ESTGF | POLITÉCNICO DO PORTO

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Uma metodologia para o cálculo do Índice de Maturidade da Segurança Informática

DESIGNAÇÃO DO MESTRADO	Engenharia Informática
AUTOR	Sérgio Manuel Barbosa Monteiro
ORIENTADOR(ES)	Professor Doutor João Paulo Magalhães
AN	2017

Agradecimentos

Tomo a liberdade de agradecer o contributo inestimável a todos aqueles que, pelo apoio e estímulo constante, tornaram possível a realização deste projeto/dissertação.

Ao Professor Doutor João Paulo Magalhães, pelo incentivo, pela disponibilidade, pelas sugestões dadas, pelos desafios que colocou e por me fazer acreditar e orientar com o desenvolvimento deste trabalho. A ele, o meu apreço, gratidão e estima.

À minha esposa Hermínia Pinto e ao meu filho, Guilherme Monteiro, companheiros de todas as horas, em primeiro pela minha ausência, e depois pela paciência, compreensão e incentivo em todos os momentos.

À minha família, particularmente à minha mãe, ao meu pai, à minha avó Adelaide e ao meu irmão e cunhada, pelo reforço positivo e pelo constante cuidado.

A todos os colegas e amigos que me apoiaram em todos os momentos.

A todas as organizações, que de forma aberta e espontânea aceitaram colaborar com o presente estudo.

Resumo

Os Sistemas de Informação (SI) baseados em tecnologias computacionais continuam a ditar uma profunda mudança nas organizações e nas pessoas. Eles são fundamentais para suportar as atividades em áreas operacionais, táticas e estratégicas, bem como a competitividade, sustentabilidade e o desenvolvimento das organizações. A dependência destes sistemas tem um senão. O risco associado à indisponibilidade dos sistemas, extravio de informação e adulteração de dados cresce tornando necessária a adoção de medidas eficazes para mitigar o risco. Neste âmbito surgem modelos de avaliação de risco quantitativos e qualitativos que permitem às organizações avaliar o risco face à exploração de vulnerabilidades existente e grau de ameaça considerando sempre o valor do bem a proteger. Ainda que extremamente importantes, estes modelos exigem alguma maturidade por parte das empresas dificultando a sua adoção em massa.

Neste trabalho, propomos uma metodologia *entry-level* para o cálculo do Índice de Maturidade da Segurança Informática das organizações (IMSI). Esta metodologia baseia-se na análise de três eixos e três áreas funcionais (pessoas, processos e tecnologia) e pretende ser uma primeira abordagem, com a simplicidade da linguagem e foco no destinatário, para a medição quantitativa de potenciais riscos à segurança de informação. A metodologia já foi aplicada em contexto real e os resultados revelam a sua utilidade. Os resultados são simples de entender facilitando a disseminação de uma cultura de consciencialização de segurança, ao mesmo tempo que permitem às organizações a adoção de medidas imediatas para mitigar os principais problemas encontrados ou contribuir para justificar uma análise de risco mais profunda.

Palavras-Chave:
Segurança de Informação, Risco, Metodologia de análise de risco, Ameaça, Vulnerabilidades.

Abstract

Information Systems (IS) based on computer technologies continue to pose a profound change in organizations and people. IS are fundamental to support operational, tactical and strategic activities, as well as the competitiveness, sustainability and development of organizations. Unfortunately, the higher dependence of these systems has a main drawback, i.e., the risk associated with unavailability, data leaks and data tampering increases, making it necessary to take effective risk mitigation measures. There are a few of quantitative and qualitative risk models that allow organizations to measure the risk considering the type of vulnerabilities and degree of threat. The models are extremely important, but they require some maturity from the organisations making it difficult its mass adoption.

In this work, we propose an entry-level methodology for the determination of a Maturity Index of Computer Security. This methodology is based on the analysis of three axes and three functional areas (people, processes and technology) and aims to be a first approach, with the simplicity of language and focus on the recipient, for the quantitative measurement of potential security risks. The methodology has already been applied in a real context and the results reveals the usefulness of it. Its results are simply to understand facilitating the spread of a security awareness culture, while allow the organisations to take immediate actions to mitigate the main issues found or contribute to justify a deeper risk analysis.

Keywords:

Information Security, Risk, Risk Analysis Methodology, Threats, Vulnerabilities

Publicações

O resultado deste trabalho resultou na seguinte publicação científica.

Monteiro S. and Magalhães J. P., "Information Security Maturity Level: A Fast Assessment Methodology", In proceedings of the 8th International Conference on Ambient Intelligence - Workshop Security in Ambient Intelligent Environments, June 2017, Porto, Portugal (IN PRESS).

Índice

Resumo iii
Palavras-Chave: iii
Abstract v
Publicações vii
Índice ix
Índice de Figuras xi
Índice de Equações xiii
Índice de Tabelas xv
Lista de Abreviaturas xvii
Capitulo 1 - Introdução 19
1.1 Estrutura da dissertação 21
Capítulo 2 - Enquadramento Teórico 23
2.1 Segurança de Informação 23
2.2 Risco 24
2.3 Métodos e orientações atuais de gestão e de análise de risco 28
2.3.1 O Papel das Normas para a Segurança de Informação 28
2.3.2 Cybersecurity Framework 29
2.3.3 Modelos de avaliação de risco 31
Capítulo 3 - Índice de Maturidade de Segurança Informática 37
3.1 Metodologia subjacente ao IMSI 39
3.2 Enquadramento de nível 39
3.3 Inquéritos 41
3.3.1 Algoritmo de cálculo do IMSI 48
3.3.2. Cálculo Individual das questões 49
3.4 Engenharia Social – Teste de Pessoas (Eixo 2) 54
3.4.1 Metodologia 54
3.4.2 Algoritmo de cálculo do IMSI 58
3.5 Análise de Vulnerabilidades Tecnológicas 59
3.5.1 Algoritmo de cálculo do IMSI 63
3.5.2 Fases a executar – Metodologia IMSI 63
Capitulo 4 - Experimentação da metodologia 67
4.1 Ações e planeamento do eixo 1 67
4.2 Ações e planeamento do eixo 2 70

4.3 Análise de resultados 73
4.4 Resultados inter-eixos 98
Capitulo 5 - Conclusões e Trabalho Futuro 99
5.1 Trabalho Futuro 101
Referências bibliográficas 103
Anexo I | Inquérito por Questionário 107
Anexo II | Declaração de autorização 119
Anexo III | Macro auto-executável (eixo 2) 121

Índice de Figuras

Figura 1: Processo de gestão de riscos (adaptado de [19]) 24
Figura 2: Núcleo da framework NIST, publicado em fev. 2014 30
Figura 3: Eixos base de análise para o cálculo do IMSI 37
Figura 4: Curva de nível Deloitte 39
Figura 5: Curva de nível (adotada da Deloitte [4] 40
Figura 6: Etapas da Investigação por Inquérito (adaptado de PSE [31]) 42
Figura 7: Amplitude do inquérito. Áreas em análise 43
Figura 8: Algoritmo de cálculo do IMSI do eixo 1 49
Figura 9: Algoritmo para o cálculo da força da password 52
Figura 10: Fases da Engenharia Social 56
Figura 11: Algoritmo de cálculo do IMSI do eixo 2 58
Figura 12: Algoritmo de cálculo do IMSI do eixo 3 63
Figura 13: Fluxograma de etapas a executar nos três eixos de análise 64
Figura 14: E-mail para preenchimento de inquérito 69
Figura 15: Questões – Relação e Tipo 74
Figura 16: Número e Percentagem de Questões por tipo e atribuição de pesos 75
Figura 17: Análise Inquéritos da Instituição A – Colaboradores 76
Figura 18:Análise de Inquéritos Instituição A – Gestão 77
Figura 19: Análise de Inquéritos Instituição A - Informática 78
Figura 20: Enquadramento de Nível da Instituição A (inquéritos) 79
Figura 21: Análise de Inquéritos Instituição B – Colaboradores 80
Figura 22: Enquadramento de nível Instituição B (Inquéritos) 81
Figura 23: Análise de iquéritos Instituição C - Colaboradores 82
Figura 24 - Análise de Inquéritos Instituição C – Gestão 83
Figura 25: Análise de Inquéritos Instituição C – Informática 84
Figura 26: Enquadramento de Nível Instituição C (Inquéritos) 86
Figura 27: Análise de Inquéritos Instituição D - Colaboradores 86
Figura 28: Análise de Inquéritos Instituição D – Gestão 87
Figura 29: Análise de Inquéritos Instituição D – Informática 88
Figura 30: Enquadramento de Nível da Instituição D (Inquéritos) 90
Figura 31: Posição/comparação das organizações (Eixo 1) 91
Figura 32: E-mail Campanha Phishing 93
Figura 33: Estatísticas globais da campanha – Instituição A 94
Figura 34: Estatísticas globais da campanha 95
Figura 35: Estatísticas globais da campanha 96

Figura 36: Estatísticas globais da campanha 96
Figura 37: Resultados comparativos (eixo 2).....98

Índice de Equações

Equação 1: Risco (ISO 27001) 26
Equação 2: Expectativa Anual de Perdas (EAP) 33
Equação 3: Percentagem de questões tipo 1 47
Equação 4: Percentagem de questões tipo 2 47
Equação 5: Cálculo de Questões do padrão 1.....50

Índice de Tabelas

Tabela 1: Vantagens e desvantagens dos métodos quantitativos e qualitativos 31
Tabela 2: Comparação de modelos de análise de risco quantitativos.....32
Tabela 3: Foco de análise por nível e por área. 46
Tabela 4: Exemplo de Cálculo para cotação de questões 48
Tabela 5: Exemplo de cálculo de nível 53
Tabela 6: Definição da estrutura dos ataques a executar 57
Tabela 7: Enquadramento de nível.....59
Tabela 8: Ações efetuadas e respostas obtidas (Eixo 1) 70
Tabela 9: Campanha de Phishing.....72
Tabela 10: Resultados inter-eixos 98

Lista de Abreviaturas

IMSI – Índice de Maturidade de Segurança Informática
SGSI - Sistema de Gestão da Segurança de segurança de informação
B2C – Business-to-Consumer
SI - Sistemas de Informação
TI - Tecnologias de Informação
ISO - International Organization for Standardization

Capitulo 1 - Introdução

A Internet, veio revolucionar a forma como as pessoas e organizações se relacionam. Segundo um estudo do Facebook, no final de 2015, havia 2,3 mil milhões de utilizadores com acesso à Internet em todo o mundo [1]. Em Portugal, de acordo com a Marktest [2], são 5,6 milhões os utilizadores ligados. Há muito que a dimensão da Internet nos fez deixar de tentar contabilizar tudo aquilo que se passa a cada instante, mas não deixa de ser curioso a evolução desses números e ver a quantidade de coisas que acontecem a cada 60 segundos na Internet. Em 2016, e de acordo com o estudo desenvolvido pela Excelacom [3], a cada minuto que passa: são visualizados 2,78 milhões de vídeos no YouTube; são efetuadas 2,4 milhões de pesquisas no Google; são enviados 150 milhões de e-mails e mais de 20 milhões de mensagens no WhatsApp; a Amazon fatura mais de 200 mil dólares em vendas. Ainda, segundo a Pordata, na sua publicação de Base de dados de Portugal Contemporâneo, publicado em 2016 [4], nos 28 países da União Europeia, 98% das empresas com 10 ou mais pessoas utilizam o computador como instrumento básico de trabalho.

Atualmente é indiscutível que a tecnologia influencia cada vez mais as sociedades e a metodologia de trabalho das pessoas. O advento da sociedade de informação, tendo como pilar e garante a necessidade de informação e a sua valorização, tem permitido o crescimento exponencial da competitividade, da modernização e inovação.

Infelizmente a evolução faz-se sentir também em algo menos positivo, nomeadamente no surgimento e proliferação do fenómeno dos ciberataques, que se traduz em práticas como o cibercrime, ciberespionagem, ciberguerra e o *hacktvismo*. Nos últimos tempos tem-se verificado um crescimento em número, sofisticação e impacto destes ataques. De acordo com o estudo realizado pela McAfee [5] em 2013 "*the Economic Impact of Cybercrime and Cyber Espionage*", o cibercrime é responsável por perdas anuais, em organizações de todo o mundo, entre 300 mil milhões a $1 milhão de milhões de dólares, ou seja, entre 0,4% a 1,4% do Produto Interno Bruto (PIB) global. A pesquisa da Juniper Research efetuada em maio de 2015 [6] prevê que a rápida digitalização das vidas dos consumidores e registos corporativos aumentará o custo das violações de dados para $ 2,1 milhão de milhões até 2019. Os números não são exatos uma vez que existe falta de informação confiável sobre a temática pelo facto de muitas vítimas considerarem a violação dos seus sistemas de segurança como algo de constrangedor e, por isso, nem sempre relatarem as mesmas. Além das perdas financeiras diretas, há consequências mais difíceis de contabilizar e que representam valor para as organizações. Entre estas temos as perdas de reputação e de confiança. Também a European Union Agency for Network and Information Security (ENISA), entidade europeia para a segurança de informação, produz anualmente um

relatório com uma análise sobre os incidentes que ocorrem no sector das comunicações. No relatório de 2012 [7], menciona que de 2011 para 2012 os incidentes causados por ciberataques subiram 4% (de 2% para 6%).

O crescente número de ataques e os seus impactos têm contribuído para o aumento da consciência das organizações revelada pela preocupação em protegerem-se de eventuais ataques e exposição ao risco. Por todo o mundo, empresas e especialistas com reconhecidas e abrangentes competências no espectro da cibersegurança colocam as questões da segurança de informação no topo das prioridades. A consultora Deloitte [8] e Armaghan, B. & Rafhana [9], consideram nas suas várias publicações, que as ameaças e ataques cibernéticos estão a crescer em número e complexidade e atravessam vários domínios de atuação. O relatório de segurança interna publicado pelo Ministério da Administração Interna Português [10] alerta para esse facto ao referir que "*as lacunas de segurança nas infraestruturas informáticas de diferentes serviços e/ou organismos públicos, permitiram operações hacktivistas com alguma gravidade e especial impacto mediático*". Os próprios estados estão cada vez mais conscientes do risco e tal como outros países, Portugal, em outubro de 2014 criou o Centro Nacional de Cibersegurança [11], com o objetivo de "*Implementar as medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento dos organismos do estado, das infraestruturas críticas e dos interesses nacionais*". Se a situação já era clara para os especialistas da área, agora a necessidade de lidar com a escalada do problema torna-se prioritária. Nunca como antes a análise de risco subjacente a cada organização e a definição dos controlos adequados para a sua mitigação, conforme indicação e recomendação da ISO 31000 [12] e de outras *frameworks*, esteve tão ativa.

