100 Fax. + 351 254 890 109 Email: geral@cm-mesaofrio.pt	1	
Câmara Municipal de Miranda do Douro Largo D. João III 5210-190 Miranda do Douro Tel. + 351 273 430 020 Fax. + 351 273 431 075 Email: geral@cm-mdouro.pt	1	
Câmara Municipal de Mirandela Largo do Município 5370-288 Mirandela Tel. + 351 278 200 200 Fax. + 351 278 265 753 Email: cmmrdl@mail.telepac.pt	0	erro envio mail
Câmara Municipal de Mogadouro Convento de S. Francisco 5200-244 Mogadouro Tel. + 351 279 340 100 Fax. + 351 279 341 874 Email: camaramogadouro@netc.pt;	1	

Nome da Entidade	Enviados	Observações
camaramogadouro@mail.telepac.pt **Câmara Municipal de Moimenta da Beira** Largo do Tabolado 3620-324 Moimenta da Beira Tel. + 351 254 520 070 Fax. + 351 254 520 071 Email: cmmbeira@cm-moimenta.pt	1	
Câmara Municipal de Monção Largo de Camões 4950-444 Monção Tel. + 351 251 649 000 Fax. + 351 251 652 966 Email: cmmoncao@mail.telepac.pt; gap@cm-moncao.pt	1	
Câmara Municipal de Mondim de Basto Largo do Conde de Vila Real 4880-236 Mondim de Basto Tel. + 351 255 389 300 Fax. + 351 255 389 398 Email: geral@cm-mondimdebasto.pt	1	
Câmara Municipal de Montalegre Praça do Município 5470-909 Montalegre Tel. + 351 276 510 200 Fax. + 351 276 510 201 Email: municipio@cm-montalegre.pt	1	
Câmara Municipal de Murça Praça 5 de Outubro, 10 5090-112 Murça Tel. + 351 259 510 120 Fax. + 351 259 510 129 Email: cmmurca@mail.telepac.pt	1	
Câmara Municipal de Oliveira de Azeméis Largo da República 3720-240 Oliveira de Azeméis Tel. + 351 256 600 600 Fax. + 351 256 660 896 Email: c.m.o.azemeis@mail.telepac.pt; geral@cm-oaz.pt	1	
Câmara Municipal de Paredes de Coura Largo Visconde de Moselos 4940-525 Paredes de Coura Tel. + 351 251 780 100 Fax. + 351 251 780 118 Email: contacto@cm-paredes-coura.pt	1	
Câmara Municipal de Penedono Largo da Devesa 3630-253 Penedono Tel. + 351 254 509 030 Fax. + 351 254 509 039 Email: cm.penedono@mail.telepac.pt	0	erro envio mail
Câmara Municipal de Peso da Régua Rua Serpa Pinto, 327 5054-003 Peso da Régua Tel. + 351 254 320 230 Fax. + 351 254 314 365 Email: cmregua@cmpr.pt	1	
Câmara Municipal de Ponte da Barca Praça da República 4980-626 Ponte da Barca		

Nome da Entidade	Enviados	Observações
Tel. + 351 258 480 180 Fax. + 351 258 480 189		
Email: geral@cm-pontedabarca.pt	0	erro envio mail
Câmara Municipal de Ponte de Lima		
Praça da República		
4990-062 Ponte de Lima		
Tel. + 351 258 900 400 Fax. + 351 258 900 410		
Email: geral@cm-pontedelima.pt	1	
Câmara Municipal de Póvoa de Lanhoso		
Av. da República, 1		
4830-513 Póvoa de Lanhoso		
Tel. + 351 253 639 700 Fax. + 351 253 639 709		
Email: geral@mun-planhoso.pt	1	
Câmara Municipal de Póvoa de Varzim		
Praça do Almada		
4490-438 Póvoa de Varzim		
Tel. + 351 252 298 500 Fax. + 351 252 624 828		
Email: pvarzim@cm-pvarzim.pt	1	
Câmara Municipal de Resende		
Av. Rebelo Moniz		
4660-215 Resende		
Tel. + 351 254 877 153 Fax. + 351 254 877 424		
Email: geral@cm-resende.pt	1	
Câmara Municipal de Ribeira de Pena		
Praça do Município		
4870-152 Ribeira de Pena		
Tel. + 351 259 490 500 Fax. + 351 259 493 520		
Email: cmribeirapena@mail.telepac.pt	1	
Câmara Municipal de Sabrosa		
Rua do Loreto		
5060-328 Sabrosa		
Tel. + 351 259 937 120 Fax. + 351 259 937 129		
Email: geral@cm-sabrosa.pt	1	
Câmara Municipal de Santa Marta de Penaguião		
Rua dos Combatentes		
5030-477 Santa Marta de Penaguião		
Tel. + 351 254 810 130 Fax. + 351 254 810 131		
Email: geral@cm-smpenaguiao.pt	1	
Câmara Municipal de São João da Pesqueira		
Av. Marquês do Soveral		
5130-321 São João da Pesqueira		
Tel. + 351 254 489 999 Fax. + 351 254 489 989		
Email: cmsjp@sjpesqueira.pt	1	
Câmara Municipal de Sernancelhe		
Rua Dr. Oliveira Serrão		
3640-240 Sernacelhe		
Tel. + 351 254 598 300 Fax. + 351 254 598 319		
Email: geral@cm-sernancelhe.pt	1	
Câmara Municipal de Tabuaço		
Rua Dr. Ant.º José de Almeida		
5120-423 Tabuaço		

Nome da Entidade	Enviados	Observações
Tel. + 351 254 780 000 Fax. + 351 254 789 142 Email: cm-tabuaco@mail.telepac.pt; geral@cm-tabuaco.pt; cm-tabuaco@cm-tabuaco.pt	1	
Câmara Municipal de Tarouca Av. Dr. Alexandre T. Cardoso 3610-128 Tarouca Tel. + 351 254 678 650 Fax. + 351 254 678 552 Email: camara@cm-tarouca.pt	1	
Câmara Municipal de Terras de Bouro Largo do Município 4840-100 Terras de Bouro Tel. + 351 253 350 010 Fax. + 351 253 351 894 Email: geral@cm-terrasdebouro.pt	1	
Câmara Municipal de Torre de Moncorvo Paços do Concelho 5160-267 Torre de Moncorvo Tel. + 351 279 200 220 Fax. + 351 279 200 240 Email: geral@cm-moncorvo.pt	1	
Câmara Municipal de Vale de Cambra Av. Camilo Tavares de Matos 3730-901 Vale de Cambra Tel. + 351 256 420 510 Fax. + 351 256 420 519 Email: vcambra@cm-vale-cambra.pt	0	erro envio mail
Câmara Municipal de Valença Praça da República 4930-702 Valença Tel. + 351 251 809 500 Fax. + 351 251 809 519 Email: cmv-gap@cm-valenca.pt; cm-valenca@cm-valenca.pt	1	
Câmara Municipal de Valpaços Paços do Concelho 5430-469 Valpaços Tel. + 351 278 710 130 Fax. + 351 278 713 574 Email: sas@valpacos.pt	1	
Câmara Municipal de Vila Flor Av. Marechal Carmona 5360-303 Vila Flor Tel. + 351 278 510 100 Fax. + 351 278 512 380 Email: cm.vila.flor@mail.telepac.pt	1	
Câmara Municipal de Vila Nova da Cerveira Largo do Município 4920-284 Vila Nova de Cerveira Tel. + 351 251 708 020 Fax. + 351 251 708 022 Email: camaracerveira@mail.telepac.pt; gap@cm-vncerveira.pt	1	
Câmara Municipal de Vila Nova de Famalicão Praça Álvaro Marques 4760-502 Vila Nova de Famalicão Tel. + 351 252 320 900 Fax. + 351 252 323 751 Email:camaramunicipal@vilanovadefamalicao.org	1	
Câmara Municipal de Vila Nova de Foz Côa		

Nome da Entidade	Enviados	Observações
Praça do Município 5150-642 Vila Nova de Foz Côa Tel. + 351 279 760 400 Fax. + 351 279 760 438 Email: correio@cm-fozcoa.pt	1	
Câmara Municipal de Vila Pouca de Aguiar Rua Henrique Botelho 5450-020 Vila Pouca de Aguiar Tel. + 351 259 419 100 Fax. + 351 259 419 106 Email: geral-cmvpa@mail.telepac.pt; geral@cm-vpaguiar.pt	1	
Câmara Municipal de Vila Verde Praça do Município 4730-733 Vila Verde Tel. + 351 253 310 500 Fax. + 351 253 312 036 Email: geral@cm-vilaverde.pt	1	
Câmara Municipal de Vimioso Praça Eduardo Coelho 5230-315 Vimioso Tel. + 351 273 518 120 Fax. + 351 273 512 510 Email: gi.cmv@mail.telepac.pt; gi.cmv@cm-vimioso.pt	1	
Câmara Municipal de Vinhais Rua das Freiras 5320-326 Vinhais Tel. + 351 273 770 300 Fax. + 351 273 771 108 Email: c.m.vinhais@mail.telepac.pt; geral@cm-vinhais.pt	1	
34 - EAmb - Esposende Ambiente, EEM Rua da Ribeira 4740-245 Esposende Tel. + 351 253 969 380 Fax. + 351 253 969 385 Email: geral@esposendeambiente.pt	1	
EMARVR - Água e Resíduos de Vila Real, EEM Av. Rainha Sta. Isabel, n.º 1 5000-434 Vila Real Tel. + 351 259 330 800 Fax. + 351 259 321 144 Email: geral@emar-vr.com	1	
EPMAR - Empresa Pública Municipal de Águas Resíduos e Equipamrentos, EM Av. João da Torre, 217 4850-523 Vieira do Minho Tel. + 351 253 646 800 Fax. + 351 253 646 889 Email: epmar.em@gmail.com; info@vieiradominho.pt	1	
INDAQUA Fafe - Gestão de Águas de Fafe, SA Parque 1º de Dezembro 4820-141 Fafe Tel. + 351 253 700 020 Fax. + 351 253 700 026 Email: if@indaquafafe.pt	0	erro envio mail
INDAQUA Feira - Indústria de Águas de Santa Maria da Feria, SA		

Nome da Entidade	Enviados	Observações
Rua Dr. Alcides Strech Monteiro, 17, Apartado 28 4524-909 Santa Maria da Feira Tel. + 351 256 371 500 Fax. + 351 256 371 519 Email: geralfeira@indaquafeira.pt	1	recebido
INDAQUA Matosinhos - Gestão de Águas de Matosinhos, SA Av. Fabril do Norte, 1601 4460-316 Senhora da Hora Tel. + 351 229 393 200 Fax. + 351 229 372 919 Email: geral@indaquamatosinhos.pt	1	
INDAQUA Santo Tirso/Trofa – Gestão de Águas de Santo Tirso e Trofa SA Rua Luís de Camões, 49 4780-497 Santo Tirso Tel. + 351 252 800 600 Fax. + 351 252 800 699 Email: geralstt@indaquastirsotrofa.pt	1	
INDAQUA Vila do Conde - Gestão de Águas de Vila do Conde, SA Praça José Régio, n.º 101 - R/C 4480-718 Vila do Conde Tel. + 351 252 291 220 Fax. + 351 252 291 229 Email: geralvconde@indaquavconde.pt	1	
Penafiel Verde, EM Rua Abílio Miranda - Apartado 94 4560-501 Penafiel Tel. + 351 255 710 130 Fax. + 351 255 710 139 Email: geral@penafielverde.pt	1	
Serviços Municipalizados de Abrantes Via Industrial 1, Lote 65 2200-480 Abrantes Tel. + 351 241 360 120 Fax. + 351 241 360 125 Email: smabrantes@mail.telepac.pt	0	erro envio mail
Serviços Municipalizados de Água de Mirandela Rua Clemente Menéres 5370-321 Mirandela Tel. + 351 278 201 460 Fax. + 351 278 262 303 Email: smamdl.dtecnico@sapo.pt	1	
Serviços Municipalizados de Água e Electricidade e Saneamento de Santo Tirso Rua Dr. José Cardoso Miranda nº18 - Apartado 30 4780-449 Santo Tirso Tel. + 351 252 830 400 Fax. + 351 252 856 473 Email: smaes.tirso@vianw.pt	0	0
Serviços Municipalizados de Electricidade, Água e Saneamento da Maia R. Dr. Carlos Felgueiras 4471-909 Maia Codex Tel. + 351 22 9430800 Fax. + 351 22 9412155 Email: smas-maia@smeas-maia.pt	1	
Serviços Municipalizados de Saneamento Básico de Viana do Castelo		