Pese embora os *standards* e *frameworks* apresentem a base e as indicações para a avaliação e mitigação do risco, nem sempre, pela sua amplitude e caracter geral, se adequam à necessidade e realidade de muitas das organizações, nomeadamente às pequenas e médias empresas. Neste sentido, há a clara necessidade de existir algo mais simples e rápido que possa ser feito, no que respeita à gestão do risco da segurança de informação. A construção de um Índice de Maturidade de Segurança Informática (IMSI), tal como nos propomos a fazer, tem por objetivo dar resposta a essa necessidade.

Neste trabalho apresentamos a base para o desenvolvimento de uma metodologia simples e prática do cálculo do Índice de Maturidade de Segurança Informática (IMSI) das organizações. Para este cálculo serão considerados três eixos de análise (processos, pessoas e tecnologias) cujo cruzamento dos seus resultados permitirá atribuir um valor quantitativo. Este valor por sua vez possibilitará, através de uma linguagem mais facilmente

compreendida pelas estruturas de gestão, compreender o nível de risco/*score* de segurança informática e o posicionamento da organização relativamente aos seus *peers.* Desta forma, e antes de ser necessário entrar na profundidade da análise de risco tradicional, as organizações ficarão a conhecer melhor os seus pontos fracos, podendo desde logo adotar medidas preventivas/corretivas para mitigar os riscos identificados. Este trabalho, enquanto base de apoio para a quantificação de um *score* de segurança de informação, envolve:

- A criação de uma metodologia de análise aplicável a diferentes tipos de organização;
- A definição de meios técnicos e não técnicos para a recolha de dados com vista à quantificação do *score* de maturidade de segurança informática;
- A experimentação da metodologia no terreno e nos respetivos ajustes de forma e linguagem.

A definição de uma metodologia como a que propomos é útil na medida em que combina análises técnicas e não técnicas para aferir sobre potenciais falhas de segurança e riscos associados a estas. Ao utilizar uma metodologia base o processo pode ser replicado entre organizações e com a simplicidade de linguagem e *focus* no destinatário, procuramos maximizar a compreensão e valor dos resultados obtidos. A criação de um Índice de Maturidade de Segurança Informática baseada em tal metodologia é, até onde o nosso conhecimento na matéria nos permite dizer, inovador e potencia uma fácil compreensão da situação atual quer pela análise do simples índice obtido quer pela comparação com outros *peers*. Neste trabalho, para além da definição da metodologia, incluímos uma fase de análise e resultados, baseada na metodologia, e resultante da sua aplicação prática em contexto real. É de referir que a metodologia subjacente ao IMSI não deve substituir uma análise de risco tradicional. Tal deve ser vista como instrumento facilitador, na medida em que desperta consciências e revela evidências que por sua vez podem levar a um aprofundamento da análise e mitigação dos riscos.

1.1 Estrutura da dissertação

Esta dissertação está organizada em 5 capítulos. No capítulo 2 é feito o enquadramento teórico relacionado com a área da dissertação, no capítulo 3 é apresentada a proposta e a metodologia de trabalho desenvolvida, no capítulo 4 apresenta-se a prova de conceito e os resultados alcançados. Por fim, no capítulo 5 é feita a conclusão da dissertação.

Capítulo 2 - Enquadramento Teórico

A informação é o centro da segurança informática. Conforme se compreende na ISO 27001 [13], é na informação que reside o conhecimento e, nela, o valor de cada organização.

No contexto do presente estudo, e como refere a ISO 27002 [14], a informação é um ativo que, como qualquer outro, é essencial para os negócios de uma organização, e deve ser adequadamente protegido. A informação é encarada, atualmente, como um dos recursos mais importantes de uma organização, contribuindo decisivamente para a uma maior ou menor competitividade. De facto, com o aumento da concorrência de mercado, tornou-se vital melhorar a capacidade de decisão em todos os níveis. Como resultado deste significativo aumento da interconetividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

Antes de entrar na profundidade de análise, importa realçar e enquadrar alguns dos termos e conceitos recorrentes ao longo de todo o documento.

2.1 Segurança de Informação

A Segurança de Informação é definida na norma ISO/IEC 27000:2009 como sendo a preservação da Confidencialidade, Integridade e Disponibilidade (CIA – Confidentiality, Integrity Availability) da informação. Partindo destes três pilares, procura-se o garante de outras propriedades como o não-repúdio, a responsabilidade e a confiabilidade [15].

Para Rezende D.[16], a segurança de informação trata da guarda e recuperação de dados, controlo de acesso, auditoria, logística dos componentes de tecnologia e da segurança organizacional, lógica, física e outras. Ferreira [17] acrescenta ainda, que a segurança pode ser dividida em quatro aspetos:

- Segurança computacional: tem por objetivo proteger o ambiente informático contra eventos inesperados que possam causar algum prejuízo;
- Segurança lógica: prevenir acesso de pessoas não autorizadas à informação;
- Segurança física: evitar acesso não autorizado, danos e interferências nas instalações físicas da organização;
- Continuidade de negócio: visa reduzir a um nível aceitável, por meio de ações preventivas e de recuperação, o risco de paralisação da organização por desastres ou falhas.

Deste modo, podemos definir a segurança de informação como a área do conhecimento e de aplicação dedicada à proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou à sua indisponibilidade.

2.2 Risco

Se há um tema para o qual se encontra variadíssima literatura é o risco. O risco é o grau de incerteza que se tem em relação a um evento e pode ser definido, consoante afirma Gitman [53], "como a probabilidade de perda".

Em relação a segurança, de acordo com Dantas, M [18] os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas e calculado através da fórmula constante na Equação 1. Tal como ilustrado na Figura 1, o risco deve ser analisado seguindo um processo. Na base do processo temos duas grandes áreas: Análise de Risco e Gestão de Risco. O processo de análise engloba a avaliação do risco.

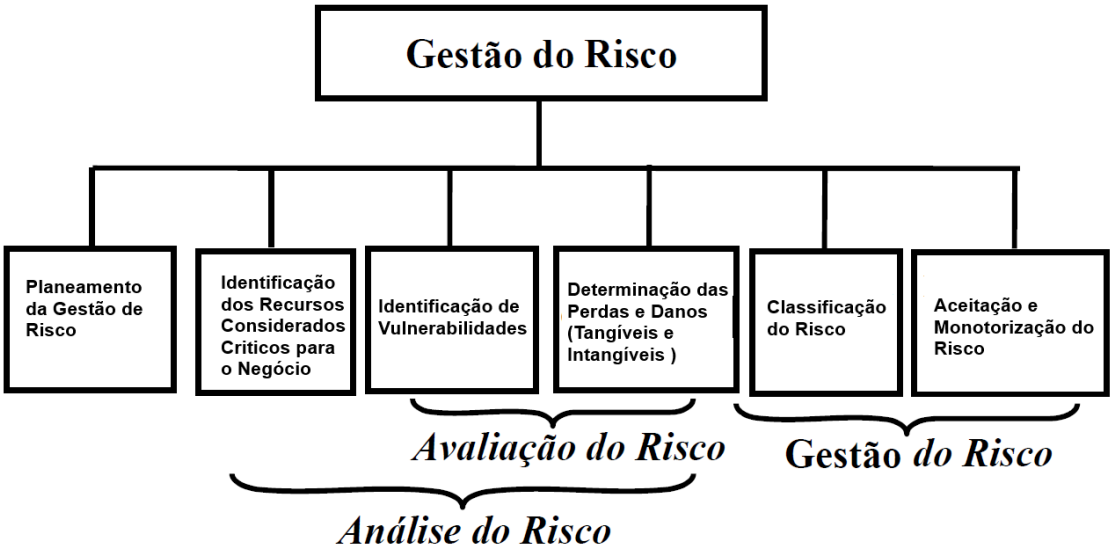


Figura 1: Processo de gestão de riscos (adaptado de [19])

No contexto da segurança de informação, de acordo com Gaivéo [20] o termo "Análise de risco" pode ser entendido como *"o processo que identifica e avalia de forma sistemática, metodológica e repetível os riscos de segurança a que os recursos críticos de negócio das organizações se encontram sujeitos, possibilitando a definição dos meios através dos quais estes podem ser protegidos*". Este processo engloba:

- Planeamento do trabalho a desenvolver, com definição de tarefas e cronograma;

- Identificação dos recursos considerados críticos para a atividade e sobrevivência da organização, recursos estes que são valorizados de acordo com a sua relevância para o negócio, facilidade de substituição e investimento (direto e/ou indireto) necessário para reparação ou substituição;
- Identificação das vulnerabilidades que se encontram associadas a estes recursos e das ameaças a que estes se encontram expostos, bem como a sua probabilidade de ocorrência e impacto esperado (quantificado, sempre que possível);
- Determinação, o mais realista possível, das perdas e danos (tangíveis e intangíveis) associados aos impactos resultantes da concretização de uma ou mais ameaças, sobre um dado recurso. Deste cálculo decorre o nível de risco associado ao recurso em questão;
- De acordo com o nível de risco identificado, segue-se a classificação deste quanto à sua aceitação ou necessidade de mitigação, atendendo ao grau de conforto pretendido pela organização;
- Um nível de risco pode ser aceite caso a organização decida que este não acarreta consequências significativas para a concretização das suas atividades críticas de negócio, sendo que a aceitação de um determinado nível de risco pode, contudo, presumir a realização de esforços no sentido de mitigá-lo, reduzindo-o a um valor considerado aceitável para a organização, dotando-a de um nível de conforto desejável.

Apesar das etapas serem comumente aceites pela comunidade e refletirem as principais recomendações das normas internacionais (ISO´s), quando se chega à fase de análise de risco começam-se a levantar dúvidas que condicionam a implementação dos planos de segurança informática. Estas dúvidas surgem da dificuldade que as organizações têm em quantificar o valor dos bens a proteger e da dificuldade em avaliar o grau de exposição ao risco. Neste âmbito a comunidade académica e a indústria têm proposto vários modelos de análise de risco, mas continua-se a verificar que muitos destes são de complexa aplicação, em particular nas organizações sem recursos humanos dedicados à área da segurança.

A análise de risco e a avaliação da gestão de riscos é a base para a proteção da informação, cada vez mais necessária e indispensável às organizações. Como a gestão de riscos exige uma avaliação precisa, como condição, a análise de risco, segundo Gaivéo [20] é um aspeto indispensável da gestão da proteção de informações para o uso eficiente de consulta, análise e gestão de dados.

O propósito de qualquer análise de risco é fornecer aos decisores a melhor informação possível sobre as vulnerabilidades, ameaças e probabilidade de perda. Como resultado, é importante que os decisores se identifiquem com o método de análise de risco utilizado, e que as informações resultantes sejam úteis e esclarecedoras da situação da organização.

A gestão de riscos é uma das etapas mais importantes da gestão da segurança de informação e leva em consideração as vulnerabilidades e ameaças (Equação 1). Entende-se por vulnerabilidade as falhas ou falta de segurança das quais pessoas mal-intencionadas podem se valer para invadir, subtrair, aceder ilegalmente, adulterar e destruir informações confidenciais. Além de poder comprometer, corromper e inutilizar o sistema. Segundo Campos [10], vulnerabilidades são as fraquezas presentes nos ativos, que podem ser exploradas, seja ela intencionalmente ou não, resultando assim na quebra de um ou mais princípios da segurança de informação. Ao terem sido identificadas as vulnerabilidades ou os pontos fracos, será possível dimensionar os ricos aos quais o ambiente está exposto e assim definir medidas de segurança apropriadas para sua correção.

Dantas M. [18] refere ainda que "*as vulnerabilidades podem advir de vários aspetos: instalações físicas desprotegidas contra incêndios, inundações, e desastres naturais; material inadequado empregado nas construções; ausência de política de segurança para RH; funcionários sem formação e desmotivados nos locais de trabalho; ausência de procedimento de controlo de acesso e utilização de equipamentos por pessoal contratado; equipamento obsoletos, sem manutenção e sem restrições para sua utilização; software sem patch de atualização e sem licenças de funcionamento, etc*". A ameaça, de acordo com o mesmo autor [18] pode ser considerada um agente externo ao ativo de informação, na medida em que se aproveita das suas vulnerabilidades para quebrar os princípios básicos da informação: confidencialidade, integridade ou disponibilidade. Refere ainda, que as ameaças podem ser, naturais: são aquelas que se originam de fenómenos da natureza; involuntárias: são as que resultam de ações desprovidas de intenção para causar algum dano, e intencionais: são aquelas deliberadas, que objetivam causar danos, tais como hackers.

RISCO = (Ameaça) x (Vulnerabilidade) x (Probabilidade da Ocorrência)

Equação1: Risco (ISO 27001)

Todos os componentes de um qualquer sistema de informação podem ser alvo de ataque. O possível dano ao alvo do ataque é chamado de ameaça, e cada ameaça tem os seus possíveis agentes causadores, que tentarão explorar vulnerabilidades e comprometer a segurança. Como refere Nakamura E. [21] *"é preciso entender que muitos ataques são*

resultado da exploração de vulnerabilidades, as quais passam a existir devido a uma falha no projeto ou na implementação de um protocolo, aplicação, serviço ou sistema, ou ainda devido a erros de configuração e administração de recursos computacionais. Isso significa que uma falha pode ser corrigida, porém novos bugs vão aparecer".

A defesa destas ameaças é complexa e onerosa e inclui proteção contra diversos vetores de ataque: *software* malicioso (como os vírus de computador); roubo de dados e ficheiros (impedir que sejam copiados sem autorização); acesso não autorizado por pessoas internas ou externas, interceção e interferência nas telecomunicações, entre outras [22]. Além das ameaças aos dados em trânsito, há a permanente ameaça de acesso remoto não autorizado aos postos de trabalho e aos servidores da organização. Um atacante pode conseguir acesso explorando vulnerabilidades em equipamentos e *softwares* mal configurados, com *passwords* fracas ou que apresentem falhas no desenvolvimento dos *softwares*. A exposição dos sistemas à Internet faz aumentar ainda mais o risco de ataque.

> *Antes do surgimento de aplicações web, os esforços das organizações para proteger-se contra ataques externos foram, em grande parte, focados no perímetro da rede. Defender este perímetro implicou o reforço e correção para os serviços de que precisava expor e bloqueio do acesso a outros serviços.*
>
> *Aplicações Web mudaram tudo isso. […] Se existe uma vulnerabilidade numa aplicação web, um atacante pode, através da Internet, comprometer sistemas internos centrais da organização submetendo apenas dados criados a partir de seu browser* [23].

Face a este cenário é fundamental que as organizações, independentemente do seu tamanho, possam compreender e mapear as ameaças de forma a poder decidir entre: aplicar controlos e medidas de segurança (investir); transferir o risco às seguradoras ou fornecedores, o que também envolve custos; aceitar os riscos ou evitá-los quando possível, eliminando o serviço ou componente alvo da ameaça [13].

Por contarem com poucos recursos disponíveis para investir em tecnologia da informação, as médias e pequenas empresas muitas vezes não conhecem os riscos e mesmo quando os conhecem são obrigadas a aceita-los colocando a organização em perigo. Há ainda que considerar o risco de contágio (pelo efeito em cascata) que a exploração destas vulnerabilidades pode provocar na comunicação com organizações terceiras.

Face a esta situação, é cada vez mais necessário que as organizações formalizem um documento com a sua análise de risco e definição dos ativos a proteger, esta é aliás, uma das motivações para a realização do trabalho. A metodologia agora proposta tem como

objetivo ser uma metodologia de "*entry level*", pelo que se espera que seja de mais simples acesso e aceitação, na compreensão e mapeamento das ameaças no que respeita à gestão do risco da segurança de informação.

2.3 Métodos e orientações atuais de gestão e de análise de risco

Atualmente os sistemas informáticos suportam uma grande parte dos aspetos do nosso quotidiano e têm vindo a permitir uma transformação da nossa sociedade. A par da sua evolução é necessário garantir a segurança dos dados que ai circulam e são produzidos, preservando os princípios básicos da informação. As infraestruturas informáticas são atualmente uma combinação de sistemas, uma verdadeira rede de redes, com frações de tecnologia moderna e obsoleta, combinadas num panorama fragmentado pela partilha entre a propriedade pública e privada e a sua relação. A rápida banalização da Internet e a integração da tecnologia móvel com os computadores ligaram as infraestruturas entre si e criaram uma gigantesca e vulnerável rede de interdependências que está exposta a um grande número de ameaças, internas e externas. Assim, apesar de isoladas fisicamente, as infraestruturas tecnológicas estão sujeitas aos potenciais efeitos em cascata, muitas vezes, resultantes apenas da falha de uma delas. Os sistemas de controlo não raras vezes são vulneráveis a ataques vindos do ciberespaço e este facto foi já demonstrado por diversas vezes numa série de incidentes que causaram grande impacto tanto nas infraestruturas como na sociedade que delas dependem. A identificação e gestão dos riscos associados a estas infraestruturas é hoje uma área que suscita interesse a todos os níveis como forma de assegurar um futuro mais seguro, minimizando o impacto das múltiplas ameaças que pendem sobre o conjunto das infraestruturas informáticas que estão na base do modo de vida das sociedades modernas. Neste sentido, e como refere Natário R. [24] começa a generalizar-se a adição de procedimentos, baseados em normas internacionais, que embora sejam de aplicação genérica podem ser adaptadas às especificidades de cada um e das suas necessidades.

2.3.1 O Papel das Normas para a Segurança de Informação

As normas providenciam um guião que permite a construção de métricas e indicadores de modo a existir eficiência na organização (15). A ISO/IEC e a *National Institute of Standards and Technology* (NIST) [25] são entidades que, a nível mundial, atuam na criação, manutenção e disseminação de normas.

Cabe elucidar, de acordo com Sêmola [55], que "*As normas apenas apontam os aspetos que merecem atenção, indicando O QUE fazer para a adequada gestão, sem, no*

entanto, indicar com precisão metodológica COMO se devem realizar as atividades. É o mesmo que sermos instruídos a realizar com periodicidade anual um check-up do nosso estado de saúde, considerando os sistemas respiratório, circulatório, digestivo, etc., sem que soubéssemos exatamente como fazê-lo, senão procurar um especialista. Este, por sua vez, que detém especificidade, irá aplicar toda a sua base de conhecimento seguindo, com riqueza de detalhes e precisão inerentes à atividade, uma metodologia própria. Um grande "manual" que permitirá considerar todos os pontos importantes para análise e apontará as ferramentas mais apropriadas para cada tipo de exame".

2.3.2 Cybersecurity Framework

Sendo a segurança de informação um assunto com relevância na atualidade, vários têm sido os estudos e a discussão sobre a temática. O NIST [25], que é uma divisão do departamento de comércio dos EUA, através do seu Laboratório de Sistemas de Computação (*Computer Systems Laboratory*), promove padrões abertos e de interoperabilidade com o objetivo de estimular o desenvolvimento económico das indústrias baseadas em tecnologia. Em fevereiro de 2014 o NIST publicou a primeira versão da sua *Cybersecurity Framework* (CSF) em resposta à Ordem Executiva 13636 do presidente dos EUA de fevereiro de 2013. Esta ordem executiva tinha como objetivo aumentar a segurança cibernética e resiliência da infraestrutura crítica do país. A *framework* foi criada com a colaboração entre o governo norte-americano e o setor privado, tendo como foco a gestão de riscos com custos eficientes e permitir que as organizações apliquem princípios e melhores práticas de gestão de riscos para melhorar a segurança e resiliência das suas infraestrutura crítica, independentemente do tamanho da empresa, grau de risco ou sofisticação de seu sistema de segurança [25].

De acordo com SCHNEIER, B [26] A *Cybersecurity Framework* (CSF) utiliza a metodologia de gestão de riscos para permitir que as organizações possam informar e priorizar decisões relativas à cibersegurança. É adaptativa para prover uma implementação flexível baseada na gestão de riscos e é composta por três partes essenciais:

- **Núcleo da *Framework***: um conjunto de atividades de segurança, resultados desejados e referências aplicáveis que são comuns a diversos setores críticos. Compreende cinco funções concorrentes e contínuas, cada uma com categorias (Figura 2) e subcategorias que são relacionadas com padrões e práticas de mercado, tais como COBIT e ISO 27001.
- **Níveis de Implementação** (*Tiers*): providencia contexto para a forma como as organizações vêm os riscos de segurança e os processos para a sua gestão. Esses

níveis caracterizam a organização entre Parcial (Tier 1) a Adaptativo (Tier 4) e refletem o progresso na implementação dos controlos.

- **Perfil:** representa as categorias e subcategorias da *framework* que uma organização selecionou baseada nas suas necessidades de negócio. Os perfis podem ser usados para identificar oportunidades de melhoria ao criar um "perfil atual" e um "perfil desejado" da organização. Também podem ser úteis para a comunicação de padrões de segurança na organização e com outras organizações. As cinco funções do NIST CSF organizam as atividades de segurança ao seu mais alto nível. As vinte e duas categorias são subdivisões das funções em grupos de resultados intimamente ligados a necessidades e atividades específicas. As funções definidas pelo *framework são*:

- Identificar: entender o contexto dos negócios e os recursos que suportam serviços críticos para fazer uma efetiva gestão de riscos a partir das prioridades da organização;
- Proteger: desenvolver e implementar proteções aos recursos que suportam serviços críticos e limitar os impactos de um evento de segurança;
- Detetar: implementar atividades para garantir que os eventos de segurança sejam detetados;
- Responder: responder de forma apropriada aos eventos de segurança para conter os impactos;
- Recuperar: manter planos de contingência e de restauração da capacidade dos recursos afetados por um evento de segurança.

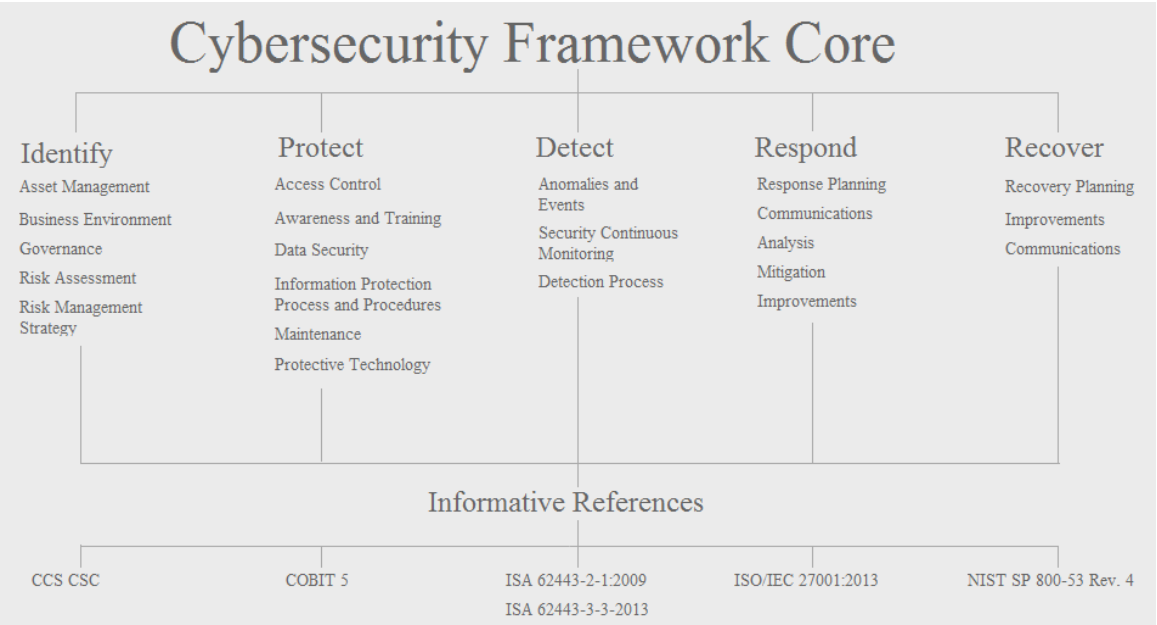


Figura 2: Núcleo da framework NIST, publicado em fev. 2014

2.3.3 Modelos de avaliação de risco

Atualmente, pelos motivos referidos anteriormente, existe uma panóplia alargada de modelos de avaliação de risco. Os modelos de avaliação de risco podem ser divididos em quantitativos e qualitativos. De acordo com Ming-Chang L [27], os modelos quantitativos usam dados objetivos e mensuráveis para determinar o valor de ativos, probabilidade de perda e risco associado (custo-benefício) para cada uma das componentes identificadas. Os modelos qualitativos, com base em categorias normalmente descritivas (baixo, médio, alto, …), avaliam a magnitude do impacto e probabilidade dos riscos identificados de uma potencial ameaça. Ambas as abordagens têm vantagens e desvantagens. A Tabela 1 resume as vantagens e desvantagens de cada abordagem.

	Quantitativo	Qualitativo
Vantagens	• Os resultados podem ser expressos em termos específicos da gestão (por exemplo, valores monetários e probabilidade expressa como uma percentagem específica). • Permite definição das consequências de incidentes de forma quantitativa. • Permite obter uma imagem mais precisa do risco.	• Permite visibilidade e compreensão da classificação de risco. • Mais fácil chegar a um consenso. • Sem necessidade de quantificar a frequência das ameaças. • Não é necessário determinar o valor dos ativos.
Desvantagens	• Valores de impacto atribuídos aos riscos são baseados em opiniões subjetivas dos participantes. • Processo por vezes com cálculos complexos e de demorados consensos.	• Insuficiente diferenciação entre riscos importantes. • Sem base para uma análise custo-benefício. • Resultados mais ambíguos.

Tabela 1: Vantagens e desvantagens dos métodos quantitativos e qualitativos (adaptado de Ming-Chang L [14])

No âmbito do estudo foi feito um levantamento tendo-se identificado, pelo menos, vinte e sete modelos de avaliação de risco em segurança de informação distintos [28, 29, 30, 31, 32]. Destes vinte e sete, dezasseis dizem respeito a modelos de análise de risco qualitativo, um diz respeito a modelos de análise quantitativo e três combinam os dois tipos. Foram ainda identificados sete modelos sobre os quais não foi possível aferir o seu tipo.

O objetivo do Índice de Maturidade de Segurança Informática (IMSI) proposto neste trabalho é o de quantificar de uma forma uniforme, e por isso comparável, o risco sobre a perspetiva da maturidade. Por esta razão as metodologias que assentam em modelos de análise quantitativos são as que melhor se enquadram. Neste sentido, de entre os vários modelos, focamos os quantitativos bem como os que combinam a análise quantitativa e

qualitativa. Para cada um dos modelos analisamos fatores relativos à sua complexidade de aplicação e ao tipo de licenciamento para utilização. A análise tem por base o trabalho realizado por Macedo [28]. A Tabela 2 apresenta o resultado da análise.

Modelos	Análise	Complexidade	Descrição	Licença
ISAMM	Quantitativa	N/A	Os riscos são avaliados em função da sua expectativa de perda anual	N/A
IRAM	Quantitativa e Qualitativa	Médio	Análise baseada em *workshops* com a equipa de informática (IT)	Grátis para subscritores
MAGARETI	Quantitativa e Qualitativa	Médio	Sugere mais do que uma técnica para cálculo de risco (questionários, análise algorítmica)	Grátis
MEHARI	Quantitativa e Qualitativa	Difícil	Análise baseada em questionários, fórmulas e parâmetros. As auditorias são realizadas para identificar potenciais vulnerabilidades nos sistemas de Informação	Pago

Tabela 2: Comparação de modelos de análise de risco quantitativos

Pela importância que estes modelos assumem no âmbito deste trabalho, importa de forma mais pormenorizada descrever os modelos supra mencionados. Para tal, iremos considerar as informações disponibilizadas pela ENISA – "The European Union Agency for Network and Information Security, enquanto centro de conhecimento para a cibersegurança na Europa [33].