Nome da Entidade	Enviados	Observações
Rua Frei Bartolomeu dos Mártires, nº 156 4901-878 Viana do Castelo Tel. + 351 258 806 900 Fax. + 351 258 806 990 Email: geral@smsbvc.pt	1	
Trofáguas - Serviços Ambientais, EEM Rua Infante D. Henrique, 307 Bloco E 4785-185 Trofa Tel. + 351 252 450 630 Fax. + 351 252 450 639 Email: geral@trofaguas.pt	1	
VIMÁGUA - Empresa de Água a Saneamento de Guimarães e Vizela, EIM, SA Rua do Rei Pegu, 172 4810-025 Guimarães Tel. + 351 253 439 560 Fax. + 351 253 410 444 Email: vimagua@vimagua .pt	1	

2.2 - Região Centro

Nome da Entidade	Enviados	Observações
Águas da Covilhã, EM Rua Conde da Ericeira 6201-957 Covilhã Tel. + 351 275 310 810 Fax. + 351 275 310 819 Email: geral@aguasdacovilha.pt	1	
Águas da Figueira, S.A. Rua Dr. Mendes Pinheiro, s/n 3080-032 Figueira da Foz Tel. + 351 233 401 450 Fax. + 351 233 422 128 Email: geral@aguasdafigueira.com	1	
Águas da Região de Aveiro, SA Travessa Rua da Paz, 4 3800-587 Aveiro Tel. + 351 234 910 200 Fax. + 351 234 910 299 Email: adra@adra.pt	0	Erro entrega mail
AdS - Águas da Serra, SA Rua Senhora da Estrela, 20 6200-454 Boidobra Tel. + 351 275 313 260 Fax. + 351 275 336 462 Email: aguasdaserra@ags.pt	1	
Águas da Teja, SA Av" Comunidades Europeias N" 39 6420-044 Trancoso Tel. + 351 271 829 000 Fax. + 351 271 829 009 Email: aguasdateja@lusagua.pt	1	
Águas de Coimbra, EEM Rua da Alegria, 111 3000-018 Coimbra		

Nome da Entidade	Enviados	Observações
Tel. + 351 239 096 000 Fax. + 351 239 096 198		
Email: geral@aguasdecoimbra.pt	1	
Águas do Lena, SA		
Lote 10 - Célula B		
2440-118 Batalha		
Tel. + 351 244 764 080 Fax. + 351 244 764 088		
Email: vvicente@lusagua.pt	1	
Águas do Planalto, SA		
Estação de Tratamento de Água		
3460-304 Tondela		
Tel. + 351 232 819 240 Fax. + 351 232 819 259		
Email: aguasdoplanalto@lusagua.pt	1	
AQUAFUNDÁLIA - Águas do Fundão, SA		
Av. Dr. Alfredo Mendes Gil, Mercado Municipal, lj 15/16		
6230-287 Fundão		
Tel. 275771482		
Email: aquafundalia@fcc.es	1	
Câmara Municipal de Aguiar da Beira		
Av. da Liberdade, n.º 21		
3570-018 Aguiar da Beira		
Tel. + 351 232 689 100 Fax. + 351 232 688 894		
Email: geral@cm-aguiardabeira.pt	1	
Câmara Municipal de Almeida		
Praça da Liberdade		
6350-130 Almeida		
Tel. + 351 271 570 022 Fax. + 351 271 570 021		
Email: cmalmeida@mail.telepac.pt	0	erro - envio mail
Câmara Municipal de Alvaiázere		
Rua Conselheiro Furtado Santos		
3250-100 Alvaiázere		
Tel. + 351 236 650 600 Fax. + 351 236 650 609		
Email: camara.alvaiazere@net.pt; geral@cm-alvaiazere.pt	1	
Câmara Municipal de Ansião		
Praça do Município		
3240-143 Ansião		
Tel. + 351 236 670 200 Fax. + 351 236 677 481		
Email: cm.ansiao@mail.telepac.pt; geral@cm-ansiao.pt	0	erro - envio mail
Câmara Municipal de Arganil		
Praça Dr. Simões Dias		
3304-954 Arganil		
Tel. + 351 235 200 150 Fax. + 351 235 200 158		
Email: arganil@cm-arganil.pt	0	erro - envio mail

Nome da Entidade	Enviados	Observações
Câmara Municipal de Batalha Rua Infante D. Fernando 2440-118 Batalha Tel. + 351 244 769 110 Fax. + 351 244 769 111 Email: cmbatalha@mail.telepac.pt; geral@cm-batalha.pt	1	
Câmara Municipal de Belmonte Rua Pedro Álvares Cabral 6250-088 Belmonte Tel. + 351 275 910 010 Fax. + 351 275 910 019 Email: cmbelmonte@mail.telepac.pt	1	
Câmara Municipal de Carregal do Sal Praça do Municipio 3430-909 Carregal do Sal Tel. + 351 232 960 400 Fax. + 351 232 960 409 Email: geral@cm-carregal.pt	1	
Câmara Municipal de Castanheira de Pêra Praça do Visconde 3280-017 Castanheira de Pêra Tel. + 351 236 430 280 Fax. + 351 236 432 307 Email: aguas@cm-castanheiradepera.pt	1	
Câmara Municipal de Castro Daire Rua Dr. Pio Figueiredo, 42 3600-214 Castro Daire Tel. + 351 232 382 214 Fax. + 351 232 382 923 Email: geral@cm-castrodaire.pt	1	
Câmara Municipal de Celorico da Beira Rua Sacadura Cabral 6360-350 Celorico da Beira Tel. + 351 271 747 400 Fax. + 351 271 747 409 Email: geral@cm-celoricodabeira.pt	1	
Câmara Municipal de Condeixa-a-Nova Largo Artur Barreto 3150-124 Condeixa-a-Nova Tel. + 351 239 949 120 Fax. + 351 239 945 445 Email: geral@cm-condeixa.pt	1	
Câmara Municipal de Figueira de Castelo Rodrigo Largo Doutora Vilhena n.º 1 6440-001 Figueira de Castelo Rodrigo Tel. + 351 271 319 000 Fax. + 351 271 319 009 Email: vereadora.cmfcr@gmail.com; cm-fcr@cm-fcr.pt	0	erro no envio mail
Câmara Municipal de Figueiró dos Vinhos Praça do Município		

Nome da Entidade	Enviados	Observações
3260-408 Figueiró dos Vinhos		
Tel. + 351 236 559 550 Fax. + 351 236 552 596		
Email: presidencia@cm-figueirodosvinhos.pt	1	
Câmara Municipal de Fornos de Algodres		
Estrada Nacional, 16		
6370-999 Fornos de Algodres		
Tel. + 351 271 700 060 Fax. + 351 271 700 069		
Email: geral@cm-fornosdealgodres.pt	1	
Câmara Municipal de Fundão		
Praça do Município		
6230-338 Fundão		
Tel. + 351 275 779 060 Fax. + 351 275 779 079		
Email: municipe@cm-fundao.pt; secretaria.gap@cm-fundao.pt	1	
Câmara Municipal de Góis		
Praça da República		
3330-310 Góis		
Tel. + 351 235 770 110 Fax. + 351 235 770 114		
Email: correio@cm-gois.pt	1	
Câmara Municipal de Gouveia		
Av. 25 de Abril		
6290-554 Gouveia		
Tel. + 351 238 490 210 Fax. + 351 238 494 686		
Email: gap@cmgouveia.com	0	erro envio mail
Câmara Municipal de Idanha-a-Nova		
Largo do Município		
6060-163 Idanha-a-Nova		
Tel. + 351 277 200 570 Fax. + 351 277 200 580		
Email: camara@cm.idanhanova.pt	0	erro envio mail
Câmara Municipal de Lousã		
Rua Dr. João Santos		
3200-953 Lousã		
Tel. + 351 239 990 370 Fax. + 351 239 990 381		
Email: geral@cm-lousa.pt	1	
Câmara Municipal de Mação		
Rua Padre António Pereira Figueiredo		
6120-750 Mação		
Tel. + 351 241 577 200 Fax. + 351 241 577 280		
Email: geral@cm_macao.pt - ERRO	0	
Câmara Municipal de Mangualde		
Largo Dr. Couto		
3534-004 Mangualde		
Tel. + 351 232 619 880 Fax. + 351 232 623 958		
Email: cmmangualde@mail.telepac.pt;	1	

Nome da Entidade	Enviados	Observações
geral@cmmangualde.pt		
Câmara Municipal de Manteigas		
Rua 1º de Maio		
6260-101 Manteigas		
Tel. + 351 275 980 000 Fax. + 351 275 982 092		
Email: geral@cm-manteigas.pt	1	
Câmara Municipal de Marinha Grande		
Praça Guilherme Stephens		
2430-960 Marinha Grande		
Tel. + 351 244 573 300 Fax. + 351 244 561 710		
Email: camara.mgrande@mail.telepac.pt; geral@cm-mgrande.pt	1	
Câmara Municipal de Mealhada		
Largo do Município		
3054-001 Mealhada		
Tel. + 351 231 200 980 Fax. + 351 231 203 618		
Email: gabpresidencia@cm-mealhada.pt	1	
Câmara Municipal de Mêda		
Largo do Município		
6430-197 Meda		
Tel. + 351 279 880 040 Fax. + 351 279 882 520		
Email: cmeda@cm-meda.pt	1	
Câmara Municipal de Mira		
Praça da República		
3070-304 Mira		
Tel. + 351 231 480 550 Fax. + 351 231 458 185		
Email: geral@cm-mira.pt	1	
Câmara Municipal de Miranda do Corvo		
Praça José Falcão		
3220-206 Miranda do Corvo		
Tel. + 351 239 530 320 Fax. + 351 239 532 952		
Email: camara@cm-mirandadocorvo.pt	1	
Câmara Municipal de Montemor-o-Velho		
Praça da República		
3140-258 Montemor-o-Velho		
Tel. + 351 239 687 300 Fax. + 351 239 687 318		
Email: geral@cm-montemorvelho.pt	1	
Câmara Municipal de Mortágua		
Rua Dr. João Lopes Morais		
3450-153 Mortágua		
Tel. + 351 231 927 460 Fax. + 351 231 927 469		
Email: mortagua@cm-mortagua.pt	1	
Câmara Municipal de Nelas		
Praça do Município		

Nome da Entidade	Enviados	Observações
3520-001 Nelas		
Tel. + 351 232 941 300 Fax. + 351 232 940 899		
Email: geral@cm-nelas.pt	1	
Câmara Municipal de Oleiros		
Praça do Município		
6160-409 Oleiros		
Tel. + 351 272 680 130 Fax. + 351 272 682 446		
Email: cmoleiros@netc.pt; geral@cm-oleiros.pt	1	
Câmara Municipal de Oliveira de Frades		
Largo Dr. Joaquim de Almeida		
3680-111 Oliveira de Frades		
Tel. + 351 232 760 300 Fax. + 351 232 761 727		
Email: cmofrades@mail.telepac.pt	1	
Câmara Municipal de Oliveira do Hospital		
Largo Conselheiro Cabral Metello		
3400-062 Oliveira do hospital		
Tel. + 351 238 605 250 Fax. + 351 238 609 739		
Email: geral@cm-oliveiradohospital.pt	1	
Câmara Municipal de Pampilhosa da Serra		
Rua Rangel de Lima		
3320-229 Pampilhosa da Serra		
Tel. + 351 235 590 320 Fax. + 351 235 590 329		
Email: cmapps@mail.telepac.pt, municipio@cm-pampilhosadaserra.pt	1	
Câmara Municipal de Pedrógão Grande		
A Devesa		
3271-909 Pedrógão Grande		
Tel. + 351 236 480 150 Fax. + 351 236 480 159		
Email: geral@cm-pedrogaogrande.pt	1	
Câmara Municipal de Penacova		
Largo Alberto Leitão, 5		
3360-191 Penacova		
Tel. + 351 239 470 300 Fax. + 351 239 478 098		
Email: cmp@aircnet.airc.pt	0	erro envio mail
Câmara Municipal de Penalva do Castelo		
Avenida Castendo		
3550-185 Penalva do Castelo		
Tel. + 351 232 640 020 Fax. + 351 232 640 022		
Email: geral@cm-penalvadocastelo.pt	1	
Câmara Municipal de Penamacor		
Largo do Município		
6090-543 Penamacor		
Tel. + 351 277 394 106 Fax. + 351 277 394 196		
Email: serv.urb.ambiente@cm-penamacor.pt		