2.3.3.1 ISAMM

A metodologia ISAMM- "*Information Security Assessment & Monitoring Method*" [34] ou Método de Monitorização e Análise de Segurança de Informação é um método de gestão de risco para um Sistema de Gestão da Segurança de Informação (SGSI), com ferramentas de apoio. Projetada e continuamente melhorada com base na experiência da *Telindus*, que, em 20 anos de experiência, reuniu milhares de projetos de gestão de riscos e de segurança de informação e dezenas de outras ferramentas e métodos de gestão de riscos. Apesar de

ser considerada uma metodologia de gestão de riscos do tipo quantitativa/qualitativa os seus prossupostos assentam maioritariamente na análise qualitativa, na qual os riscos são expressos em unidades monetárias, por meio do indicador de EAP - Expectativa Anual de Perdas ("*ALE-Annual Loss Expectancy*"). A EAP é a perda ou custo anual esperado caso uma ameaça se materialize e é dada através do cálculo apresentado na Equação 2.

Expectativa Anual de Perdas (EAP) = [probabilidade] x [impacto médio]

Equação 2: Expectativa Anual de Perdas (EAP)

Tal avaliação constitui a base da abordagem baseada no Retorno do Investimento ("*ROI-Return of Investment*") e na capacidade económica da metodologia ISAMM em relação ao plano de tratamento de riscos. A ISAMM simula e exibe o efeito da redução de riscos EAP para cada controlo de melhoria e compara-o ao custo da sua implementação.

As etapas necessárias na análise de riscos usam o maior número possível de controlos da ISO/IEC 27002. O forte apoio à norma ISO/IEC 27001 [13] foi considerado um aspeto importante no projeto e no desenvolvimento da ISAMM.

A última versão da metodologia ISAMM introduziu uma abordagem baseada em ativos, isto significa que ela pode ser usada para realizar a análise de riscos de um único ativo ou em um grupo de ativos.

A análise de riscos ISAMM é composta por três passos/partes principais:

1. Definição do Escopo;
2. Análise - Ameaças e Conformidade;
3. Resultados – Cálculo e Emissão de Relatório.

Conforme as recomendações da norma ISO/IEC 27001 [13] e referido por Ohtoshi P. [54], o primeiro passo na análise de riscos é selecionar os tipos de ativos relevantes e pré-definidos, assim como, definir os ativos mais importantes de cada um desses tipos. Os ativos selecionados devem ser avaliados tendo em consideração os princípios básicos da informação (confidencialidade, integridade, disponibilidade e substituição). O segundo passo consiste em selecionar as ameaças relevantes entre as principais ameaças genéricas pré-definidas. Baseada nessa seleção, a metodologia ISAMM [34] irá identificar os tipos de ativos selecionados de acordo com as respetivas ameaças para gerar um número adequado de cenários. Após o mapeamento das ameaças, a metodologia apresentará todos os controlos que podem afetar esses cenários de riscos.

2.3.3.2 MAGERIT

A "*MAGERIT – Metodología de Analisis y GEstión del Riesgo de IT* [35] é uma metodologia aberta para a análise e gestão de riscos, foi desenvolvida pelo Ministério de

Administração Pública do Governo Espanhol, e é oferecida como um arcabouço e um guia para a Administração Pública Espanhola. Devido à sua natureza aberta, é também utilizada fora da Administração Pública.

Os objetivos da Metodologia *MAGERIT* são:

1. Consciencializar os responsáveis pelos sistemas de informação sobre a existência dos riscos e sobre a necessidade de tratá-los no tempo adequado;
2. Fornecer um método sistemático para analisar estes riscos;
3. Auxiliar a descrição e o planeamento das medidas apropriadas para manter os riscos sob controlo;
4. Indiretamente preparar a organização para os processos de avaliação, auditoria, certificação ou credenciação, conforme o caso.

A versão 2 da Metodologia MAGERIT [35] está organizada em três livros:

Livro 1 – Metodologia: Descreve os passos essenciais e as tarefas básicas, tais como: a elaboração de um projeto de gestão e de análise de risco; a descrição formal do projeto; a aplicação no desenvolvimento dos sistemas de informação, além de oferecer um grande número de sugestões práticas e de fundamentos teóricos e algumas informações complementares.

Livro 2 - Catálogo de Elementos: Oferece os elementos padrão e um critério para a modelagem de risco de sistemas de informação: ativos, classes, medidas de avaliação, critérios de avaliação, ameaças críticas e medidas de controlo a serem implementadas; descreve os relatórios contendo os resultados e as conclusões (modelo de avaliação, mapa de risco, avaliação das medidas de proteção, estado do risco, relatórios de fraquezas e plano de segurança), contribuindo, dessa forma, para alcançar a homogeneidade.

Livro 3 - Técnicas Práticas: Descreve as técnicas normalmente usadas para elaborar projetos de gestão e de análise de riscos tais como: algoritmos de análise e de tabulação; árvore de ameaças; análise de custo/benefício; diagramas de fluxo de dados; diagramas de processos; técnicas para a elaboração de gráficos; planeamento de processos; sessões de trabalho (entrevistas, reuniões, apresentações) e análise Delphi (processo através do qual se recolhe a opinião de especialistas de modo iterativo). A aplicação da metodologia pode ser realizada com a ajuda da ferramenta de *software* PILAR/EAR, que melhora a eficiência e explora as potencialidades da metodologia. A ferramenta PILAR é restrita à administração pública espanhola e a EAR é um produto comercial.

2.3.3.3 MEHARI

A MEHARI [36] é uma metodologia francesa, desenvolvida pelo CLUSIF – *Club de la Securite Informatique Français*. Como principais características da metodologia podemos destacar:

a. Modelo de gestão de riscos baseado em processos e componentes modulares;
b. Inclui uma classificação de ativos – identifica as vulnerabilidades por meio de auditoria;
c. Analisa uma lista de situações de risco estabelecendo um nível de criticidade para cada uma delas;
d. A análise baseia-se em fórmulas e parâmetros;
e. Permite uma seleção otimizada de ações corretivas;
f. Fornece medidas de proteção adicionais em conformidade com as recomendações das várias ISO.

A metodologia MEHARI [36] foi inicialmente projetada para auxiliar as equipas de segurança de informação na tarefa de implantação da gestão da segurança de informação.

A MEHARI [36] é composta por um conjunto de ferramentas especificamente projetadas para a gestão da segurança, que envolve um grupo de ações de gestão e controlo, cada qual com um objetivo específico:

a. Desenvolvimento de planos estratégicos e de segurança;
b. Implementação de políticas e regras de segurança;
c. Aplicação de análises superficiais ou detalhadas do estado da segurança;
d. Gestão e avaliação de riscos;
e. Garantia de inclusão do requisito segurança na gestão de desenvolvimento de projetos;
f. Formação e consciencialização das questões da segurança.

2.3.3.4 IRAM2

A metodologia do ISF [37], Informação Risk Assessment Methodology 2 (IRAM2) foi projetada para ajudar as organizações a entender e gerir os riscos de informação. Segundo o ISF [21] esta metodologia fornece aos profissionais de análise de risco uma abordagem completa para a realização de avaliações de risco de informação com foco em negócios.

Pode-se ainda ler na ficha do produto que a gestão de riscos da informação da IRAM2 tem como intuito ajudar as organizações a:

- **Aplicar uma abordagem simples, prática, mas rigorosa:** foco na simplicidade e praticidade, com incorporação de rigor durante todo o processo de avaliação;

- **Falar uma linguagem comum:** fornecer um vocabulário e uma estrutura comum, permitindo que os profissionais de gestão de riscos da informação detenham uma visão unificada do risco da informação nas diferentes áreas do negócio;
- **Concentrarem-se na perspetiva de negócio:** O risco de informações é avaliado a partir da perspetiva do negócio. O resultado final é um perfil de risco que reflete uma visão dos riscos da informação em termos de negócios;
- **Obter uma maior cobertura de riscos:** Promover uma cobertura mais ampla e mais abrangente do risco;
- **Concentrarem-se nos riscos mais significativos:** concentração dos recursos, a fim de lidar com os riscos de informação que são mais significativos para a organização.

Apesar do anunciado, de acordo com o referido por Barão A. [38] após a realização de testes, verificou-se que a metodologia é pouco objetiva e de difícil aplicação, para além de não contemplar a atribuição de pesos (quantitativos/qualitativos) nos requisitos de segurança para a mitigação das ameaças.

Os modelos, apesar de distintos têm em comum (inclusive os considerados mais simples) uma certa complexidade de implementação. Todos os modelos obrigam a uma fase de literatura extensa e compreensão de informação técnica. Tal complexidade torna-os ininteligíveis para muitas organizações, em particular para as que não possuem recursos técnicos, humanos e financeiros para a sua compreensão e implementação. Sendo modelos complexos as metodologias que tiram partido dos mesmos tendem igualmente a ser complexas. A complexidade tende a ser um entrave à sua aceitação.

A metodologia que propomos tenta eliminar estas condicionante na medida em que: apresenta uma análise quantitativa em contraciclo com a maioria dos modelos identificados; desperta, através de uma linguagem simples, universal e facilmente compreendida pelas estruturas das organizações (baseada em níveis/escalas/percentagens), a consciência e compreensão dos riscos efetivos e da necessidade de os mitigar em prol de uma maior fiabilidade, disponibilidade e confiabilidade da informação.

No próximo capítulo apresentamos a metodologia proposta, baseada em modelos quantitativos e que visa uma rápida e pragmática avaliação dos riscos de segurança de informação apresentada sobre a forma de um Índice de Maturidade de Segurança Informática.

Capítulo 3 - Índice de Maturidade de Segurança Informática

O principal objetivo do trabalho aqui apresentado é criar uma metodologia de referência para o cálculo de um Índice de Maturidade de Segurança Informática (IMSI). Tal metodologia deverá ser simples de aplicar, evolutiva e capaz de permitir a avaliação objetiva das fragilidades com base em critérios específicos e característicos das organizações. A metodologia consiste num guia de referência no qual estão elencados o conjunto de procedimentos a realizar. Está dividida em três áreas funcionais de análise às quais damos o nome de eixo (Figura 3). O emprego da metodologia, além de medir quantitativamente aspetos relativos à segurança de informação, contribui para o aumento da consciencialização da importância da temática, ao nível dos procedimentos, das tecnologias e das pessoas. Esta metodologia é criada com o intuito de ser a base que pode ser replicada entre organizações com o mínimo de esforço de adaptação. Tal metodologia permitirá também, num estado mais maduro, fruto da evolução promovida pelo histórico de aplicação e análise dos resultados extraídos, ser refinada até ao ponto de as próprias organizações, sem grandes requisitos técnicos, poderem efetuar a sua auto-avaliação e, com isso, poderem determinar o seu IMSI de forma continua no tempo.

Os três eixos identificados como ponto de partida para a definição da metodologia são ilustrados na Figura 3.

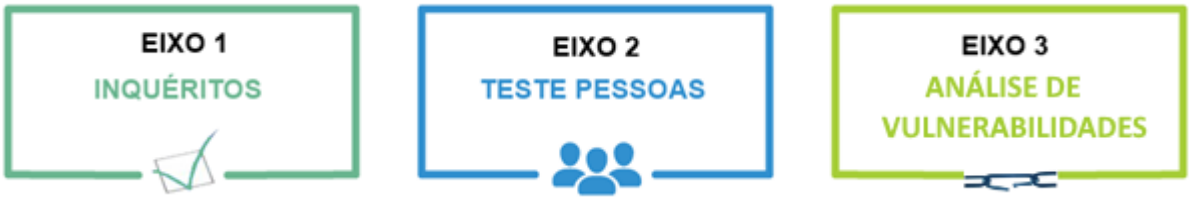


Figura 3: Eixos base de análise para o cálculo do IMSI

O Eixo1 (Inquéritos) é constituído por um inquérito tipo e respetivo modelo de análise considerando diferentes públicos-alvo. Os inquéritos a dirigir ao público-alvo resultam da instanciação de questões pré-definidas e elencadas na própria metodologia facilitando assim todo o processo de criação e análise. Um dos público-alvo é a equipa de IT e avaliará, entre outros, o parque informático, as soluções e medidas de segurança adotadas na organização. Outro público-alvo são os utilizadores de cada organização, e incidirá sobre medidas usadas no quotidiano com vista a aferir o grau de "conhecimento"/sensibilidade sobre os riscos associados à falta de segurança e comportamentos de risco. Por fim a área da gestão, com o intuito de, entre outras, avaliar a importância das questões da segurança

de informação nas decisões. Neste eixo a classificação do nível das organizações tem em consideração as opções de cada resposta, classificadas em cada um dos níveis de forma criteriosa e devidamente justificada. Este eixo é extremamente útil para, partindo dos inquéritos, deduzir o risco potencial relativo a perdas no acesso à informação por via de indisponibilidades ou ataques bem como sobre o extravio de informação ou adulteração de dados. Sendo a segurança de informação uma questão de topo e que a todos diz respeito, o envolvimento e cruzamento dos vários público-alvo é fundamental.

Tipicamente, os inquéritos são instrumentos usados na análise de risco qualitativa. No entanto, como veremos mais à frente, a aplicação e construção de questões com características específicas à definição da problemática a estudar e consequente especificação da metodologia a seguir na recolha e análise dos dados, interpretação e integração dos resultados, de acordo com as hipóteses e problemática, permite-nos a obtenção de dados com valor quantitativo.

No segundo eixo (Teste Pessoas), ir-se-á através do uso de um conjunto de procedimentos e/ou ferramentas testar as pessoas/utilizadores, cujos procedimentos adotados possam por em risco a organização. Também aqui será criada uma classificação de nível quantitativa, balizada em critérios específicos definidos na metodologia.

O terceiro eixo consiste na análise de vulnerabilidades informáticas que possam vir a ser exploradas no âmbito de um ataque. A análise referente a este eixo poderá ser refinada tendo em consideração as vulnerabilidades provenientes dos resultados do eixo 1 e eixo 2, alargada a outras dimensões/análises, nomeadamente os serviços assentes na Web, canal frequentemente usado e explorado pelos hackers. Uma vez que para gerir o risco é preciso conhecer as vulnerabilidades, a análise de risco neste eixo poderá ser facilitada e simultaneamente dar respostas (objetivo) às vulnerabilidades identificadas nos eixos 1 e 2. Este índice será enquadrado num dos cinco níveis, abaixo identificados, tendo em consideração o tipo de vulnerabilidade encontrada.

Para cada eixo de análise será medido um *score* de maturidade de segurança informática. Este *score* mapeia onze grandes áreas de atuação que serão adiante apresentadas.

A curva de nível de referência para o modelo é ilustrada na Figura 4 [8] e apresenta cinco níveis de maturidade delineados em função do maior ou menor cumprimento de itens associados às áreas chave. Esta abordagem foi adotada para o modelo aqui proposto, adequando-se apenas o *focus* de aplicação.