Nome da Entidade	Enviados	Observações
Câmara Municipal de Penela Praça do Município 3230-253 Penela		
Tel. + 351 239 560 120 Fax. + 351 239 569 400		
Email: cmpenela@cm-penela.pt	1	
Câmara Municipal de Pinhel Travessa Portão Norte, nº 2 6400-303 Pinhel		
Tel. + 351 271 410 000 Fax. + 351 271 413 388		
Email: cm-pinhel@cm-pinhel.pt	1	
Câmara Municipal de Pombal Largo do Cardal 3100-440 Pombal		
Tel. + 351 236 210 500 Fax. + 351 236 210 599		
Email: geral@cm-pombal.pt	1	
Câmara Municipal de Porto de Mós Praça do Município 2480-851 Porto de Mós		
Tel. + 351 244 499 600 Fax. + 351 244 499 601		
Email: geral@municipio-portodemos.pt	1	
Câmara Municipal de Proença-a-Nova Largo Dr. Pedro da Fonseca 6150-518 Proença-a-Nova		
Tel. + 351 274 670 000 Fax. + 351 274 672 697		
Email: geral@cm-proencanova.pt	1	
Câmara Municipal de Sabugal Praça da República 6324-007 Sabugal		
Tel. + 351 271 751 040 Fax. + 351 271 753 408		
Email: cm-sabugal@domdigital.pt; geral@cm-sabugal.pt	1	
Câmara Municipal de Santa Comba Dão Largo do Município, 13 3440-337 Santa Comba Dão		
Tel. + 351 232 880 500 Fax. + 351 232 881 436		
Email: geral@cm-santacombadao.pt	1	
Câmara Municipal de São Pedro do Sul Largo de Camões 3660-436 São Pedro do Sul		
Tel. + 351 232 723 003 Fax. + 351 232 723 406		
Email: geral@cm-spsul.pt	1	
Câmara Municipal de Sátão Praça Paulo VI 3560-154 Sátão		

Nome da Entidade	Enviados	Observações
Tel. + 351 232 980 000 Fax. + 351 232 982 093		
Email: cm.satao@mail.telepac.pt; geral@cm-satao.pt	1	
Câmara Municipal de Seia		
Largo Dr. António Borges Pires		
6270-494 Seia		
Tel. + 351 238 310 230 Fax. + 351 238 310 232		
Email: cm-seia@cm-seia.pt	1	
Câmara Municipal de Sertã		
Largo do Município		
6100-738 Sertã		
Tel. + 351 274 600 300 Fax. + 351 274 600 301		
Email: cmsgeral@cm-serta.pt	1	
Câmara Municipal de Soure		
Praça da República		
3130-218 Soure		
Tel. + 351 239 506 550 Fax. + 351 239 502 951		
Email: geral@cm-soure.pt	1	
Câmara Municipal de Tábua		
Largo da Câmara		
3420-308 Tábua		
Tel. + 351 235 410 340 Fax. + 351 235 413 025		
Email: geral@cm-tabua.pt	1	
Câmara Municipal de Tondela		
Largo da República, nº. 16		
3464-001 Tondela		
Tel. + 351 232 811 110 Fax. + 351 232 811 120		
Email: cmtondela@mail.telepac.pt	1	
Câmara Municipal de Vila de Rei		
Praça Família Mattos e Silva Neves		
6110-174 Vila de Rei		
Tel. + 351 274 890 010 Fax. + 351 274 890 018		
Email: ambiente@cm-viladerei.pt; geral@cm-viladerei.pt	1	
Câmara Municipal de Vila Nova de Paiva		
Praça D. Afonso Henriques, 1		
3650-207 Vila Nova de Paiva		
Tel. + 351 232 609 900 Fax. + 351 232 609 909		
Email: geral@cm-vnpaiva.pt; ambiente@cm-vnpaiva.pt	1	
Câmara Municipal de Vila Nova de Poiares		
Largo da República		
3350-156 Vila Nova de Poiares		
Tel. + 351 239 420 850 Fax. + 351 239 421 800		

Nome da Entidade	Enviados	Observações
Email: cmvnp@mail.telepac.pt	1	
Câmara Municipal de Vila Velha de Ródão Rua de Santana 6030-230 Vila Velha de Ródão		
Tel. + 351 272 540 300 Fax. + 351 272 540 301		
Email: camara.rodao@mail.telepac.pt; geral@cm-vvrodao.pt	1	
Câmara Municipal de Vouzela Alameda D. Duarte de Almeida 3670-250 Vouzela		
Tel. + 351 232 740 740 Fax. + 351 232 771 513		
Email: geral@cm-vouzela.pt	1	
ICOVI, Infra-estruturas e Concessões da Covilhã, EEM Avenida Viriato, n.º 194 6200-722 Tortosendo		
Tel. + 351 275 950 531 Fax. + 351 275 950 533		
Email: geral@icovi.pt	0	erro envio mail
INOVA - Empresa de Desemvolvimento Económico e Social de Cantanhede, EM Zona Industrial de Cantanhede 3064-909 Cantanhede		
Tel. + 351 231 410 830 Fax. + 351 231 410 839		
Email: geral@inova-em.pt	1	
Serviços Municipalizados de Água e Saneamento de Anadia Praça do Município 3780-102 Anadia		
Tel. + 351 231 510 540 Fax. + 351 231 510 549		
Email: smasgeral@cm-anadia.pt	1	
Serviços Municipalizados de Água e Saneamento de Guarda Largo de S. Vicente, 7 6300-600 Guarda		
Tel. + 351 271 232 740 Fax. + 351 271 232 749		
Email: dpea@mun-guarda.pt; geral@smasguarda.com	1	
Serviços Municipalizados de Água e Saneamento de Leiria Rua da Cooperativa, nº65 C S. Romão 2410-256 Leiria		
Tel. + 351 244 817 300 Fax. + 351 244 817 301		
Email: geral@smas-leiria.pt	1	
Serviços Municipalizados de Água e Saneamento de Viseu R. Conselheiro Afonso de Melo 3510-024 Viseu		
Tel. + 351 232 470 670 Fax. + 351 232 424 080		

Nome da Entidade	Enviados	Observações
Email: geral@smasviseu.pt	1	
Serviços Municipalizados de Castelo Branco Av. Nuno Alvares, 32 - r/c 6000-083 Castelo Branco		
Tel. + 351 272 340 500 Fax. + 351 272 340 501		
Email: geral@sm-castelobranco.pt	1	

2.3- Região Lisboa e Vale do Tejo

Nome da Entidade	Enviados	Observações
Serviços Municipalizados de Água e Saneamento de Sintra	1	Enviados a todos os elementos do CA, dirigentes e funcionários
Abrantaqua - Serviço de Águas Residuais Urbanas do Município de Abrantes, SA Rua do Comércio, 29 2200-050 Abrantes		
Tel. + 351 241 331 562 Fax. + 351 241 331 570		
Email: geral@abrantaqua.pt	1	
Águas da Azambuja, SA Rua Teodoro José da Silva, 37 2050-335 Azambuja		
Tel. + 351 263 001 920 Fax. + 351 263 001 929		
Email: geral@aguasdaazambuja.pt	1	
Águas de Alenquer, SA Rua Sacadura Cabral, 22 C - R/C 2580-371 Alenquer		
Tel. + 351 263 731 210 Fax. + 351 263 731 219		
Email: geral@aguasdealenquer.pt	1	
Águas de Cascais, SA Avenida do Ultramar, 210 2754-525 Cascais		
Tel. + 351 214 838 300 Fax. + 351 214 838 379		
Email: geral@aguasdecascais.pt	1	
Águas de Santarém, EM, SA Praça Visconde Serra do Pilar 2001-904 Santarém		
Tel. + 351 243 305 050 Fax. + 351 243 305 051		
Email: geral@aguasdesantarem.pt	1	
Águas do Ribatejo, EIM Rua Gaspar Costa Ramalho, 38 2120-098 Salvaterra de Magos		
Tel. + 351 263 509 400 Fax. + 351 263 509 499		
Email: geral@aguasdoribatejo.com	1	

Nome da Entidade	Enviados	Observações
Águas do Sado, SA Av. Luisa Todi, 287 2900-464 Setúbal Tel. + 351 707 109 019 Fax. + 351 265 549 340 Email: geral@aguasdosado.pt	1	
AUSTRA - Associação de Utilizadores do Sistema de Águas Residuais de Alcanena Lagar do Freixo - Apartado 762384-909 Alcanena 2384 - 909 Alcanena Tel. + 351 249 881 338 Fax. + 351 249 891 531 Email: austra@mail.telepac.pt	1	
Câmara Municipal de Alcanena Praça 8 de Maio 2380-037 Alcanena Tel. + 351 249 889 010 Fax. + 351 249 891 357 Email: geral@cm-alcanena.pt	1	
Câmara Municipal de Alcochete Largo de S. João Baptista 2894-001 Alcochete Tel. + 351 212 348 600 Fax. + 351 212 348 690 Email: geral@cm-alcochete.pt	1	
Câmara Municipal de Arruda dos Vinhos Praça Miguel Bombarda 2630-269 Arruda dos Vinhos Tel. + 351 263 977 000 Fax. + 351 263 977 002 Email: cm-arruda@cm-arruda.pt	1	
Câmara Municipal de Barreiro Rua Miguel Bombarda 2830-355 Barreiro Tel. + 351 212 068 000 Fax. + 351 212 068 001 Email: dirp@cm-barreiro.pt	1	
Câmara Municipal de Bombarral Largo do Município 2540-046 Bombarral Tel. + 351 262 609 021 Fax. + 351 262 609 041 Email: pij.bombarral@mail.telepac.pt;	0	0
Câmara Municipal de Cadaval Av. Dr. Francisco Sá Carneiro 2550-103 Cadaval Tel. + 351 262 690 100 Fax. + 351 262 695 270 Email: geral@cm-cadaval.pt	1	
Câmara Municipal de Constância Estrada Nacional, 3 2250-909 Constância		

Nome da Entidade	Enviados	Observações
Tel. + 351 249 730 050 Fax. + 351 249 739 514		
Email: cmconstancia@mail.telepac.pt; geral@cm-constancia.pt	1	
Câmara Municipal de Entroncamento		
Largo José Duarte Coelho		
2330-078 Entroncamento		
Tel. + 351 249 720 400 Fax. + 351 249 718 615		
Email: financeira@cm-entroncamento.pt	0	0
Câmara Municipal de Ferreira do Zêzere		
Praça Dias Ferreira		
2240-341 Ferreira do Zêzere		
Tel. + 351 249 360 150 Fax. + 351 249 360 169		
Email: geral@cm-ferreiradozezere.pt	1	
Câmara Municipal de Golegã		
Largo D. Manuel I		
2150-128 Golegã		
Tel. + 351 249 979 050 Fax. + 351 249 979 059		
Email: camara.golega@mail.telepac.pt; geral@cm-golega.pt	1	
Câmara Municipal de Lisboa		
Praça do Município		
1100-365 Lisboa		
Tel. + 351 213 227 000 Fax. + 351 213 227 018		
Email: geral@cm-lisboa.pt	1	0
Câmara Municipal de Nazaré		
Avenida Vieira Guimarães, 54		
2450-951 Nazaré		
Tel. + 351 262 550 010 Fax. + 351 262 550 019		
Email: sua@cm-nazare.pt	1	
Câmara Municipal de Óbidos		
Largo de S. Pedro		
2510-086 Óbidos		
Tel. + 351 262 955 500 Fax. + 351 262 955 501		
Email: c.m.obidos@mail.telepac.pt; geral@cm-obidos.pt	1	
Câmara Municipal de Ourém		
Praça do Município, 11		
2490-499 Ourém		
Tel. + 351 249 540 900 Fax. + 351 249 540 908		
Email: geral@mail.cm-ourem.pt	1	vai responder - encaminhou mail para as TI
Câmara Municipal de Palmela		
Largo do Município		
2951-505 Palmela		

Nome da Entidade	Enviados	Observações
Tel. + 351 212 336 600 Fax. + 351 212 336 659 Email: cmpalmela@mail.telepac.pt; geral@cm-palmela.pt **Câmara Municipal de Rio Maior** Praça da República 2040-320 Rio Maior Tel. + 351 243 999 300 Fax. + 351 243 992 236 Email: cmriomaior@mail.telepac.pt **Câmara Municipal de Sardoal** Praça da República 2230-139 Sardoal Tel. + 351 241 850 000 Fax. + 351 241 855 684 Email: geral@cm-sardoal.pt **Câmara Municipal de Seixal** Alameda dos Bombeiros Voluntários, n.º 45 2844-001 Seixal Tel. + 351 212 276 700 Fax. + 351 212 276 701 Email: cmseixal@mail.telepac.pt; geral@cm-seixal.pt **Câmara Municipal de Sesimbra** Rua da República, 3 2970-741 Sesimbra Tel. + 351 212 288 500 Fax. + 351 212 288 517 Email: cmsesimbra@mun-sesimbra.pt; girp@cm-sesimbra.pt **Câmara Municipal de Sobral de Monte Agraço** Praça Dr. Eugênio Dias 2590-016 Sobral de Monte Agraço Tel. + 351 261 940 300 Fax. + 351 261 940 310 Email: geral@cm-sobral.pt **Câmara Municipal de Torres Novas** Rua General António César Vasconcelos Correia 2350-421 Tores Novas Tel. + 351 249 839 430 Fax. + 351 249 811 780 Email: geral@cm-torresnovas.pt **Câmara Municipal de Vila Nova da Barquinha** Praça da República 2260-411 Vila Nova da Barquinha Tel. + 351 249 720 350 Fax. + 351 249 720 368 Email: geral@cm-vnbarquinha.pt **Cartágua - Águas do Cartaxo, SA** Zona Industrial do Cartaxo - Lote 20 2070-681 Vila Chã de Ourique Tel. + 351 243 750 110 Fax. +351 243 750 111	1 1 1 1 1 1 1	

Nome da Entidade	Enviados	Observações
Email: geral@cartagua.pt	1	
Compagnie Générale des Eaux - Mafra Rua Constância Maria Rodrigues, n º 19 2644-013 Mafra		
Tel. + 351 261 816 650 Fax. + 351 261 816 659		
Email: AGUAS.MAFRA@VEOLIAAGUA.COM.PT	1	
Compagnie Générale des Eaux - Ourém Rua Dr. Carlos Vaz Faria de Almeida, 21 - R/C 2490-547 Ourém		
Tel. + 351 249 540 010 Fax. + 351 249 540 022		
Email: aguas.ourem@veoliaagua.com.pt	1	
EPAL - Empresa Portuguesa de Águas Livres, SA Av. da Liberdade, 24 1250-144 Lisboa		
Tel. + 351 213 251 000 Fax. + 351 213 251 397		
Email: epal@epal.pt	1	
Luságua Alcanena - Gestão de Águas, S.A. Rua Monte Branco, n.º 136 2380-057 Alcanena		
Tel. + 351 249 889 320 Fax. + 351 249 889 329		
Email: alcanena@lusagua.pt	1	
Serviços Municipalizados de Água e Saneamento de Almada Praceta Ricardo Jorge, nº2 2800-709 Almada		
Tel. + 351 212 726 000 Fax. + 351 212 741 629		
Email: geral@smasalmada.pt	1	
Serviços Municipalizados de Água e Saneamento de Caldas da Rainha Prç. 25 de Abril 2500-110 Caldas da Rainha		
Tel. + 351 262 240 002 Fax. + 351 262 839 728		
Email: geral@smas-caldas-rainha.pt	1	
Serviços Municipalizados de Água e Saneamento de Montijo Av. dos Pescadores 2870-114 Montijo		
Tel. + 351 212 327 768 Fax. + 351 212 327 708		
Email: smas.montijo@mun-montijo.pt	1	
Serviços Municipalizados de Água e Saneamento de Oeiras e Amadora Av. Dr. Francisco Sá Carneiro, 19 2784-541 Oeiras		
Tel. + 351 214 400 600 Fax. + 351 214 400 601		
Email: labdcq@smas-oeiras-amadora.pt	1	
Serviços Municipalizados de Água e Saneamento de Peniche		

Nome da Entidade	Enviados	Observações
Rua 13 de Infantaria, 19-21 2520-256 Peniche Tel. + 351 262 780 050 Fax. + 351 262 784 049 Email: smaspeniche@cm-peniche.pt	1	
Serviços Municipalizados de Água e Saneamento de Tomar Praça da República, 4 2304-909 Tomar Tel. + 351 249 329 890 Fax. + 351 249 321 671 Email: geral@smastomar.pt	1	
Serviços Municipalizados de Água e Saneamento de Torres Vedras Rua da Electricidade 2560-316 Torres Vedras Tel. + 351 261 336 500 Fax. + 351 261 336 502 Email: geral@smastv.pt	1	
Serviços Municipalizados de Água e Saneamento de Vila Franca de Xira Av. Pedro Vitor, 5 2600-221 Vila Franca de Xira Tel. + 351 263 200 600 Fax. + 351 263 200 628 Email: administracao@smas.vfxira.pt	0	0
Serviços Municipalizados de Alcobaça Rua da Liberdade 2460-060 Alcobaça Tel. + 351 262 580 900 Fax. + 351 262 580 905 Email: geral@smalcobaca.pt	1	
Serviços Municipalizados de Loures Rua Ilha da Madeira, 2 2674-504 Loures Tel. + 351 219 848 500 Fax. + 351 219 848 585 Email: scii@smas-loures.pt; geral@smas-loures.pt	1	
Serviços Municipalizados de Nazaré Av. Vieira Guimarães 2450-951 Nazaré Tel. + 351 262 561 153 Fax. + 351 262 568 442 Email: geral.smnazare@mail.telepac.pt	1	

2.4- Região Alentejo

Nome da Entidade	Enviados	Observações
Águas de Santo André, SA Cerca da Água - Rua dos Cravos 7500-999 Vila Nova de Santo André Tel. + 351 269 708 240 Fax. + 351 269 708 269 Email: geral@aguasdesantoandre.com.pt	1	
Aquamaior, Águas de Campo Maior, SA		

Nome da Entidade	Enviados	Observações
Rua de S. João, 2 A 7370-202 Campo Maior Tel. + 351 268 689 309 Fax. + 351 268 689 312 Email: Cagoncalvesp@fcc.es	1	
Câmara Municipal de Alandroal Praça da República 7250-116 Alandroal Tel. + 351 268 440 040 Fax. + 351 268 440 041 Email: cm-alandroal@mail.telepac.pt	1	
Câmara Municipal de Alcacér do Sal Largo Pedro Nunes 7580-125 Alcacér do Sal Tel. + 351 265 610 040 Fax. + 351 265 610 059 Email: geral@cm-alcacerdosal.pt	0	erro envio mail
Câmara Municipal de Aljustrel Av. 1º de Maio 7600-010 Aljustrel Tel. + 351 284 600 070 Fax. + 351 284 602 055 Email: cma.gap@mail.telepac.pt; geral@mun-aljustrel.pt	0	erro envio mail
Câmara Municipal de Almodôvar Rua Serpa Pinto 7700-081 Almodôvar Tel. + 351 286 660 600 Fax. + 351 286 662 282 Email: cm-almodovar@cm-almodovar.pt	0	erro envio mail
Câmara Municipal de Alter do Chão Largo do Município 7440-026 Alter do Chão Tel. + 351 245 610 000 Fax. + 351 245 612 431 Email: cm.alterchao@mail.telepac.pt; geral@cm-alter-chao.pt	1	
Câmara Municipal de Alvito Largo do Relógio, 1 7920-022 Alvito Tel. + 351 284 480 800 Fax. + 351 284 485 157 Email: geral@cm-alvito.pt	1	
Câmara Municipal de Arraiolos Praça Lima e Brito 7040-027 Arraiolos Tel. + 351 266 490 240 Fax. + 351 266 490 257 Email: vmarques@cm-arraiolos.pt	1	
Câmara Municipal de Arronches Praça da República 7340-012 Arronches		

Nome da Entidade	Enviados	Observações
Tel. + 351 245 580 080 Fax. + 351 245 580 081 Email: np58gg@mail.telepac.pt; geral@cm-arronches.pt	1	
Câmara Municipal de Avis Largo Cândido dos Reis 7480-999 Avis Tel. + 351 242 410 060 Fax. + 351 242 410 099 Email: geral@cm-avis.pt	1	
Câmara Municipal de Barrancos Praça do Município, 2 7230-030 Barrancos Tel. + 351 285 950 630 Fax. + 351 285 950 638 Email: geral@cm-barrancos.pt	1	
Câmara Municipal de Borba Praça da República 7150-999 Borba Tel. + 351 268 891 630 Fax. + 351 268 894 806 Email: cmborba@mail.telepac.pt	0	erro envio mail
Câmara Municipal de Castelo de Vide Rua Bartolomeu Álvares Santa 7320-117 Castelo de Vide Tel. + 351 245 908 220 Fax. + 351 245 901 827 Email: cm.castvide@mail.telepac.pt	1	
Câmara Municipal de Castro Verde Praça do Município 7780-217 Castro Verde Tel. + 351 286 320 700 Fax. + 351 286 320 709 Email: geral@cm-castroverde.pt	1	
Câmara Municipal de Crato Praça do Município 7430-999 Crato Tel. + 351 245 990 111 Fax. + 351 245 996 679 Email: direccao@cm-crato.pt	1	
Câmara Municipal de Cuba Rua Serpa Pinto, 84 7940-172 Cuba Tel. + 351 284 419 900 Fax. + 351 284 415 137 Email: geral@cm-cuba.pt	1	
Câmara Municipal de Estremoz Rossio Marquês de Pombal 7100-513 Estremoz Tel. + 351 268 339 200 Fax. + 351 268 334 010 Email: ambiente@cm-estremoz.pt	1	

Nome da Entidade	Enviados	Observações
Câmara Municipal de Évora Praça do Sertório 7000-506 Évora Tel. + 351 266 777 000 Fax. + 351 266 777 161 Email: cmevora@mail.evora.net	1	
Câmara Municipal de Ferreira do Alentejo Praça Comendador Infante Passanha, 5 7900-571 Ferreira do Alentejo Tel. + 351 284 738 700 Fax. + 351 284 739 250 Email: geral@cm-ferreira-alentejo.pt	1	
Câmara Municipal de Fronteira Praça do Município 7460-110 Fronteira Tel. + 351 245 600 070 Fax. + 351 245 600 099 Email: cmfronteira@mail.pt; municipio@cm-fronteira.pt	1	
Câmara Municipal de Gavião Largo do Município 6040-102 Gavião Tel. + 351 241 639 070 Fax. + 351 241 632 190 Email: cmg.md@mail,telepac.pt; geral@cm-gaviao.pt	1	
Câmara Municipal de Grândola Rua Dr. José Pereira Barradas 7570-281 Grândola Tel. + 351 269 450 000 Fax. + 351 269 442 699 Email: aguas@cm-grandola.pt	1	
Câmara Municipal de Marvão Largo Santa Maria 7330-101 Marvão Tel. + 351 245 909 130 Fax. + 351 245 993 526 Email: geral@cm-marvao.pt	1	
Câmara Municipal de Mértola Praça Luís de Camões 7750-329 Mértola Tel. + 351 286 610 100 Fax. + 351 286 610 101 Email: geral@cm-mertola.pt	1	
Câmara Municipal de Monforte Praça da República 7450-115 Monforte Tel. + 351 245 578 060 Fax. + 351 245 573 423 Email: aguas.cmmonforte@mail.telepac.pt	1	
Câmara Municipal de Montemor-o-Novo Largo dos Paços do Concelho		