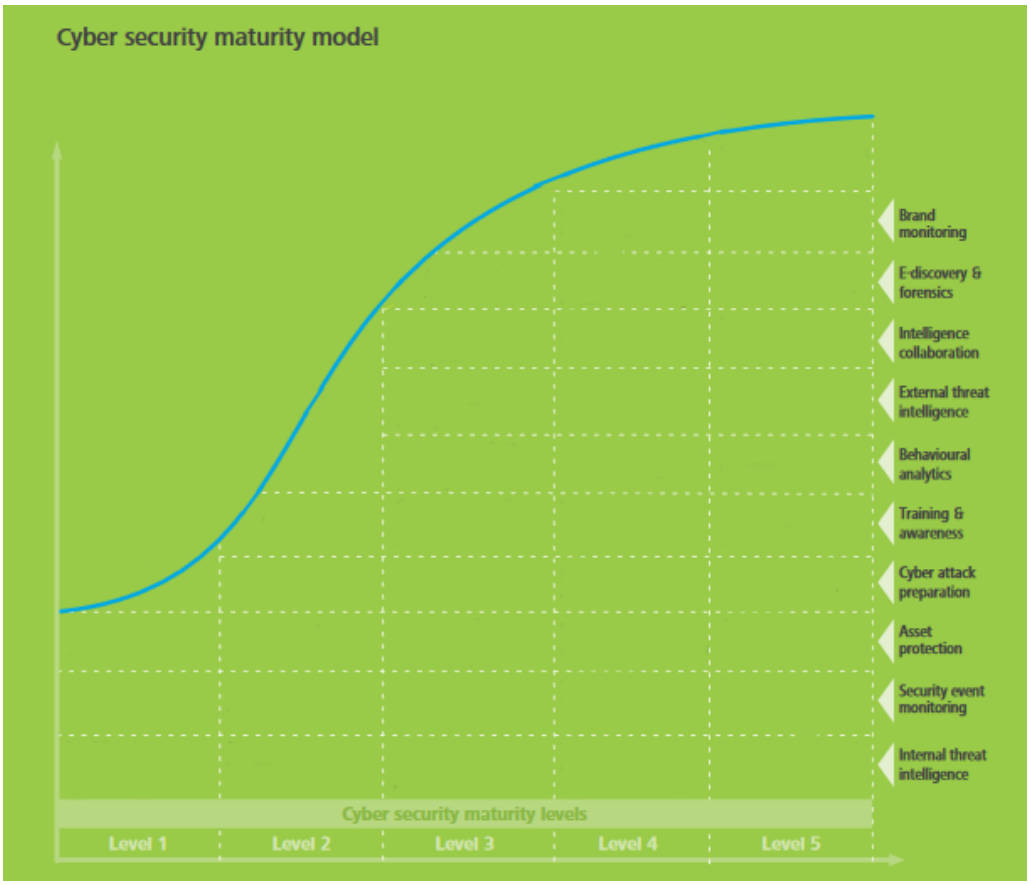


Figura 4: Curva de nível Deloitte

3.1 Metodologia subjacente ao IMSI

Ao longo desta secção será apresentada a metodologia desenvolvida para a determinação do IMSI intra e entre organizações. A metodologia agrega os três eixos apresentados anteriormente.

3.2 Enquadramento de nível

Para o enquadramento de nível, foi adotada a curva de nível apresentada pela consultora Deloitte, "*cyber security maturity mode*l" na sua publicação "*The cyber security imperative – Protect you organization from cyber threats*" (Figura 4) [8]. Pela análise da figura, pode-se observar que a curva foi delineada tendo por base as dez grandes áreas de atuação identificadas pela Deloitte, analisadas e associadas até um máximo de onze áreas da gestão dos riscos distribuídas pelos cinco níveis.

Considerando a experiência da Deloitte na área, começamos por identificar, para um conjunto de pequenas e medias empresas, áreas de atuação que se revelem fundamentais à gestão da segurança de informação. Do exercício, resultaram onze áreas de atuação: (1) Staff adequado, (2) Credenciais, (3) Dependência de sistemas, (4) Formação especifica, (5)

sensibilidades, (6) Auditoria, (7) Análise de risco, (8) Relação com terceiros, (9) Politicas, (10) Monotorização e (11) Controlos. Partindo destas onze áreas, foi possível adotar a curva da Figura 4.

Uma vez que o pretendido é uma avaliação quantitativa, existe a necessidade de quantificar as áreas identificadas para a gestão do risco com vista ao enquadramento de nível das organizações. A opção recaiu sobre a definição de valores percentuais para cada um dos cinco níveis propostos. Considerando as onze áreas de atuação identificadas, o valor percentual de cada nível, que damos como apresentados na Figura 5, foi calculado tendo em consideração a divisão das também onze áreas de gestão do risco ("caixas" distribuídas pelos níveis) apresentadas pela Deloitte (Figura 4). Pela semelhança e igualdade do número das áreas em análise para a gestão do risco, à falta de outro referencial à data e de histórico de aplicação da metodologia aqui definida, adotou-se a curva de nível apresentada, isto é, os mesmos intervalos de nível. Visto tratar-se de um enquadramento de maturidade, depois de uma exausta pesquisa, análise e avaliação, a curva de nível proposta pela Deloitte é, pelos motivos supra citados, a que melhor reflete e apresenta uma divisão equitativa para atribuição deste tipo de análise. Os três primeiros níveis apresentam intervalos mais alargados, ao passo que o nível quatro e cinco, os indicativos de maior maturidade, apresentam um intervalo bastante reduzido, o que limita o número e tipo de fragilidades/ameaças encontradas.

Figura 5: Curva de nível (adotada da Deloitte [4]

Importa salientar que na presente metodologia associado a cada eixo existem cinco níveis de maturidade. A maturidade de Segurança Informática é tanto maior quanto maior for o nível em que a organização se encontre. Em cada um dos eixos haverá lugar ao cálculo de um índice enquadrado num dos cinco níveis de maturidade listados. Cada um dos índices tem validade por si só, porém a análise da maturidade será tanto melhor quanto maior for a cobertura da análise realizada. Para o efeito pretende-se apresentar não só o nível obtido em cada eixo como também o resultado combinado dos eixos. Tanto para o cálculo individual como para o integrado será definida uma fórmula de cálculo uniforme permitindo a comparação dos resultados entre diferentes entidades.

3.3. Inquéritos

A investigação por inquérito é um instrumento útil para o cálculo do Índice de Maturidade de Segurança Informática (IMSI), que usado de uma forma equilibrada em relação à complexidade e à abrangência/profundidade, permite a obtenção e extração de dados que de outra forma seriam mais complexos de obter.

Começa-se por elucidar o planeamento e desenho do questionário e abordam-se, entre outros, a conceção das questões, o desenho do questionário e os métodos de recolha e análise de dados.

No que se refere à análise dos dados apresentam-se as diversas técnicas de análise, nomeadamente o algoritmo a adotar para o cálculo de nível.

Os inquéritos estatísticos são usados para recolher informação quantitativa em várias áreas. Como refere Alves N. [39] "*Um inquérito pode incidir sobre opiniões ou informação factual, dependendo do seu objetivo, mas todos os inquéritos envolvem a administração de perguntas a indivíduos. Quando as questões são administradas pelo inquirido, o inquérito é referido por questionário ou inquérito autoadministrado, caso contrário é uma entrevista".*

Nos processos de análise/tomada de decisão de qualquer organização é essencial obter o máximo de informação sobre o meio que a envolve. Deste modo, os inquéritos, se corretamente utilizados, são meios eficazes de obtenção de informação.

Em qualquer investigação e/ou recolha de dados, os inquéritos estatísticos apresentam algumas vantagens quando comparados com outros métodos:

- São uma forma eficiente de recolher informação de um grande número de inquiridos. Podem ser usadas técnicas estatísticas para determinar a validade, a fiabilidade e a significância estatística;

- São flexíveis no sentido em que pode ser recolhida uma grande variedade de informação;
- São relativamente fáceis de administrar;
- Há uma economia da recolha dos dados devido à focalização providenciada por questões padronizadas, ou seja, não há um gasto de tempo e dinheiro em questões tangenciais.

É necessário ter em consideração que fazer um inquérito é muito mais que construir um questionário. É um processo com múltiplos passos onde cada etapa deverá estar claramente definida. Para se maximizar o sucesso deve-se planear cuidadosamente todas estas etapas desde a forma de recolha da informação até à apresentação dos resultados.

A pesquisa por inquérito, de acordo com o *site* do PSE [40], pode ser dividida em quatro etapas principais, como se mostra na Figura 6. Para que se obtenha sucesso, qualquer das etapas deve ser corretamente implementada. As etapas são:

1. Planeamento e desenho do inquérito;
2. Inquérito;
3. Análise dos dados;
4. Produção do relatório.

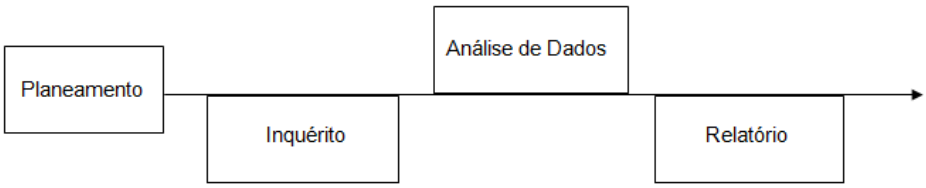


Figura 6: Etapas da Investigação por Inquérito (adaptado de PSE [31])

Antes de se iniciar o processo de construção do inquérito, é necessário determinar os objetivos e recursos do projeto, de forma a tornar o seu propósito claro, aceite e determinante para a concretização do seu objetivo.

"*Um bom formulário começa com uma boa hipótese cuidadosamente estudada*"[41], pelo que a etapa de planeamento assume particular importância em todo o processo.

De modo a aumentar a eficiência, dever-se-á procurar no planeamento e desenho do inquérito as seguintes características:

- Ser claro – os seus objetivos devem ser precisos;
- Fáceis – os inquiridos devem perceber facilmente o seu conteúdo;
- Fiáveis – os dados recolhidos devem traduzir a opinião do inquirido - sem erros;

- Analisado – os dados devem ser sujeitos a análise estatística para se poder inferir resultados e tomar decisões;
- Atempado – o tempo entre o seu planeamento e a obtenção de resultados deve ser o menor possível para que seja útil à decisão.

Tratando-se de um inquérito, cujo objetivo é obter as práticas do uso e manutenção de equipamentos e serviços informáticos das organizações com a finalidade de enquadrar a entidade num dos cinco níveis de maturidade de segurança informática, existe a necessidade, com base nos prossupostos supra expostos, de pensar e desenhar as questões de forma abrangente e capazes de permitirem obter dados suficientemente amplos e transversais a toda esta temática. É necessário considerar e ter em atenção que a construção do questionário e a formulação das questões constituem uma fase fundamental do desenvolvimento de um inquérito [42].

Segundo Ghiglione e Matalon [42], antes de se realizar um inquérito deve-se saber quem se quer inquirir e o que se deve perguntar. Tais fatores levam-nos a propor, para a base da metodologia, a construção de um inquérito dirigido a três públicos-alvo: dirigentes, equipa de informática e utilizadores, onde as questões dos utilizadores deverão, salvo raras exceções e por decisão do inquiridor, ser comuns aos restantes grupos. Esta situação permite, além de outros, obter o valor e importância e sensibilidade com que a segurança de informação é considerada na organização em análise.

Neste processo, é imprescindível a obtenção de uma imagem ampla e transversal de toda a organização, pelo que, além da divisão das questões nos públicos supra mencionada, é imperioso a criação de questões que abordem aspetos relativos às pessoas, processos e tecnologias, em função do tipo, dimensão e área de negócio, conforme ilustração da Figura 7. A análise conjunta destas três áreas é fundamental na medida em que a segurança informática depende de todas.

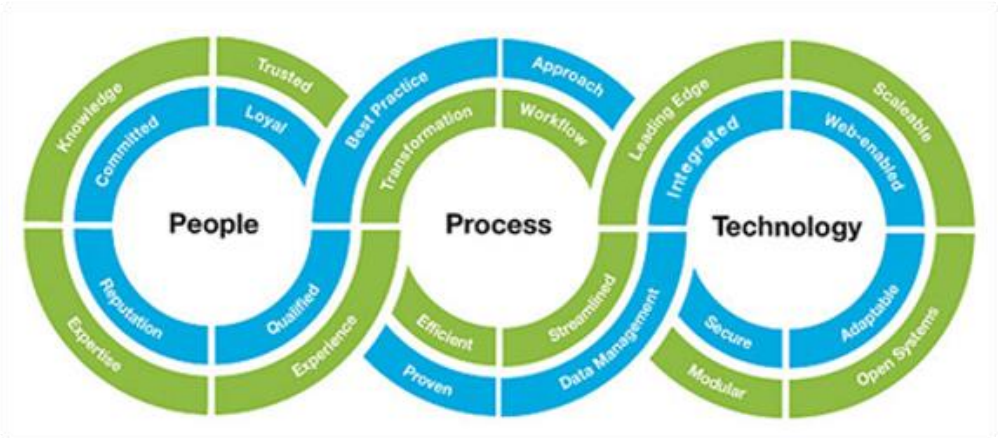


Figura 7: Amplitude do inquérito. Áreas em análise

Outro aspeto a considerar deverá ser o tamanho do inquérito. Considerando que um questionário composto, na sua maioria, por questões fechadas, não deve ultrapassar os 45 minutos, quando a sua aplicação é feita em boas condições, ou seja, em casa do inquirido ou num lugar tranquilo [42], recomendamos, face às condições onde normalmente este será respondido, que o mesmo não deverá ultrapassar os 15/20 minutos ou 30 a 50 questões.

Tal recomendação, não deverá invalidar uma discussão prévia entre a equipa responsável pela criação do inquérito e a estrutura dirigente da organização a avaliar, no sentido de se apurar objetivos claros sobre o tipo de informação a recolher. Tal situação poderá levar à criação de um inquérito com mais ou menos questões das anteriormente sugeridas.

Apesar dos fundamentos/objetivos dos vários métodos de recolha de dados num inquérito serem praticamente os mesmos, é importante salientar que na altura da planificação seja definido o método de recolha de informação a utilizar, pois a construção do questionário depende muito do método escolhido.