Nome da Entidade	Enviados	Observações
7050-127 Montemor-o-Novo Tel. + 351 266 898 100 Fax. + 351 266 898 190 Email: cmmontemor@cm-montemornovo.pt	1	
Câmara Municipal de Mora Rua do Município 7490-243 Mora Tel. + 351 266 439 070 Fax. + 351 266 403 260 Email: cmmora@mail.telepac.pt	1	
Câmara Municipal de Moura Praça Sacadura Cabral 7860-207 Moura Tel. + 351 285 250 400 Fax. + 351 285 251 702 Email: cmmoura@cm-moura.pt	1	
Câmara Municipal de Mourão Praça da República, 20 7240-233 Mourão Tel. + 351 266 560 010 Fax. + 351 266 560 025 Email: gap@cm-mourao.pt	0	erro envio mail
Câmara Municipal de Nisa Praça do Município 6050-358 Nisa Tel. + 351 245 410 000 Fax. + 351 245 412 799 Email: nisa@cm-nisa.pt	0	erro envio mail
Câmara Municipal de Odemira Praça da República 7630-139 Odemira Tel. + 351 283 320 900 Fax. + 351 283 327 323 Email: ambiente@cm-odemira.pt; geral@cm-odemira.pt	1	
Câmara Municipal de Ourique Av. 25 de Abril 7670-281 Ourique Tel. + 351 286 510 030 Fax. + 351 286 510 040 Email: cmourique@mail.telepac.pt; geral@cmourique.pt	1	
Câmara Municipal de Ponte de Sôr Largo 25 de Abril 7400-288 Ponte de Sôr Tel. + 351 242 291 580 Fax. + 351 242 292 589 Email: cm-pontedesor@clix.pt; geral@cm-pontedesor.pt	1	
Câmara Municipal de Portalegre Praça do Município 7300-110 Portalegre		

Nome da Entidade	Enviados	Observações
Tel. + 351 245 307 400 Fax. + 351 245 330 235		
Email: municipio@cm-portalegre.pt	1	
Câmara Municipal de Portel		
Praça D. Nuno Alvares Pereira, 4		
7220-375 Portel		
Tel. + 351 266 619 030 Fax. + 351 266 611 347		
Email: geral@mail.cm-portel.pt	1	
Câmara Municipal de Redondo		
Praça da República		
7170-011 Redondo		
Tel. + 351 266 989 210 Fax. + 351 266 909 039		
Email: geral@cm-redondo.pt	1	
Câmara Municipal de Reguengos de Monsaraz		
Praça da Liberdade		
7200-370 Reguengos de Monsaraz		
Tel. + 351 266 508 040 Fax. + 351 266 508 059		
Email: geral@cm-reguengos-monsaraz.pt	1	mail encaminhado dentro da organização
Câmara Municipal de Santiago do Cacém		
Praça do Município		
7540-136 Santiago do Cacém		
Tel. + 351 269 829 400 Fax. + 351 269 829 498		
Email: geral@cm-santiagocacem.pt; dasb@cm-santiagocacem.pt	1	
Câmara Municipal de Serpa		
Praça da República		
7830-389 Serpa		
Tel. + 351 284 540 100 Fax. + 351 284 540 109		
Email: geral@cm-serpa.pt	1	
Câmara Municipal de Sines		
Largo João de Deus		
7520-159 Sines		
Tel. + 351 269 630 607 Fax. + 351 269 636 146		
Email: info@mun-sines.pt	1	
Câmara Municipal de Sousel		
Praça da República, 1		
7470-220 Sousel		
Tel. + 351 268 550 100 Fax. + 351 268 550 110		
Email: geral@cm-sousel.pt	1	
Câmara Municipal de Vendas Novas		
Praça da República		
7080-099 Vendas Novas		
Tel. + 351 265 807 700 Fax. + 351 265 892 152		

Nome da Entidade	Enviados	Observações
Email: geral@cm-vendasnovas.pt	1	
Câmara Municipal de Viana do Alentejo Rua Brito Camacho, 13 7090-237 Viana do Alentejo Tel. + 351 266 930 010 Fax. + 351 266 930 019		
Email: camara@cm-vianadoalentejo.pt	1	
Câmara Municipal de Vidigueira Praça da República 7960-225 Vidigueira Tel. + 351 284 437 400 Fax. + 351 284 436 110		
Email: geral@cm-vidigueira.pt	1	
Câmara Municipal de Vila Viçosa Praça da República 7160-207 Vila Viçosa Tel. + 351 268 889 310 Fax. + 351 268 980 604		
Email: geral@cm-vilavicosa.pt	1	
EMAS - Empresa Municipal de Água e Saneamento de Beja, E.E.M. Rua Conde da Boavista, 16 7800-456 Beja Tel. + 351 284 313 450 Fax. + 351 284 313 459		
Email: geral@emas-beja.pt	1	
Serviços Municipalizados de Águas e Transportes de Portalegre Rua Guilherme Gomes Fernandes, n.º 28 7300-186 Portalegre Tel. + 351 245 307 401 Fax. + 351 245 307 475		
Email: smatp@cm-portalegre.pt	1	

2.5- Região Algarve

Nome da Entidade	Enviados	Observações
Câmara Municipal de Albufeira Cerro da Alagoa 8200-863 Albufeira Tel. + 351 289 599 500 Fax. + 351 289 599 511		
Email: geral@cm-albufeira.pt	1	
Câmara Municipal de Alcoutim Praça do Município, 12 8970-066 Alcoutim Tel. + 351 281 540 500 Fax. + 351 281 546 363		
Email: cmalcoutim@hotmail.com; geral@cm-alcoutim.pt	1	
Câmara Municipal de Aljezur Rua Capitão Salgueiro Maia		

Nome da Entidade	Enviados	Observações
8670-005 Aljezur Tel. + 351 282 990 010 Fax. + 351 282 990 011 Email: cm.aljezur@mail.telepac.pt; geral@cm-aljezur.pt	1	
Câmara Municipal de Castro Marim Rua Dr. José Alves Moreira, 10 8950-138 Castro Marim Tel. + 351 281 510 740 Fax. + 351 281 510 743 Email: camara@cm-castromarim.pt	1	
Câmara Municipal de Lagoa Largo do Município 8400-851 Lagoa Tel. + 351 282 380 400 Fax. + 351 282 341 416 Email: expediente@cm-lagoa.pt	1	
Câmara Municipal de Lagos Edifício Paços do Concelho Séc. XXI, Praça do Município 8600-293 Lagos Tel. + 351 282 780 060 Fax. + 351 282 769 317 Email: expediente.geral@cm-lagos.pt	1	
Câmara Municipal de Loulé Praça da República 8100-951 Loulé Tel. + 351 289 400 600 Fax. + 351 289 415 557 Email: cmloule@cm-loule.pt	1	
Câmara Municipal de Monchique Travessa da Portela, 2 8551-951 Monchique Tel. + 351 282 910 200 Fax. + 351 282 912 810 Email: geral@cm-monchique.pt	1	
Câmara Municipal de Olhão Largo Sebastião Martins Mestre 8700-349 Olhão Tel. + 351 289 700 100 Fax. + 351 289 700 111 Email: camaraolhao@mail.telepac.pt; geral@cm-olhao.pt	1	
Câmara Municipal de São Brás de Alportel Rua Gago Coutinho, 1 8150-151 São Brás de Alportel Tel. + 351 289 840 000 Fax. + 351 289 842 455 Email: geral@cm-sbras.pt	1	
Câmara Municipal de Silves Praça do Município 8300-117 Silves		

Nome da Entidade	Enviados	Observações
Tel. + 351 282 440 800 Fax. + 351 282 440 850		
Email: presidente@cm-silves.pt	0	caixa cheia
Câmara Municipal de Vila do Bispo		
Praça do Município		
8650-407 Vila do Bispo		
Tel. + 351 282 630 600 Fax. + 351 282 639 208		
Email: geral@cm-viladobispo.pt	1	
EMARP - Empresa Municipal de Águas e Resíduos de Portimão, EEM		
R. José António Marques, 17		
8501-953 Portimão		
Tel. + 351 282 400 260 Fax. + 351 282 400 269		
Email: geral@emarp.pt	1	
FAGAR - Faro, Gestão de Águas e Resíduos, EM		
Rua Prof. Norberto Silva, 8		
8004-002 Faro		
Tel. + 351 289 860 900 Fax. + 351 289 860 919		
Email: mail@fagar.pt	1	
Tavira Verde, Empresa Municipal de Ambiente, EM		
Rua 25 de Abril, 1 - r/c - Esq.		
8800-427 Tavira		
Tel. + 351 281 380 620 Fax. + 351 281 380 629		
Email: geral@taviraverde.pt	1	
VRSA Sociedade de Gestão Urbana, EM, SA		
Rua José Barão, 4 - 1º - Apartado 30		
8900-316 Vila Real de Santo António		
Tel. + 351 281 510 020 Fax. + 351 281 541 144		
Email: sgu@sgu.cm-vrsa.pt	1	

2.6 - Região Autónoma dos Açores

Nome da Entidade	Enviados	Observações
Câmara Municipal de Calheta		
Rua 25 de Abril		
9850-032 Calheta		
Tel. + 351 295 416 324 Fax. + 351 295 416 437		
Email: cmcalheta@hotmail.com	0	0
Câmara Municipal de Corvo		
Rua Jogo da Bola		
9980-024 Corvo		
Tel. + 351 292 590 200 Fax. + 351 292 596 120		
Email: cmc.nelia@mail.telepac.pt	1	
Câmara Municipal de Horta		

Nome da Entidade	Enviados	Observações
Largo Duque d'Ávila e Bolama 9900-997 Horta Tel. + 351 292 202 000 Fax. + 351 292 293 990 Email: geral@cmhorta.pt	1	
Câmara Municipal de Lagoa (Açores) Largo D. João III - Santa Cruz 9560-045 Lagoa Tel. + 351 296 960 600 Fax. + 351 296 916 229 Email: cmlagoa.az@mail.telepac.pt	1	
Câmara Municipal de Lajes das Flores Av. Peixoto Pimentel 9960-431 Lajes das Flores Tel. + 351 292 590 800 Fax. + 351 292 590 826 Email: geral@cmlflores.raacores.net	0	erro envio mail
Câmara Municipal de Lajes do Pico Convento de São Francisco Rua São Francisco 9930-135 Lajes do Pico Tel. + 351 292 679 700 Fax. + 351 292 679 710 Email: cmlpico@mail.telepac.pt	1	
Câmara Municipal de Madalena Largo Cardeal Costa Nunes 9950-324 Madalena Tel. + 351 292 628 700 Fax. + 351 292 622 740 Email: op1394@mail.telepac.pt	0	erro - envio mail
Câmara Municipal de Povoação Largo do Município 9650-411 Povoação Tel. + 351 296 585 549 Fax. + 351 296 585 374 Email: cmpovoacao@mail.telepac.pt	1	
Câmara Municipal de Ribeira Grande Largo Conselheiro Hintze Ribeiro 9600-509 Ribeira Grande Tel. + 351 296 472 118 Fax. + 351 296 472 720 Email: geralcmrg@cm-ribeiragrande.pt	1	
Câmara Municipal de Santa Cruz da Graciosa Largo Vasco da Gama 9880-352 Santa Cruz da Graciosa Tel. + 351 295 730 040 Fax. + 351 295 712 124 Email: cmscgraciosa@mail.telepac.pt	0	erro envio mail
Câmara Municipal de Santa Cruz das Flores Rua Senador André de Freitas, 13 9970-337 Santa Cruz das Flores		

Nome da Entidade	Enviados	Observações
Tel. + 351 292 590 700 Fax. + 351 292 590 718		
Email: cmscf@mail.telepac.pt	0	erro envio mail
Câmara Municipal de São Roque do Pico		
Alameda 10 de Novembro de 1542		
9940-353 São Roque do Pico		
Tel. + 351 292 648 700 Fax. + 351 292 648 709		
Email: cmsrp@mail.telepac.pt	1	
Câmara Municipal de Velas		
Rua de São João		
9800-539 Velas		
Tel. + 351 295 412 214 Fax. + 351 295 412 351		
Email: geral.m.valas@mail.telepac.pt	0	erro envio mail
Câmara Municipal de Vila do Porto		
Largo Nossa Senhora da Conceição		
9580-539 Vila do Porto		
Tel. + 351 296 820 000 Fax. + 351 296 820 009		
Email: geral@cm-viladoporto.pt	1	
Câmara Municipal de Vila Franca do Campo		
Praça da República		
9680-115 Vila Franca do Campo		
Tel. + 351 296 539 100 Fax. + 351 296 539 257		
Email: geral@cmvfc.pt	1	
Nordeste Activo - Empresa Municipal de Actividades Desp., Recr. e Tur., Águas e Resíduos, EEM		
Rua Dona Maria do Rosário, 4		
9630-144 Nordeste		
Tel. + 351 296 488 364 Fax. + 351 296 488 366		
Email: nordesteactivo@mail.telepac.pt	1	
Praia Ambiente, EM		
Rua do Evangelho		
9760-456 Praia da Vitória		
Tel. + 351 295 545 530 Fax. + 351 295 545 539		
Email: geral@praiaambiente.pt	1	
Serviços Municipalizados de Angra do Heroísmo		
Rua do Barcelos, 4		
9700-026 Angra do Heroísmo		
Tel. + 351 295 204 850 Fax. + 351 295 204 880		
Email: secretaria@smah.pt	1	
Serviços Municipalizados de Água e Saneamento de Ponta Delgada		
Rua Tavares de Resende, 165		
9504-507 Ponta Delgada		
Tel. + 351 296 205 660 Fax. + 351 296 282 385		
Email: geral@smaspdl.pt	1	

2.7 - Região Autónoma da Madeira

Nome da Entidade	Enviados	Observações
ARM - Águas e Resíduos da Madeira, SA Rua dos Ferreiros, 148-150 9000-082 Funchal Tel. + 351 291 201 020 Fax. + 351 219 201 021 Email: geral@aguasdamadeira.pt	1	
Câmara Municipal de Calheta (Madeira) Vila da Calheta 9370-136 Calheta Tel. + 351 291 820 200 Fax. + 351 291 823 235 Email: camera@cm-calheta-madeira.pt	0	erro envio mail
Câmara Municipal de Câmara de Lobos Largo da República 9300-138 Câmara de Lobos Tel. + 351 291 911 080 Fax. + 351 291 944 499 Email: cmcl@netmadeira.com	0	erro envio mail
Câmara Municipal de Funchal Praça do Município 9004-512 Funchal Tel. + 351 291 211 000 Fax. + 351 291 226 343 Email: cmf@cm-funchal.pt	1	
Câmara Municipal de Machico Largo do Município 9200-099 Machico Tel. + 351 291 969 990 Fax. + 351 291 965 515 Email: gabinete.apoio@cm-machico.pt	1	
Câmara Municipal de Ponta do Sol Rua Santo António, 5 9360-219 Ponta do Sol Tel. + 351 291 972 106 Fax. + 351 291 972 711 Email: cmpontadosol@mail.telepac.pt	0	erro envio mail
Câmara Municipal de Porto Moniz Praça do Lyra 9270-053 Porto Moniz Tel. + 351 291 850 180 Fax. + 351 291 852 998 Email: geral@portomoniz.pt	1	
Câmara Municipal de Ribeira Brava Rua Visconde Ribeira Brava 9350-213 Ribeira Brava Tel. + 351 291 952 548 Fax. + 351 291 952 182 Email: cmribravpt@mail.telepac.pt	0	erro envio mail
Câmara Municipal de Santa Cruz Largo do Município		

Nome da Entidade	Enviados	Observações
9100-157 Santa Cruz Tel. + 351 291 520 100 Fax. + 351 291 524 062 Email: geral@cm-santacruz.pt	1	
Câmara Municipal de Santana Sítio do Serrado 9230-116 Santana Tel. + 351 291 570 200 Fax. + 351 291 570 201 Email: duarte.ornelas@cm-santana.pt	0	erro envio mail
Câmara Municipal de São Vicente Vila de São Vicente 9240-225 São Vicente Tel. + 351 291 842 135 Fax. + 351 291 842 666 Email: camarasvicente@mail.telepac.pt	0	erro envio mail
IGA - Investimentos e Gestão de Água, SA Rua dos Ferreiros, 148-150 9000-082 Porto Santo Tel. + 351 291 201 020 Fax. + 351 291 201 021 Email: geral@iga.pt	1	

2.8 - Entidades Gestoras Plurimunicipais

Nome da Entidade	Enviados	Observações
Águas da Região de Aveiro, SA Travessa Rua da Paz, 4 3801-101 Aveiro Tel. + 351 234 910 200 Fax. + 351 234 910 299 Email: adra@adra.pt	1	erro no envio mail
Águas de Santo André, S.A. Cerca da Água, Rua dos Cravos, Apartado 64 7500-130 Vila Nova de Santo André Tel. + 351 269 708 240 Fax. + 351 269 708 269 Email: geral@aguasdesantoandre.com.pt	1	
Águas de Trás-os-Montes e Alto Douro, S.A. Avenida Osnabruck, 29 5000-427 Vila Real Tel. + 351 259 309 370 Fax. + 351 259 309 371 Email: geral@atmad.pt	1	
Águas do Algarve, S.A. Rua do Repouso, 10 8000-302 Faro Tel. + 351 289 899 070 Fax. + 351 289 807 919 Email: geral@aguasdoalgarve.pt	1	
Águas do Centro Alentejo, S.A. Av. D. Leonor Fernandes, 5, r/c		

Nome da Entidade	Enviados	Observações
7005-144 Évora Tel. + 351 266 769 650 Fax. + 351 266 769 651 Email: geral@adca.com.pt	1	
Águas do Centro, S.A. Rua São João de Deus, 27 4.º Esq. 6000-276 Castelo Branco Tel. + 351 272 348 700 Fax. + 351 272 348 701 Email: geral@aguasdocentro.com.pt	0	erro no envio mail
Águas do Douro e Paiva, S.A. Rua do Vilar, 235 – 5.º 4050-626 Porto Tel. + 351 226 059 300 Fax. + 351 226 059 301 Email: correio@addp.pt	1	
Águas do Mondego, SA ETA da Boavista Av. Dr. Luís Albuquerque 3030-410 Coimbra Tel. + 351 239 980 900 Fax. + 351 239 980 949 Email: geral@mondego.adp.pt	1	
Águas do Noroeste, SA Lugar de Gaído 4755-045 Lugar de Gaído Tel. + 351 253 919 020 Fax. + 351 253 919 029 Email: geral@adnoroeste.pt	1	
Águas do Norte Alentejano, S.A. Rua da Casa de Saúde nº 5 7300-137 Portalegre Tel. + 351 245 302 100 Fax. + 351 245 302 103 Email: info@adna.com.pt	1	
Águas do Oeste, S.A. Convento de São Miguel das Gaeiras 2510-718 Gaieras Tel. + 351 262 955 200 Fax. + 351 262 955 201 Email: geral@aguasdooeste.com	1	
Águas do Planalto, S.A. Estação de Tratamento de Água - Mosteiro de Fráguas 3460-304 Tondela Tel. + 351 232 819 240 Fax. + 351 232 819 259 Email: aguasdoplanalto@lusagua.pt	1	
Águas do Ribatejo, EIM Rua Gaspar Costa Ramalho, 38 2120-098 Salvaterra de Magos Tel. + 351 263 509 400 Fax. + 351 263 509 499		

Nome da Entidade	Enviados	Observações
Email: geral@aguasdoribatejo.com	1	
Águas do Vouga, S.A. E.N. 1, Lugar Feira Nova 3850-200 Albergaria-a-Velha Tel. + 351 234 520 090 Fax. + 351 234 520 099		
Email: avouga@lusagua.pt	1	
Águas do Zêzere e Côa, S.A. Rua Dr. Francisco Pissara de Matos nº21 6300-906 Guarda Tel. + 351 271 225 317 Fax. + 351 271 221 955		
Email: geral@adzc.adp.pt	1	
Águas Públicas do Alentejo, SA Rua Dr. Aresta Branco N.º 51 7800-310 Beja Tel. + 351 284 101 100 Fax. + 351 284 101 199		
Email: geral@agda.pt	1	
EPAL - Emp. Portuguesa das Águas Livres, S.A. Avendida da Liberdade, 24 1250-144 Lisboa Tel. + 351 213 251 000 Fax. + 351 213 251 397		
Email: epal@epal.pt	1	
IGA - Investimentos e Gestão da Água, S.A. Rua dos Ferreiros,148-150 9000-082 Funchal Tel. + 351 291 201 020 Fax. + 351 291 201 021		
Email: igamadeira@iga.pt	1	
SANEST - Saneamento da Costa do Estoril, S.A. Rua Flor da Murta - Terrugem 2770-064 Paço de Arcos Tel. + 351 214 462 100 Fax. + 351 214 462 270		
Email: sanest@sanest.pt	1	
SIMARSUL - Sistema Integrado Multimunicipal de Águas Residuais da Península de Setúbal, SA Avenida Luisa Todi, nº300 - 3º Andar 2900-452 Setúbal Tel. + 351 265 544 000 Fax. + 351 265 544 001		
Email: geral@simarsul.pt	1	
SIMDOURO, SA Rua Mártir S. Sebastião, 251 - 1º A 4400-499 São Pedro da Afurada VNGaia Tel. + 351 221 209 300 Fax. + 351 221 209 399		
Email: geral@simdouro.pt	1	
SIMLIS - Saneamento Integrado dos Municipíos do Lis,S.A.		

Nome da Entidade	Enviados	Observações
Rua Anzebino da Cruz Saraiva, 318 1.º G 2400-098 Leiria Tel. + 351 244 849 100 Fax. + 351 244 849 101 Email: geral@simlis.pt	1	
SIMRIA - Saneamento Integrado dos Municípios da Ria, S.A. Rua Capitão Sousa Pizarro, 60, 1.º 3810-076 Aveiro Tel. + 351 234 378 230 Fax. + 351 234 378 246 Email: geral@simria.pt	1	
SIMTEJO - Saneamento Integrado dos Municípios do Tejo e Trancão, S.A. Av. Defensores de Chaves, 45, 3.º piso 1000-112 Lisboa Tel. + 351 213 107 900 Fax. + 351 213 107 901 Email: geral@simtejo.adp.pt	1	
TRATAVE - Tratamento de Águas Residuais do Ave, S.A. Rua Etar de Serzedelo 4765-543 Serzedelo Tel. + 351 252 900 670 Fax. + 351 252 900 679 Email: tratave@tratave.pt	1	
VIMÁGUA - Empresa de Água a Saneamento de Guimarães e Vizela, EIM, SA Rua do Rei Pegu, 172 4810-025 Guimarães Tel. + 351 253 439 560 Fax. + 351 253 410 444 Email: vimagua@vimagua .pt	1	

2.9 – Empresas Consultoras no Sector

Tecnirede.pt
Intergraph.pt
NovaBase.pt
Aquasis.pt
Lógica.com
Tecnilab.pt

Diagnóstico da Cultura em Segurança da Informação - Sectores Águas/Saneamento e Saúde em Portugal

Exm.º Sr(a) Este questionário surge no âmbito da minha Tese de Mestrado em Segurança em Sistemas de Informação da Faculdade de Engenharia da Universidade Católica Portuguesa, sobre «O Impacto das Crenças Individuais dos Profissionais de Segurança na Cultura de Segurança da Informação numa Organização - Estudo nos sectores das Água/Saneamento e Saúde em Portugal» Pretende-se com este questionário: - Aferir da 'cultura individual' dos profissionais de segurança da informação e do impacto desta na adopção de modelos de segurança nos sectores das Água/Saneamento e Saúde em Portugal. - Identificar os principais desafios que um profissional da segurança da informação enfrenta numa filosofia de implementação de um projecto de Governação da Segurança da Informação - "O papel do profissional de segurança da informação" – factores motivadores, inibidores, críticos de sucesso e de boas práticas. Agradeço, desde já, a sua disponibilidade por responder a este questionário. Maria Helena Ferreira da Cruz e Silva

---

*Obrigatório

1- Qual o sector onde exerce a sua actividade * Seleccione uma das opções abaixo indicadas

- ○ Águas e Saneamento
- ○ Saúde

2- Qual a sua função? * Seleccione uma das opções abaixo indicadas

- ○ Gestor de Topo (executivo ou não)
- ○ Gestor intermédio
- ○ Gestor das Tecnologias de Informação (TI)
- ○ Consultor das TI
- ○ Gestor/funcionário de segurança
- ○ Trabalhador