Um dos mais importantes e valiosos benefícios dos resultados obtidos a partir do emprego deste método, na metodologia agora apresentada, é o de instigar discussões internas que visem debater a definição do perfil da organização para determinar o nível de exposição ao risco, a sua aceitação, priorização e investimento, pelo que importa, obter um imagem abrangente e global sobre esta temática.

Neste sentido, o inquérito deverá ser o mais transversal possível, levando em consideração as áreas identificadas, o foco do problema e o objetivo final. Para tal, deverão ser instanciadas questões nas áreas chave da organização que permitam aferir as práticas correspondentes aos níveis/objetivos definidos. Na Tabela 3 constam as áreas chave que a metodologia proposta contempla. A aferição das práticas por área chave está elencada por nível de maturidade e organizada nas três áreas principais. Os níveis são cumulativos, isto é, o nível sequente, depende dos seus antecessores.

Foco/Área	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
Pessoas	- Os colaboradores têm pouca ou nenhuma consciência dos riscos de segurança. - Inexistência de uma equipa e/ou pessoas com formação e sensibilidade na área	Existe uma consciência dos riscos da segurança cibernética por parte das pessoas Existência de um departamento ou pessoa com conhecimento geral na área da informática	- Os colaboradores dispõem de oportunidades de formação na área. -Consciência dos riscos da segurança de informação e práticas abusivas Equipa informática com conhecimentos na área da segurança de informação	Equipa informática com conhecimento e habilidades necessárias a identificar e mitigar os riscos. Colaboradores conscientes dos riscos da segurança de informação, com formação sobre as boas práticas	Equipa dedicada à análise, identificação e correção de ameaças/riscos Os colaboradores recebem com regularidade formação relacionada com a cibersegurança
Processos	As decisões de negócio não priorizam nem contemplam uma avaliação de ameaças e riscos A informação de riscos e ameaças não é comunicada aos stakeholders internos Riscos geridos de forma reativa e *ad hoc*	As decisões do negócio contemplam uma avaliação do risco nas principais áreas do negócio A informação de riscos e ameaças é comunicada aos superiores, sempre que se justifique Existência de um plano de segurança	As decisões do negócio contemplam uma avaliação de risco nos contratos com terceiros. Existência de um plano de segurança, sem periodicidade de revisão. A informação de riscos e ameaças é comunicada aos superiores periodicamente	As decisões do negócio consideram as questões da segurança de informação Existência de um plano de segurança, revisto periodicamente Definição de processos e procedimentos por área de negócio A informação de riscos e ameaças é comunicada a todos *stakeholders* internos	A gestão de riscos da segurança cibernética é uma parte integrante da cultura da organização. Existência e utilização de políticas no conhecimento dos riscos, Processos, procedimentos e responsabilidades Riscos geridos de forma pro-ativa

Tecnologias	Inexistência de ferramentas para gestão de riscos	Insuficiência de ferramentas para a gestão e resolução da exposição ao risco. Tecnologia implantada, não revista, em função das principais ameaças à data de instalação	A implantação de ferramentas pode não cobrir adequadamente as áreas de exposição ao risco Existem ferramentas mas não são adequadamente verificadas ou atualizadas. A tecnologia utilizada, na sua maioria, acompanha as ameaças atuais	As ferramentas de implantação são rotineiramente ajustadas e mantidas A tecnologia utilizada acompanha as ameaças atuais	As ferramentas e tecnologias Implantadas não só visam as ameaças atuais como antecipam ameaças emergentes Os instrumentos utilizados são regularmente avaliados ao nível da eficácia e cobertura contra mudanças do ambiente e da ameaça

Tabela 3: Foco de análise por nível e por área.

Além das áreas apresentadas, deverá ser considerado aquilo que podemos designar por "ecossistema", isto é, a relação da organização com terceiros e o efeito de cascata e exposição ao risco que essa relação pode provocar.

Face à abordagem (pessoas, processo e tecnologias) e ao objetivo, estudo e experimentação do conceito, recomenda-se a instanciação de um inquérito assente nos objetivos e tipo de informação a recolher. Para tal, e atendendo às áreas supra citadas e à possibilidade da existência da criação de questões através de várias combinações possíveis, é conveniente a existência de reuniões prévias com as várias estruturas na definição das questões e no foco do problema a tratar.

Ainda no que concerne à estrutura do inquérito e conceção das questões, é recomendado a existência de questões para enquadramento da entidade, não assumindo, por isso, relevância para a análise e enquadramento de nível podendo, no entanto, permitir análises mais profundas, como seja comportamentos por faixa etária, sexo, dimensão da organização, entre outras.

As restantes questões, em função da importância e universalidade que representam para o risco, devem ser divididas em pelo menos dois tipos. A divisão é um fator essencial, na medida em que permite a atribuição de uma maior ou menor valorização na quantificação do risco em determinadas práticas que as organizações consideram mais

relevantes e potenciadoras de causar prejuízos no negócio. É por isso, que a definição das questões para cada um dos níveis, devem ser definidas tendo em consideração uma amostra representativa das entidades envolvidas e a partir de um dos seguintes métodos:

- Pré-inquérito distribuído às estruturas de gestão, onde seja possível aferir as áreas cujo incumprimento comporte mais riscos para a organização ou conjunto de organizações: Perceção do risco;
- Entrevista com as estruturas de gestão que permitam aferir e nivelar o resultado constante no ponto anterior.
- Grupo de especialistas na área (experts), que classificarão as questões em função dos objetivos definidos.

Para o resultado final concorrem todas as questões com relevância divididas em dois tipos, sendo que as perguntas de tipo 1, as que definidas como questões que comportam mais risco para as organizações em estudo, deve ser atribuído um peso superior do que às perguntas de tipo 2. O peso a atribuir a cada uma das questões deve ser definido em percentagem (%) e em acordo com as estruturas de gestão envolvidas. As questões do tipo 1 devem ter sempre uma valorização superior às questões do tipo 2.

Para a divisão das questões em dois tipos

Para o cálculo da percentagem de questões atribuídas a cada tipo devem ser usadas as Equações 3 e 4.

$$\text{Percentagem de questões tipo 1} = (TQ1/\ NTQ * 100)$$

Equação 3 – Percentagem de questões tipo 1

$$\text{Percentagem de questões tipo 2} = (TQ2/\ NTQ * 100)$$

Equação 4 - Percentagem de questões tipo 2

Na Equação 3 e 4, o dividendo (TQ1 ou TQ2) é o número total de questões identificadas como sendo do tio 1 (TQ1) ou de tipo 2 (TQ2) e o divisor (NTQ), o número total de questões apresentadas a cada público-alvo no inquérito. Exemplo, um inquérito com cinquenta questões, onde dez foram identificadas como de tipo 1 e quarenta de tipo 2, teríamos os seguintes resultados:

$$\text{Percentagem de questões tipo 1} = (10/50 *100) = 20\ (\%)$$
$$\text{Percentagem de questões tipo 2} = (40/50 *100) = 80\ (\%)$$

Como o pretendido é atribuir cotações/valorizações diferentes, em função do tipo, a metodologia prevê a atribuição de uma cotação alicerçada e baseada na percentagem das questões identificadas, através do emprego da função de proporcionalidade inversa, isto é,

considerando o exemplo anterior, iremos atribuir um peso de 80% para as questões de tipo 1 (as consideradas mais importantes e que correspondem a 20% do total das questões) e 20% às questões do tipo 2 (menos relevantes para o estudo e que representa 80% do total das questões).

Em função dos cálculos efetuados, é necessário atribuir um valor às questões para cada um dos dois tipos. Esta atribuição de valor é necessária para o cálculo do score final. O valor atribuído as questões é calculado através da divisão da percentagem das questões do tipo pelo número de questões atribuídas a esse mesmo tipo (exemplo nível 1: 80(%)/10 = 8; exemplo nível 2: 20(%)/40= 0.50).

Assim e levando em consideração o supra transcrito para um inquérito com cinquenta questões para o total dos grupos inqueridos, onde vinte e quatro (colaboradores) são comuns a todos os grupos e as restantes vinte e seis são divididas pelo grupo de informática e gestão, depois de definidas as questões do tipo 1 e tipo 2 para cada um dos grupos, com o emprego da proporcionalidade inversa no peso dos tipos de questões, os resultados são os apresentados na Tabela 4.

	Gestão				**Informática**				**Colaboradores**			
Questões	**35 (24+11)** (NTQ)		**peso Inverso** (PI)	**Valor** (V= PI/NTQ)	**39 (24+15)** (NTQ)		**peso Inverso** (PI)	**Valor** (V= PI/NTQ)	**24**		**peso Inverso** (PI)	**Valor (PI/NTQ)** (V= PI/NTQ)
Tipo 1	9	25,71%	74,29%	8,25	9	23,08%	76,92%	8,55	6	25%	75%	12,5
Tipo 2	26	74,29%	25,71%	0,99	30	76,92%	23,08%	0,77	18	75%	25%	1,39

Tabela 4: Exemplo de Cálculo para cotação de questões

Com o emprego da proporcionalidade inversa, o cálculo da média final para enquadramento de nível, é obtido através da soma dos pesos finais. Os pesos finais, são calculados através da multiplicação do peso inicial da questão (V) pelo valor percentual obtido em cada uma das questões.

3.3.1 Algoritmo de cálculo do IMSI

Seguidamente apresenta-se um algoritmo com o resumo dos cálculos do IMSI dos inquéritos (Eixo 1).

Algoritmo de cálculo do IMSI do Eixo 1

1. Segmentar Questões por tipo (grau 1 (maior risco) ou grau 2 (menor risco))
   1.1. Determinar a percentagem de questões de cada tipo (PQ_i)
   1.2. Determinar o fator de questões de cada tipo (peso) (P_x=1-PQ_i)
   Quando: x=1, i=2 e quando x=2, i=1
2. Analisar Respostas aos Inquéritos
   2.1. Obter percentagens de respostas por questão (resultado em %) – R
   2.2. Multiplicar a % de respostas em cada questão pelo fator ($F=P_x*R$) resultante em 1.2, isto é, associado ao respetivo tipo
   2.3. Resulta do 2.2 o valor ponderado face ao tipo (F)
   2.4. Soma de todos os valores de 2.3 ($RF = \sum_{n=1}^{nº\ Questões} F_n$)

3. Obter o Valor do IMSI
   3.1. Posicionar o valor RF na curva de nível

Figura 8: Algoritmo de cálculo do IMSI do eixo 1

3.3.2. Cálculo Individual das questões

Nada foi ainda referido sobre a forma de análise das respostas (R). No inquérito base existem três grupos principais de questões. Cada grupo tem a sua particularidade para análise.

3.3.2.1 Questões do grupo 1 (Sim/Não)

Para as questões cuja resposta é ***Sim*** ou ***Não*** a forma de cálculo para cada questão no questionário distribuído na organização, é feita através do somatório das respostas às questões, onde a totalidade de Sim ou Não, dependente do sentido da pergunta, é atribuído 100%, sendo feito o correspondente em % aos resultados obtidos desse somatório/questão.

Nas questões onde existem pergunta adicionais que sustentam e balizam a pergunta inicial, como por exemplo *"Tem conhecimento da existência de um plano de boas práticas e normas de segurança informática na organização?"*, além de se efetuar o cálculo em função do transcrito no parágrafo anterior, a mesma deverá ser condicionada aos valores obtidos na questão, ou somatório da questão seguinte e que a sustenta. Para tal, deverá ser

atribuído um valor percentual às opções de resposta, que se aconselha que seja medido numa escala de um a cinco. Exemplo de questão:

Uma vez que respondeu afirmativamente, indique: (de 1 a 5)
(sendo 1 nada claro/indisponível e 5 perfeitamente claro/disponível)
Acessibilidade do plano
Disponibilidade e atualização do plano
Clareza das políticas de Segurança definidas no plano
Compreensão das responsabilidades atribuídas aos colaboradores/ departamentos relacionado com a negligência informática

Neste caso e em função do transcrito, teríamos um peso de 20% (100/5), pelo que o resultado final será o valor da questão inicial (VQI) a multiplicar pela média obtida $\bar{X}$ (entre 1 e 5 – 20% e 100%) das alíneas da questão seguinte, que sustenta e está relacionada com a resposta à questão anterior.

$$F = VQI + \bar{X}, onde\ \bar{X} = \frac{\sum_{i=1}^{N} c}{N}$$

Equação 5 – Cálculo de questões do padrão 1

X_i corresponde à resposta dada pelos inqueridos na escala de 1 a 5. Neste caso o valor de R, apresentado no algoritmo, resulta da Equação 5.

3.3.2.2 Questões do grupo 2 (Cruzamento de dados)

As questões do grupo 2 são todas as questões, cuja análise de resposta obedece a um cruzamento de informação, entre as várias questões relacionadas e opções apresentadas, no sentido de se obter um valor/imagem final esclarecedora sobre determinado tema.

Como exemplo, na temática da segurança de informação, a existência de *passwords*, é uma primeira linha de defesa. Neste sentido, torna-se imperativo a existência de perguntas relacionadas com toda esta temática, sendo aconselhável, pela transversalidade da análise e pelo a seguir exposto, o uso das questões com os temas apresentadas.

Apesar da numa primeira análise ser tentador a atribuição de nível individual às questões que se relacionam com as *password*s, balizada no conteúdo da questão e no senso comum, tal não se padece com rigor e correção que se pretende para o cálculo do

IMSI, motivado pela complexidade de análise e fatores que concorrem para aquilo a que podemos chamar da qualidade e força da *password*.

A força de uma *password*, está intimamente ligada à forma e métodos que os atacantes utilizam para a quebrar.

Para a força da *password* concorrem, entre outros, fatores como tamanho e tipo de caracteres. Numa primeira análise, somos tentados em afirmar que uma *password* com mais caracteres é mais segura. Tal situação nem sempre corresponde à verdade, na medida em que existe um conjunto de palavras comumente aceites e utilizadas nas *passwords*, facilmente encontradas na web, e que os atacantes utilizam na metodologia a usar num ataque de força bruta, o que faz com que, por exemplo, "*pqzrwj"* seja uma password mais segura que *"password1".*

Não havendo consenso nem métodos precisos no que se refere à escolha de *passwords* e análise da sua segurança, pois como referido anteriormente, a força de uma password, está intimamente ligada à forma e métodos que os atacantes utilizam para a quebrar, existem combinações que nos podem dar mais ou menos confiança.

Após análise dos algoritmos apresentados pela *passwordmeeter* [43] e *Kaspersky* [44] e de exaustivos testes de aperfeiçoamento e validação do modelo definido, usando a informação disponível sobre a temática, optou-se para o caso das *passwords*, por um sistema de pontos de forma a simplificar o processo e torna-lo inteligível pelas várias estruturas.

- **Tamanho** – Atribuição de seis pontos para cada caractere que compõe a *password*, até um máximo de sessenta pontos;
- **Por utilização de minúsculas** – São concedidos cinco pontos se a *password* inclui uma letra minúscula. Serão atribuídos dez pontos se existir mais de uma letra minúscula;
- **Por utilização de maiúsculas** – São concedidos cinco pontos se a *passwor*d inclui uma letra maiúscula. Serão atribuídos dez pontos se existir mais de uma letra maiúscula;
- **Por caracteres numéricos** – São concedidos cinco pontos se a *password* inclui uma caracter numérico. Serão atribuídos dez pontos se existir mais de um caracter numérico;
- **Por utilização de símbolos** – São concedidos cinco pontos se a *password* inclui um símbolo. Serão atribuídos dez pontos se existir mais de um símbolo;
- **Pela utilização de informação pessoal e palavras conhecidas** – Caso não estejam presentes, serão atribuídos 15 pontos a cada uma das opções. No caso de estarem presentes, serão retirados 30 pontos a cada uma das opções;

- **Pela intercalação de caracteres** – Em caso afirmativo serão atribuídos 15 pontos. Serão retirados 30 pontos se não existir.

Para o cálculo final, utilizamos o seguinte algoritmo:

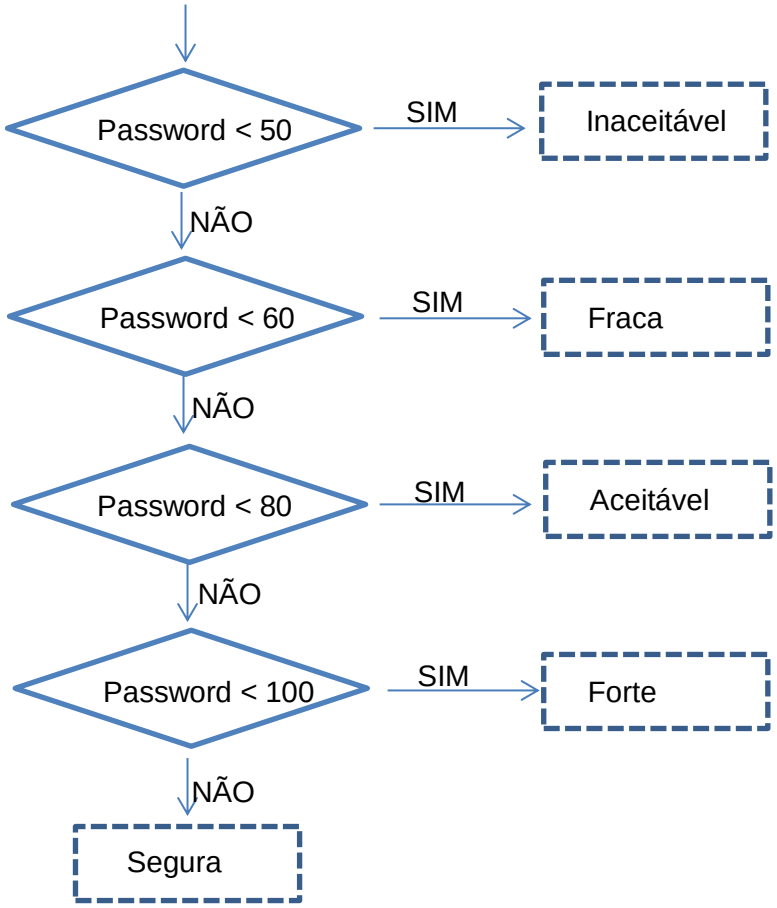


Figura 9: Algoritmo para o cálculo da força da password

Cada categoria/posição definida no algoritmo corresponde a um dos 5 níveis propostos, onde "inaceitável", corresponde ao nível mais baixo (1) e "Segura", ao nível mais elevado (5). O valor de R apresentado no algoritmo da Figura 8 resulta do valor obtido pelo algoritmo anterior (Figura 9) a multiplicar pelo valor máximo de cada nível (38, 75, 93, 98 e 100) a dividir pelo valor definido na categoria/posição onde se insere. A título de exemplo, para um valor de 75 pontos, teríamos o seguinte resultado:

75*93/80 = 87,19 %
valor obtido (75) * valor máximo do nível (Aceitável = nivel3 = 93) / valor definido na categoria/posição onde se insere (80)

3.3.2.3 Questões do grupo 3 (várias opções de escolha)

Existem ainda questões que apresentam opções de escolha. Cada opção deve corresponder a um nível mapeado numa escala de 1 a 5, onde, de acordo com a metodologia, o nível 1 é o mais baixo e o 5 o mais forte. O cálculo da percentagem final da questão, à semelhança do grupo anterior, é obtido através do somatório da multiplicação do valor máximo de cada nível (38, 75, 93, 98 e 100) pelo número de respostas desse nível a dividir pelo somatório do número de respostas, obtendo-se um valor entre 0 e 100, ou seja, o valor de R apresentado no algoritmo da Figura 8.

Apresentamos a seguir exemplo deste tipo de questões:

Bloqueia a sessão de trabalho do seu computador quando se ausenta?
Não, nunca ninguém me disse para o fazer. *(resposta de nível 1)*
Não tenho por hábito faze-lo. *(resposta de nível 2)*
Bloqueio mas apenas em ausências prolongadas. (resposta de nível 3)
Bloqueio frequentemente *(resposta de nível 4)*
Bloqueio sempre *(resposta de nível 5)*

De acordo com o exemplo, as opções de resposta têm relação direta com os níveis definidos, onde “Não, nunca ninguém me disse para o fazer”, corresponde ao nível mais baixo (1) e “Bloqueio sempre”, ao nível mais elevado (5).

Como exemplo para o cálculo anteriormente citado, considerando um inquérito respondido por 20 pessoas, a recolha de dados e cálculo de nível é a ilustrada na Tabela 5.

Bloqueia a sessão de trabalho do seu computador quando se ausenta?	Nº de Respostas	Valor Atribuído (máximo de % de cada Nível)	Resultado (respostas x valor atribuído)
Não, nunca ninguém me disse para o fazer.	3	38	114
Não tenho por hábito faze-lo.	2	75	150
Bloqueio mas apenas em ausências prolongadas.	12	93	1116
Bloqueio frequentemente	3	98	294
Bloqueio sempre	0	100	0
Resultado de nível (R): somatório do resultado a dividir pelo número total de respostas:			**83,70 (%)**

Tabela 5: Exemplo de cálculo de nível para vinte respostas numa pergunta do padrão 3

3.4 Engenharia Social – Teste de Pessoas (Eixo 2)

No espectro da segurança de informação, poder-se-á definir engenharia social como às práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da exploração da confiança e descuido das pessoas. Para Kevin Mitnick [46], famoso *hacker* e, atualmente, consultor de segurança *"a Engenharia Social é o uso da manipulação, engano e influência sobre um indivíduo pertencente a uma organização, para que este adira a um determinado pedido. Esse pedido poderá consistir na divulgação de determinada informação ou o desempenho de determinada tarefa que beneficia o atacante. Poderá ser tão simples quanto falar ao telefone, até algo tão complexo como fazer com que o alvo visite um determinado Website que explore uma falha técnica e permita ao hacker tomar conta do sistema*".

A engenharia social é uma forma de invadir as organizações sem necessidade do uso da força bruta ou da exploração de erros nas máquinas ou nos seus sistemas. O objetivo da engenharia social é explorar as falhas de segurança das próprias pessoas que, quando não são formadas ou não estão devidamente ao corrente dos perigos de determinadas práticas de ação para esse tipo de ataques, podem ser manipuladas.

É importante salientar que, a engenharia social é aplicada em diversos setores da segurança de informação independente dos sistemas computacionais, *software* e ou plataforma utilizada, o elemento mais vulnerável de qualquer sistema de segurança de informação é o ser humano, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques deste género. A engenharia social, pela sua simplicidade e engenho, é a forma mais fácil e eficaz de tornear os obstáculos que os sistemas de segurança impõem.

Neste eixo além de explorarmos os conceitos de engenharia social e as suas manifestações mais populares, apresentamos uma metodologia para avaliar a maturidade das organizações no que diz respeito à resiliência deste tipo de ataques. O propósito é gerar informação para a criação de formas de deteção, prevenção e combate. A importância do tema para as organizações e para a economia em geral fazem surgir a necessidade de tal metodologia, no sentido de identificar antecipadamente as suas vulnerabilidades para uma sensibilização em torno destas ocorrências e para a definição de uma política de segurança clara e comum a toda a organização.

3.4.1 Metodologia

Sendo o ser humano o elemento mais vulnerável de qualquer sistema de segurança de informação os testes à maturidade das pessoas sob a perspetiva da segurança

informática são fundamentais. Este tipo de testes permite dotar as várias estruturas de decisão de um conhecimento mais real e efetivo das práticas e vulnerabilidades da sua organização.

A segurança de informação, é um termo bastante lato e raramente visto e analisado nas suas mais diversas formas. Do ponto de vista da exposição ao risco de nada adianta investir em sistemas tecnológicos e de proteção altamente avançados, se a seguir, por exemplo, não se cria proteção para a forma como as pessoas cedem as suas credenciais de acesso perante um engenheiro social.

O uso da engenharia social, através das suas mais variadas formas (presencial, telefónica, e-mail, entre outras) visa essencialmente obter:

- Dados pessoais;
- Credenciais de acesso;
- Informação do negócio;
- Instalação de códigos maliciosos;
- Causar ruido ao negócio.

A determinação Índice de Maturidade de Segurança Informática relacionado com o eixo Pessoas deve ser feita a partir de duas principais etapas, cada um composta de várias fases e em constante interação: preparação da ação de engenharia social; execução da ação.

3.4.1.1 Etapa 1: preparação da ação

A equipa ou pessoa responsável por operar esta etapa do eixo 2 deverá avaliar e promover reuniões com a gestão e equipa de informática das organizações no sentido de apurar:

- Objetivos pretendidos;
- Formas de funcionamento da organização: Restrições no uso de serviços, nomeadamente a Web e gestão de correio eletrónico, formas de atuação/organização dos serviços;
- Regras: delinear e criar cenários suscetíveis de comportamentos incorretos por parte dos utilizadores;
- Delinear e quantificar os critérios para enquadramento de nível. Estes critérios podem passar pela atribuição de fatores de importância a cada teste, até, por exemplo, à concordância da percentagem de pessoas na globalidade dos analisados, que atuam de forma incorreta.

3.4.1.2 Etapa 2: execução da ação

Não havendo um fronteira explícita entre as etapas, esta segunda etapa visa essencialmente a delineação da estratégia e ação, decorrente dos objetivos e regras definidas e instituídas na primeira etapa.

Esta etapa é constituída pelas seguintes fases:

- Recolha de informação dos alvos;
- Relacionamento com os alvos – Construção do perfil do engenheiro social;
- Dar "corpo" aos cenários previamente definidos - Executar a ação/testes;
- Recolha, análise de dados e elaboração do relatório.

Sendo uma prática em uso atualmente, a metodologia agora apresentada resulta do cruzamento e análise dos métodos atuais. Um dos que mais se aproxima da metodologia apresentada é a metodologia usada pela *7–network* da *ITsupport* [47] que se dedica à área da segurança, sendo parceira e certificada por alguns dos gigantes das tecnologias. Esta metodologia apresenta como *core* para o processo de análise de a engenharia social cinco fases de acordo com a Figura 10.

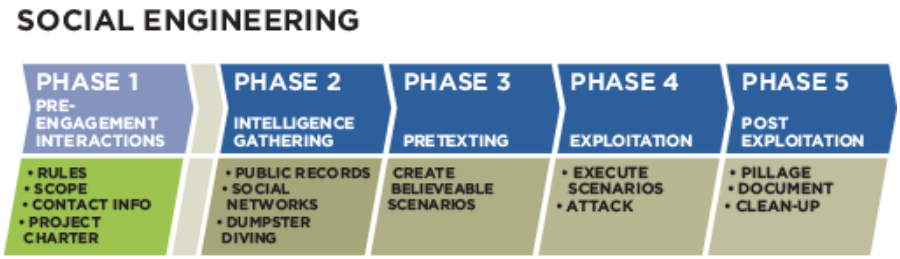


Figura 10: Fases da Engenharia Social

Para a estruturação e planeamento dos cenários, propomos que sejam definidos, em fase prévia à ação, os fatores ilustrados na Tabela 6.

Complexidade	Simples/média/ Avançada	Tipo Ação	Phishing/ Outra	Template	Definição
Objectivo	Definição dos objetivos em função da reunião estabelecida com a organização na definição dos casos. Exemplo: Avaliar se o colaborador é vulnerável a visitar sites desconhecidos.				
Alvo	Definição dos alvos. Exemplo: Colaboradores em geral; determinado departamento, entre outros.				
Descrição	Descrever o objetivo pretendido. Exemplo: Este exercício utiliza dados de contexto para convencer um colaborador a clicar num link e abrir um ficheiro aparentemente inofensivo.				
Pré Requisitos	Definição dos pré-requisitos necessários. Exemplo: Lista de e-mails; Base de Dados dos colaboradores, entre outros.				
Meios de Comunicação	Meio usado para executar o ataque. Exemplo: E-mail.				
Exemplos	Descrição do ataque a executar. Exemplo: Departamento interno ou entidade externa a informar sobre novos procedimentos.				
Output	Definição dos dados a extrair e relatório a executar. Exemplo: O Relatório de ação contém a taxa de cliques relativamente ao número total de colaboradores, que colaboradores clicaram no link, quantos abriram o ficheiro e ações recomendadas.				

Tabela 6: Definição da estrutura dos ataques a executar

No propósito da metodologia o uso de engenharia social para o cálculo do Índice de Maturidade de Segurança Informática assume-se como fundamental, na medida em que permite fazer um cruzamento de dados entre a resposta dos inqueridos (eixo 1) e a prática efetiva. Esta situação permite aferir o grau de consciência dos utilizadores (o que deve ser feito e o que efetivamente fazem), para além de permitir de uma forma mais rápida, facilitadora e económica, quantificar o risco e formar e/ou sensibilizar os utilizadores para os riscos e vulnerabilidades que determinados comportamentos (negligentes ou por desconhecimento) representam ou podem representar para o negócio.