3- Qual a sua área de formação mais relevante? * Seleccione uma das opções abaixo indicadas

- ○ Economia/Gestão
- ○ Informática/Ciências da Computação
- ○ Engenharia
- ○ Saúde
- ○ Auditoria
- ○ Direito
- ○ Outra

4- Qual o seu último / actual nível de formação (concluído) * Seleccione uma das opções abaixo indicadas

- ○ Nível não superior
- ○ Bacharelato/Licenciatura
- ○ Especialização/Pós-Graduação
- ○ Mestrado
- ○ Doutoramento/Pós-Doutoramento

5- Quantos anos tem de experiência profissional * Seleccione uma das opções abaixo indicadas

- ○ Até 5 anos
- ○ Entre 6 e 10 anos
- ○ Entre 11 e 20 anos
- ○ Entre 21 e 30 anos
- ○ Mais de 30 anos

6- Qual o número de trabalhadores na sua organização? * Seleccione uma das opções abaixo indicadas

- ○ Até 500 trabalhadores
- ○ Entre 501 e 1500 trabalhadores
- ○ Entre 1501 e 2500 trabalhadores
- ○ Entre 2501 e 3500 trabalhadores
- ○ Entre 3501 e 4500 trabalhadores
- ○ Mais de 4500 trabalhadores

7- Género? * Seleccione uma das opções abaixo indicadas

- ○ Feminino
- ○ Masculino

8- Idade? * Seleccione uma das opções abaixo indicadas

- ○ Menos de 25 anos
- ○ Entre 26 e 35 anos
- ○ Entre 36 e 45 anos
- ○ Entre 46 e 55 anos
- ○ Mais de 55 anos

9 - Considerando os seguintes FACTORES COMO MOTIVADORES para a adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização, como os classifica ? * Tenha em conta - A SUA OPINIÃO: O QUE PENSA

	1 - Não é importante	2 - Pouco importante	3 - Importante	4 - Muito importante
a) Evitar perdas financeiras	○	○	○	○
b) Ocorrência de Incidente anterior	○	○	○	○
c) Garantir a disponibilidade, confidencialidade e integridade da Informação	○	○	○	○
d) Planear a segurança da informação antes da implementação de novas tecnologias	○	○	○	○
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	○	○	○	○
f) Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização	○	○	○	○
g) Emergência contínua de novos riscos	○	○	○	○
h) Alterações contínuas na legislação/regulação	○	○	○	○
i) Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)	○	○	○	○

10 - Considerando os seguintes FACTORES COMO MOTIVADORES para a adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização, como os classifica ? * Tenha em conta - O SEU PONTO DE VISTA NO SEU SECTOR DE ACTIVIDADE / ORGANIZAÇÃO

	1 - Não é importante	2 - Pouco importante	3 - Importante	4 - Muito importante
a) Evitar perdas financeiras	○	○	○	○
b) Ocorrência de Incidente anterior	○	○	○	○
c) Garantir a disponibilidade, confidencialidade e integridade da Informação	○	○	○	○
d) Planear a segurança da informação antes da implementação de novas tecnologias	○	○	○	○
e) Responsabilizar os executivos e/ou gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança	○	○	○	○
f) Possibilitar o alinhamento da segurança da informação com os objectivos estratégicos da organização	○	○	○	○
g) Emergência contínua de novos riscos	○	○	○	○
h) Alterações contínuas na legislação/regulação	○	○	○	○
i) Obrigatoriedade de conformidade com normas internacionais (ISO/IEC 27001/2, etc.)	○	○	○	○

11 - Considerando os seguintes FACTORES COMO INIBIDORES para a adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização, como os classifica ? * Tenha em conta - A SUA OPINIÃO: O QUE PENSA

	1 - Não é importante	2 - Pouco importante	3 - Importante	4 - Muito importante
a) Valor do investimento	○	○	○	○
b) Falta de conhecimento	○	○	○	○
c) Cultura organizacional	○	○	○	○
d) Dificuldade em medir o custo/benefício	○	○	○	○
e) Acesso restrito à "Gestão de Topo"	○	○	○	○
f) Alterações contínuas na legislação/regulação	○	○	○	○
g) Emergência contínua de novos riscos	○	○	○	○

12 - Considerando os seguintes FACTORES COMO INIBIDORES para a adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização, como os classifica ? * Tenha em conta - O SEU PONTO DE VISTA NO SEU SECTOR DE ACTIVIDADE / ORGANIZAÇÃO

	1 - Não é importante	2 - Pouco importante	3 - Importante	4 - Muito importante
a) Valor do investimento	○	○	○	○
b) Falta de conhecimento	○	○	○	○
c) Cultura organizacional	○	○	○	○
d) Dificuldade em medir o custo/benefício	○	○	○	○
e) Acesso restrito à "Gestão de Topo"	○	○	○	○
f) Alterações contínuas na legislação/regulação	○	○	○	○
g) Emergência contínua de novos riscos	○	○	○	○

13 - Considerando os seguintes FACTORES COMO CRÍTICOS DE SUCESSO para a adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização, como os classifica ? * Tenha em conta - A SUA OPINIÃO: O QUE PENSA

	1 - Não é importante	2 - Pouco importante	3 - Importante	4 - Muito importante
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	○	○	○	○
b) Suporte da Gestão de Topo	○	○	○	○
c) Responsabilização pela Segurança da Informação	○	○	○	○
d) Motivação dos funcionários	○	○	○	○
e) Programas para a conscientização, educação e formação em segurança em informação	○	○	○	○
f) Conformidade com Normas Internacionais de Segurança	○	○	○	○
g) Auditorias de Segurança da Informação	○	○	○	○
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	○	○	○	○
i) Política de Segurança da Informação	○	○	○	○
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	○	○	○	○

14 - Considerando os seguintes FACTORES COMO CRÍTICOS DE SUCESSO para a adopção/implementação dum Sistema de Gestão da Segurança da Informação numa organização, como os classifica ? * Tenha em conta - O SEU PONTO DE VISTA NO SEU SECTOR DE ACTIVIDADE / ORGANIZAÇÃO

	1 - Não é importante	2 - Pouco importante	3 - Importante	4 - Muito importante
a) Entendimento da "Gestão de Topo" para as questões da segurança da informação	○	○	○	○
b) Suporte da Gestão de Topo	○	○	○	○
c) Responsabilização pela Segurança da Informação	○	○	○	○
d) Motivação dos funcionários	○	○	○	○
e) Programas para a conscientização, educação e formação em segurança em informação	○	○	○	○
f) Conformidade com Normas Internacionais de Segurança	○	○	○	○
g) Auditorias de Segurança da Informação	○	○	○	○
h) Utilização de tecnologias de suporte (COBIT, ITIL, etc.)	○	○	○	○
i) Política de Segurança da Informação	○	○	○	○
j) Modelo/Programa de Governação para a Segurança da Informação (equipa de suporte)	○	○	○	○

15 - Considerando os seguintes FACTORES COMO BOAS PRÁTICAS num Sistema de Gestão da Segurança da Informação numa organização, como os classifica ? * Tenha em conta - A SUA OPINIÃO: O QUE PENSA/FAZ

	1 - Não é importante	2 - Pouco importante	3 - Importante	4 - Muito importante
a) A minha senha de acesso não a partilho com ninguém	○	○	○	○
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	○	○	○	○
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	○	○	○	○
d) Devem existir programas para a conscientização, educação e formação em segurança	○	○	○	○
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	○	○	○	○
f) Devem existir auditorias de Segurança da Informação	○	○	○	○
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	○	○	○	○
h) Deve existir uma Política de Segurança da Informação	○	○	○	○
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	○	○	○	○

16 - Considerando os seguintes FACTORES COMO BOAS PRÁTICAS num Sistema de Gestão da Segurança da Informação numa organização, como os classifica ? * Tenha em conta - O SEU PONTO DE VISTA NO SEU SECTOR DE ACTIVIDADE / ORGANIZAÇÃO

	1 - Não é importante	2 - Pouco importante	3 - Importante	4 - Muito importante
a) A minha senha de acesso não a partilho com ninguém	○	○	○	○
b) Quando me afasto do meu posto de trabalho bloqueio a minha sessão no PC	○	○	○	○
c) Cada trabalhador apenas deve ter acesso à informação necessária ao desempenho das suas funções	○	○	○	○
d) Devem existir programas para a conscientização, educação e formação em segurança	○	○	○	○
e) Deve existir conformidade com Normas Internacionais de Segurança (ISO/IEC 27001/2, COBIT, ITIL, etc.)	○	○	○	○
f) Devem existir auditorias de Segurança da Informação	○	○	○	○
g) Devem ser utilizadas tecnologias de suporte (COBIT, ITIL, etc.)	○	○	○	○
h) Deve existir uma Política de Segurança da Informação	○	○	○	○
i) Deve existir Modelo/Programa de Governação para a Segurança da Informação	○	○	○	○

Obrigada pela sua colaboração

Fim do Questionário

TESE DE MESTRADO

«O impacto das crenças individuais dos profissionais de segurança na cultura de segurança da informação numa organização» - Estudo num sector da actividade empresarial portuguesa.

As organizações são, nos dias de hoje, cada vez mais tecno dependentes visando:

- A adequação e a melhoria do desempenho organizacional;
- A satisfação dos clientes;
- A redução e/ou minimização dos riscos;
- O garante da continuidade dos serviços prestados.

Por isso, a gestão da informação faz parte integrante da gestão das organizações e os sistemas de informação que aí existem são cada vez mais complexos sendo suportados por tecnologias, o que obrigam à necessidade de uma arquitectura integrada dos mesmos, associada ao forte alinhamento aos objectivos do `negócio´.

> «*O conceito de 'governação das TI' não existe isolado, ele é parte da `governação empresarial´. … A governação é uma necessidade básica das empresas modernas … deveríamos falar sobre partilha entre as TI e o negócio*».

Guldentops, Erik CISA, CISM (2007) Guldentops, Erik, CISA®, CISM® – "The Rule of Four of IT Governance" - Information System Control Jornal, volume 6, 2007, pp.19

Segundo *Serra, J. Paulo* em o "*Manual de Teoria da Comunicação*"(Covilhã: Livros Labcom, 2007. 203 p.p. 93-101) a Informação é «*o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe.*»

Actualmente, a Informação é um activo crítico nas organizações e na sociedade porque: *«Internet confiável e segura e as comunicações electrónicas são agora fulcrais para toda a economia e sociedade em geral. Incidentes de segurança cibernética podem ter um grande impacto sobre os utilizadores individuais, na economia e na sociedade em geral.» (Incidentes cibernéticos – caixa lateral)*

«Cyber Incident Reporting in the EU - An overview of security articles in EU legislation», de Agosto 2012 e publicado pela European Network and Information Security Agency (ENISA)

Mudanças tecnológicas, redes de comunicações globais e o intenso uso das tecnologias de informação obrigam a que, cada vez mais, haja a necessidade de efectivamente implantar sistemas que acautelem o risco e possibilitem a gestão da segurança da informação.

> *«… é imperativo que as organizações alavanquem o uso das suas tecnologias de informação (TI) para maximizar a eficiência, a eficácia e a confiança da organização num ambiente de volatilidade actual e de intensificada expectativa na governação corporativa.»*

Hamacker, Stacey, CISA®, CIA®,and Hutton, Austin CISA® - "Enterprise Governance and the Role of IT" - Information System Control Jornal, volume 6, 2005

Incidentes Cibernéticos

1. Em Junho de 2012 – violação de 6,5 milhões (SHA-1) *hashed passwords* de um grande negócio focado numa rede social. O impacto da violação não é totalmente conhecida, mas milhões de utilizadores foram convidados a alterar suas senhas, porque os seus dados pessoais poderiam estar em risco.

2. Em Dezembro de 2011 - a tempestade Dagmar afectou o fornecimento de energia para redes de comunicações electrónicas, na Noruega, Suécia e Finlândia. O resultado foi que milhões de utilizadores ficaram sem telefonia ou internet até duas semanas.

3. Em Outubro de 2011 - houve uma falha no centro de dados do Reino Unido de um grande fornecedor de *smartphone*. O resultado foi que milhões de utilizadores em toda a UE e no mundo não puderam enviar ou receber *e-mails*, o que afectou severamente o sector financeiro.

4. Durante o verão de 2011 – violação de segurança numa autoridade de certificação holandesa possibilitou a emissão de certificados falsos.

5.Em Abril de 2010 - um fornecedor de telecomunicações chinês foi atacado, desviando, durante 20 minutos, 15% do tráfego mundial de internet através de servidores chineses. Como resultado, as comunicações de Internet de milhões de utilizadores foram expostas (à escuta).»

Cyber Incident Reporting in the EU - An overview of security articles in EU legislation», de Agosto 2012 e publicado pela European Network and Information Security Agency (ENISA)

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu

GLOSSÁRIO

Risco [1]

«É a possibilidade de uma determinada ameaça explorar vulnerabilidades de um activo ou grupo de activos para causar perdas ou danos a estes.»

Controlo [2]

«É uma forma de gerir um risco, garantindo que um objectivo de negócio é atingido, ou que um processo seja seguido. É a medida posta em prática para regular, orientar e monitorizar um risco.»

Segurança da Informação [3]

«Processo de protecção dos sistemas de informação e que tem como finalidade garantir a disponibilidade, o sigilo, a integridade, a autenticidade, o controlo de acesso e o não-repúdio das informações».

Governação Corporativa [4]

«O sistema pelo qual as organizações são dirigidas e controladas.»

Governação das TI [5]

«É um conjunto de estruturas e processos que visam garantir que as TI suportam e maximizam adequadamente os objectivos e estratégias de negócio da Organização, adicionando valor aos serviços entregues, balanceando os riscos e obtendo o retorno dos investimentos».

Sistema de Gestão da Segurança da Informação (SGSI) [6]

«É projectado para assegurar a selecção de controlos de segurança adequados para proteger os activos de informação e proporcionar confiança às partes interessadas. É um standard formal que permite a certificação independente de organizações no Processo de Gestão da Segurança da Informação».

Referências
[1] Oliveira, Wilson (2001)"Segurança da Informação – Técnicas e Soluções", Centro Atlântico, Lda, 1ª Ed., 2001, pp.67
[2] Gonçalves, Hélder (2011)"A Gestão do Risco Operacional e as TIC – O Contributo da Auditoria no Sector Financeiro" Universidade Católica Editora 2011, pp.173
[3] Adaptado de [1], pp.17,19
[4] OCDE (1999) – "Principles of Corporate Governance" - citado por [2], pp.105
[5] Cobit Foundation Course- citado por [2], pp.105
[6] idem [2], pp. 161

«A governação da segurança da informação devidamente dirigida pode ser um bom trunfo para o sucesso de uma organização.»

Pironti, John P., CISA®, CISM®, CISSP®, ISSAP®, ISSMP® – "Information Security Governance: Motivations, Benefits and Outcomes" - Information System Control Jornal, volume 4, 2006, pp.45-48

«… a efectiva governação requer que o conceito de responsabilidade partilhada seja construído sobre uma estrutura de segurança da informação capaz de estabelecer resiliência operacional e de negócio.»

Poole, Vernon, CISM® – "Why Information Security Governance - Is Critical to Wider Corporate Governance Demands—A European Perspective" – Information System Control Jornal, volume 1, 2006,

Quem são, então, os actores desta responsabilidade partilhada?

São todos aqueles que integram, na totalidade ou parcialmente, a organização. Enfoque para: Gestores de topo, Executivos, Gestores das TI, Consultores de TI, Utilizadores e Profissionais de segurança.

A comunidade científica tem vindo a desenvolver e a disponibilizar "*standards*" para ajudar as organizações na implementação organizada e estruturada da Governação Corporativa, da Gestão ou Governação das TI, incluindo normas e padrões de segurança da informação de que são exemplo: ISO/IEC- 27001/2, ITIL, COBIT, etc.

No entanto, «… baseada na pesquisa/avaliação do ITGI, cerca de 70% a 80% das organizações globais claramente não têm implementado a governança da segurança da informação.»

Brotby, Krag (2007) e baseado no relatório do IT Governance Institute´s IT Governance Global Status Report 2006,

Por outro lado, «… num estudo disponibilizado pelo ISACA – Critical Elements of Information Security Program Success, os seis factores críticos mais reportados na pesquisa foram:

1. Compromisso da gestão de topo às iniciativas da segurança da informação.
2. Entendimento da gestão de topo para as questões da segurança da informação.
3. Planeamento da segurança da informação antes da implementação de novas tecnologias.
4. Integração entre o ´negócio` e a segurança da informação.
5. Alinhamento de segurança da informação com os objectivos da organização.
6. Responsabilização dos executivos e/ou dos gestores responsáveis pela implementação, acompanhamento e divulgação de informações de segurança".

Pironti, John P., CISA®, CISM®, CISSP®, ISSAP®, ISSMP® – "Information Security Governance: Motivations, Benefits and Outcomes" - Information System Control Jornal, volume 4, 2006, pp.45-48

Ainda, num estudo realizado na Bélgica pela University of Antwerp Management School sobre práticas de governação das TI e alinhamento das mesmas com o negócio, «*ficou demonstrado que é mais fácil implementar estruturas de governação das TI do que processos de governação das TI; e que mecanismos relacionais também parecem ser muito importantes nos estados de iniciação do projecto de implementação da governação das TI, tornando-se menos importantes à medida que a estrutura de governação das TI passa a ser integrada nas operações do dia-a-dia.*»

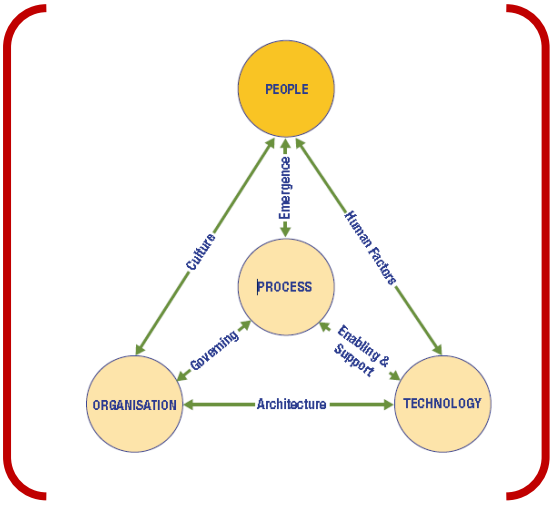
Haes, Steven De Ph.D. e Grembergen, Wim Van Ph.D. – "Practices in IT Governance and Business/IT Alignment" - Information System Control Jornal, volume 2, 2008, pp.23-27

«A segurança da informação não é uma questão técnica, mas uma questão estratégica e humana.
Não adianta adquirir uma série de dispositivos de hardware e software sem formar e consciencializar o nível administrativo da empresa e todos os seus funcionários.»

Oliveira, Wilson – "Segurança da Informação – Técnicas e Soluções" – Centro Atlântico, Lda., 1ª Ed., 2001, pp.17

Conceito de "cultura organizacional"

«Um padrão de comportamentos, crenças, suposições, atitudes e maneiras de fazer as coisas».
«A palavra 'padrão' é chave nesta definição. Culturas são



feitas de indivíduos, mas não representam necessariamente comportamentos individuais. É a cultura que influencia comportamentos individuais e de grupo.»
«na utilização do BMIS existem duas camadas de cultura a serem consideradas: a organizacional – que é formada ao longo do tempo pela concepção, estratégia organizacional e comportamento das pessoas no trabalho, sendo a segunda camada encontrada em pessoas de cultura individual que pode ser diferente e heterogénea.
Desta forma, ambas as camadas devem ser tidas em conta quando considerada a perspectiva de visualização da interconexão dinâmica (DI)-'Cultura' pois, esta, influencia a segurança.»

O BMIS refere Kiely, L.; T.V. Benzel; 'Systemic Security Management', Security & Privacy, IEEE, vol. 4, no. 6, 2006, p. 74-77 na pp.27 da publicação da ISACA, 2010
ISACA – "The Business Model for Information Security' (BMIS)", 2010, pp.27

O mote para o desenvolvimento deste trabalho surge com as seguintes questões:

- Quais os desafios na definição e na implementação de uma cultura organizacional, em particular no domínio da segurança da informação?
- Que crenças individuais têm os profissionais da segurança da informação e como é que isso se reflecte na cultura organizacional de segurança da informação nas organizações?
- Como estão as organizações portuguesas a implementar a governação da segurança da informação?
- Qual é a relação entre a governação da segurança da informação e o alinhamento/partilha com o "negócio"?
- Será que as conclusões dos estudos referidos se aplicam aos projectos de implementação de sistemas de gestão da segurança da informação?
- E será que, no mundo empresarial / organizacional português, obteremos o mesmo tipo de respostas?

Pretende-se assim lançar um questionário para *«O Diagnóstico da Cultura em Segurança da Informação – Sectores: Água/Saneamento e Saúde em Portugal»*

Resultados

Identificar a cultura organizacional em Segurança da informação:

- Aferir da 'cultura individual' dos profissionais de segurança da informação e do impacto desta na adopção de modelos de segurança nos sectores das Água/Saneamento e Saúde em Portugal.
- Identificar os principais desafios que um profissional da segurança da informação enfrenta numa filosofia de implementação de um projecto de Governação da Segurança da Informação - "O papel do profissional de segurança da informação" – factores motivadores, inibidores e críticos de sucesso.

Tendo em conta:

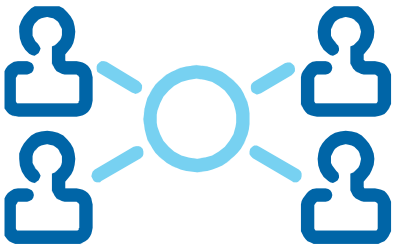
- Sector de actividade: Água/Saneamento, Saúde;
- Função: gestor de topo, gestor intermédio, gestor das TI, consultor das TI, gestor/funcionário de segurança, funcionário;
- Área de Formação mais relevante: economia/gestão, informática/ciências da computação, Engenharia, Saúde, Auditoria, Direito, outra;
- Nível de formação | Anos de experiência profissional
- N.º funcionários na organização
- Género | Grupo etário

Público alvo: gestores de topo, de nível intermédio, das TI, consultores das TI, gestores/funcionários de segurança e funcionários de organizações nas áreas das: Águas/Saneamento (ex: entidades gestoras, entidades reguladoras, …) e de Saúde (ARS, hospitais, entidades reguladoras e/ou tutelares, etc.)

Obrigada pela sua colaboração

- Participe.
- Envie o seu e-mail para mhsilva1206@gmail.com para que lhe seja enviado o questionário online.
- Poderá responder acedendo ao link: https://docs.google.com/spreadsheet/viewform?formkey=dDFENi1Nd1hvVXY5M1F4em9PYTJtYnc6MA#gid=0

Universidade Católica Portuguesa
Faculdade de Engenharia



O Impacto das Crenças Individuais dos Profissionais na Cultura de Segurança da Informação nas Organizações

– Estudo no sector da Água / Saneamento em Portugal

Maria Helena Ferreira da Cruz e Silva

Dissertação para obtenção do Grau de Mestre em Segurança em Sistemas de Informação
Anexo B

Júri

Prof. Doutor Manuel José Martinho Barata Marques (Presidente)
Prof. Doutor Rui Jorge Correia Mendes Alves Pires
Prof. Doutor Tito Santos Silva (Orientador)

Setembro de 2014

Fonte e Tratamento dos Dados

Folhas de cálculo Excel (ver CD/DVD em anexo):

- Fonte de Dados Recolhidos
- Parâmetros
- Factores Motivadores – Perspectiva do Próprio (PP) | Perspectiva do Próprio face à Organização (PPO) | Radar: PP vs PPO
- Factores Inibidores – Perspectiva do Próprio (PP) | Perspectiva do Próprio face à Organização (PPO) | Radar: PP vs PPO
- Factores Críticos de Sucesso (FCS) – Perspectiva do Próprio (PP) | Perspectiva do Próprio face à Organização (PPO) | Radar: PP vs PPO
- Factores de Boas Práticas (FBP) – Perspectiva do Próprio (PP) | Perspectiva do Próprio face à Organização (PPO) | Radar: PP vs PPO