De salientar que qualquer um dos eixos e respetivas etapas ou procedimentos deve ter a total concordância, apoio e envolvimento da estrutura de gestão, isto porque "*Em primeiro lugar, muitas vezes é difícil obter o apoio da própria alta administração da organização para realizar os investimentos necessários em segurança de informação. Os custos elevados das soluções contribuem para esse cenário, mas o desconhecimento da importância do tema é provavelmente ainda o maior problema*" [48].

3.4.2. Algoritmo de cálculo do IMSI

Os resultados obtidos neste eixo tem validade por si só, devendo no entanto, em função do estabelecido e acordado com a gestão da empresa, concorrer para o *score* e ponderação final.

Seguidamente apresenta-se um algoritmo com o resumo dos cálculos do IMSI do Eixo2.

Algoritmo de cálculo do IMSI do Eixo 2

1. Preparação da ação
   - 1.1. Reunião com as estruturas para apresentação do tipo de campanhas possíveis
   - 1.2. Selecionar o tipo de ação
   - 1.3. Determinar os pré-requisitos
   - 1.4. Obtenção de autorizações
   - 1.5. Recolha da lista de alvos

2. Desenho da ação
   - 2.1. Construir o cenário (E-mail, Landingpage, …)
     - 2.1.1. Lista de consequências (LC)
     - 2.1.2. Definição dos critérios de análise: Ação – Consequência – Nº de ocorrências - Nível (1 a 5) – Pode ser feito em conjunto com a organização.
   - 2.2. Testes internos ou grupo de testes
3. Execução da ação
   - 3.1. Lançamento da campanha
   - 3.2. Recolha de resultados
4. Cálculo do IMSI: Advém da LC resultante do 2.1.1 e acordado, para mapeamento nos níveis em 2.1.2 (número de LC permitidas em cada nível)
5. Posicionar o valor RF na curva de nível

Figura 11: Algoritmo de cálculo do IMSI do eixo 2

Tratando-se de um eixo sensível, onde o comportamento errado de apenas um elemento, pode por toda a organização em causa, é necessário um planeamento cuidado

quanto ao número, tipo de ocorrência e consequência. O número/percentagem de elementos com comportamento de risco fornece informação útil, nomeadamente na estratégia a seguir para colmatar esses comportamentos (ex. Plano de formação, definição de politicas de segurança, entre outras).

A titulo de exemplo, considerando o envio de um e-mail, como a pratica mais comum neste tipo de verificações/análises, propomos a divisão constante na Tabela 7. Assumiremos também, que basta ocorrer uma consequência das listadas.

Consequências:

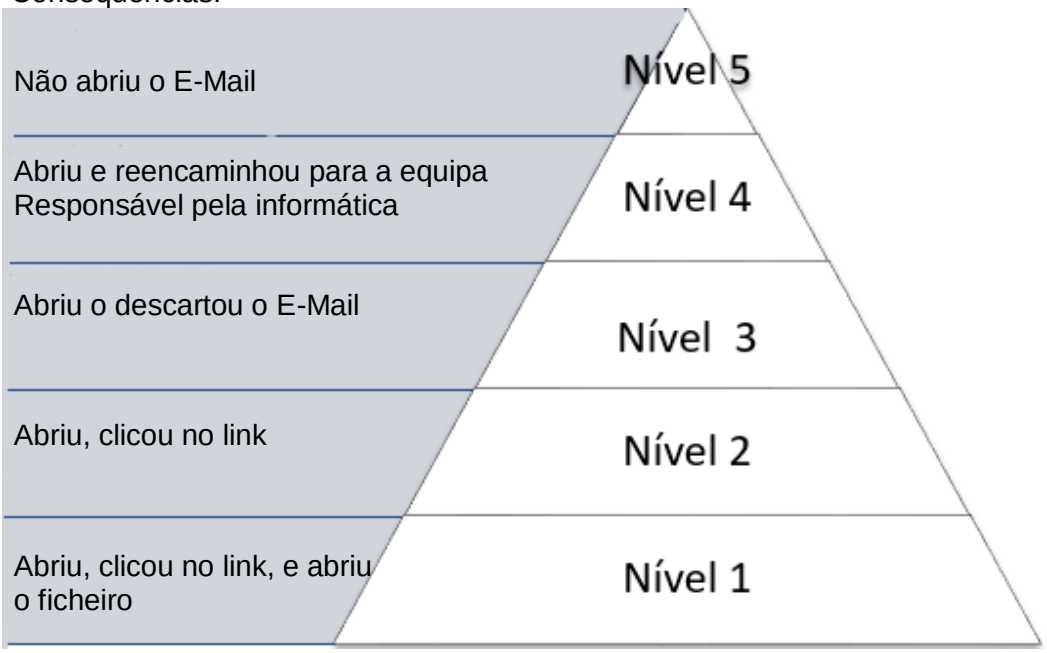


Tabela 7: Enquadramento de nível

De acordo com transcrito e o constante na tabela 7, para o exemplo, a organização fica posicionada no nível, analisado e partindo do mais baixo (1) para o mais alto (5), onde se observe um ou mais dos comportamentos definidos em cada nível, independentemente do número de alvos em análise.

3.5. Análise de Vulnerabilidades Tecnológicas

Atualmente as organizações dependem dos sistemas informáticos para o desenvolvimento da sua atividade, como tal, necessitam de uma infraestrutura tecnológica bem elaborada na produção e processamento de dados, divulgação e venda de serviços, entre outros. Neste sentido, um dos maiores desafios dos gestores é o facto de as organizações conviverem com vulnerabilidades e ameaças que elevam o risco da segurança de informação.

A vulnerabilidade consiste num indicador fundamental para a governação do risco, envolvendo os processos e impactos decorrentes de eventos de origem humana, tecnológica ou ambiental. No presente contexto, a relevância da análise da vulnerabilidade decorre da necessidade instrumental de fundamentar opções no âmbito da prevenção, redução ou mitigação do risco, assim como da necessidade de consolidar os indicadores de capacidade de suporte e de resiliência das organizações para a confidencialidade, disponibilidade e integridade da informação.

A análise de vulnerabilidade visa detetar falhas nos mais diversos componentes como seja: aplicações, *softwares*, equipamentos, sistemas operativos, comportamentos humanos, entre outros. Uma análise de vulnerabilidades deve identificar e eliminar sistematicamente vulnerabilidades encontradas.

A origem das vulnerabilidades é normalmente dividida em três grandes áreas:

- **Erros de programação** – Grande parte das vulnerabilidades surgem de erros de programação: tamanho do buffer, validação do input, má utilização de api´s e algoritmos.
- **Má configuração** – As aplicações de segurança, como a *firewall*, devem ser corretamente configuradas, ou podem ser brechas para ataques maliciosos.
- **Falha humana** – Execução de ficheiros maliciosos, engenharia social, erro, falta de conhecimento.

O objetivo da análise de vulnerabilidades é reduzir o risco em relação aos incidentes de segurança, quer seja a nível interno ou externo, pelo que é necessário detetar essas possíveis falhas e corrigi-las antecipadamente.

A análise das vulnerabilidades deve ser um processo contínuo de verificação e análise, para que a mesma fique sempre atualizada e livre de acessos não permitidos e indesejáveis.

É com este propósito que a metodologia agora apresentada não podia deixar de considerar a avaliação/auditoria da tecnologia em conjunto com a análise aos processos e pessoas. Os principais objetivos da análise de vulnerabilidades são:

- Identificar e tratar falhas de *software* que possam comprometer o seu desempenho, funcionalidade e segurança;
- Ajustar as configurações dos *softwares* com o propósito de os tornar mais eficientes e menos suscetíveis a ataques;
- Utilizar mecanismos para bloquear ataques automatizados (worms, bots, entre outros);

- Implementar a melhoria constante do controlo de segurança;
- Documentar os níveis de segurança atingidos para fins de auditoria e *compliance* com leis, regulamentações e políticas.

Para gerir o risco é preciso conhecer as vulnerabilidades. É neste contexto que consideramos a existência deste eixo como necessário e fundamental para, entre outros, avaliar e colmatar as fragilidades e vulnerabilidades provenientes dos resultados do eixo 1 e eixo 2.

Além da possibilidade da análise de vulnerabilidades poder ser direcionada e refinada com os resultados do eixo 1 e 2, não podemos deixar de focar os serviços com visibilidade do exterior (Web), que são um dos principais *focus* por parte dos atacantes.

As vendas de comércio eletrónico B2C no mercado europeu tem vindo a registar crescimentos na casa dos dois dígitos. Em 2014, os dados revelados pela Associação ECommerce Europe no novo European B2C E-commerce Report 2015, apontam para um volume de vendas no mercado europeu de 423,8 mil milhões de euros [50]. Considerando apenas os 28 países da União Europeia, verifica-se um crescimento similar, com um volume de negócios de 368,7 mil milhões de euros. O relatório, aponta ainda, que a quota do e-Commerce face ao PIB europeu continua a crescer e no final de 2014 situava-se nos 2,45%. Espera-se que essa participação cresça ainda mais nos próximos anos, atingindo cerca de 6% em 2020. Outro indicador da importância do comércio eletrónico na economia europeia é o número de *sites* B2C, que em 2014 se situava em 715 mil. O volume de empregos criados diretamente e indiretamente em redor do e-Commerce é calculado em perto de 2,5 milhões.

Face ao exposto, facilmente se compreende que atualmente existem um sem número de empresas cujo principal canal de negócio assenta na web.

Apesar deste desenvolvimento e da forte oportunidade e vantagens para as organizações no acesso ao mercado e divulgação dos serviços que estas oferecem, não raramente os sítios na web, essencialmente os de uso comercial e institucional, ainda apresentam vulnerabilidades. Uma boa parte das vulnerabilidades, deriva da forma exponencial do crescimento da rede, com o mercado/empresas a querem estar presentes, revelando para segundo lugar uma definição, planeamento estruturação dos seus sítios na rede. Assim, são priorizados os aspetos funcionais que atendem a área de negócios, enquanto os requisitos de segurança ficam em segundo plano. Tal situação, a par de uma parca assistência na monotorização e atualização das ferramentas, instigou a que um grande número de sítios na web apesentem vulnerabilidades que perante uma ameaça podem levar ao comprometimento dos sistemas/informação.

A par deste crescimento da rede, também os *hackers* foram evoluindo tanto em número como na sofisticação do tipo de ataques, pelo que será seguro afirmar que, atualmente, mesmo que se utilize todos os sistemas de segurança possíveis, é altamente provável que num determinado momento, com a evolução da Internet, haja pelo menos uma brecha que possa ser explorada num mundo onde as ameaças começam a ter uma perspetiva completamente nova.

Comumente vemos notícias de empresas/organizações com as suas bases de dados expostas, o que não raras vezes leva ao seu corrompimento com os consequentes efeitos e prejuízos que daí advêm. Além do prejuízo financeiro, existe um outro difícil de quantificar e que respeita à imagem e confiança das organizações. Dados de cartões de crédito, informações de clientes e de operações das empresas, roubos de identidades e outros dados sigilosos, informações sobre a infraestrutura de dados e vários outros podem ser usados para compor cenários de ataques com impacto para as organizações e pessoas.

Segundo o Instituto Gartner [51], mais de 75% dos problemas com segurança na Internet são devidos a falhas exploráveis a partir das aplicações web. No seu relatório "Cybersecurity at the Speed of Digital Business" prevê ainda, que em 2020, 60% das empresas digitais enfrentem grandes falhas de serviço devido à incapacidade das equipas de segurança das TI gerirem o risco digital.

Os ataques podem causar problemas com vários níveis de impacto, como por exemplo:

- Interrupção ou queda de desempenho do serviço;
- Acesso não autorizado a dados confidenciais e estratégicos;
- Roubo de informações e dados pessoais;
- Fraudes e modificação de dados no fluxo das operações;
- Perdas financeiras diretas e indiretas;
- Prejuízos à imagem da marca da empresa;
- Perda da lealdade dos Clientes;
- Gastos extraordinários com incidentes de segurança.

Assim, e de forma a obter uma imagem comum e transversal a toda a organização para o cálculo do Índice de maturidade das organizações, além da análise e mitigação das vulnerabilidades decorrentes dos eixos 1 e 2, uma das áreas que também deve ser avaliada e auditada, pela importância supra mencionada, são os serviços com visibilidade para o exterior.

Partindo do prossuposto, que os relatórios de análise de vulnerabilidades classificam as falhas encontradas em categorias como:, *Critical; high; Medium; Low: informational*

propomos que o IMSI deste eixo seja calculado em função dos resultados obtidos. O cálculo da percentagem para enquadramento na curva de nível resulta dos pré-requisitos (número de ocorrências permitidas em cada categoria) definidos nas reuniões prévias entre o auditor e as equipas de gestão/organização.

3.5.1. Algoritmo de cálculo do IMSI

Seguidamente apresenta-se um algoritmo com o resumo dos cálculos do IMSI da análise de vulnerabilidades (Eixo 3)

Algoritmo de Cálculo do IMSI do Eixo 3

1. Determinar as áreas a auditar
   - 1.1. Reunião com estruturas para definição das áreas: Redes, Sistemas, Aplicações
   - 1.2. Determinar os pré-requisitos
   - 1.3. Obtenção de autorizações
2. Execução da análise
   - 2.1. Lançamento da ação
   - 2.2. Recolha de resultados
     - 2.2.1. Obter nº de ocorrências por categorias – RC
     - 2.2.2. Obter o número total de ocorrências - RO
   - 2.3. Obter o valor do IMSI
     - 2.3.1. Cálculo do IMSI resulta do nº de ocorrências definidas em 1.2
     - 2.3.2. Posicionar o valor RF na curva de nível

Figura 12: Algoritmo de cálculo do IMSI do eixo 3

Os resultados obtidos neste eixo tem validade por si só, devendo no entanto, em função do estabelecido e acordado com a gestão da empresa, concorrer para o score e ponderação final.

3.5.2. Fases a executar – Metodologia IMSI

A figura 13 ilustra de forma consolidada as etapas de cada um dos eixos propostas na presente metodologia. A definição de tal estrutura permitiu-nos traçar um plano exequível, na planificação das atividades com vista a alcançar os objetivos desejados, para além de permitir uma visão gráfica do trabalho a seguir para a aplicação da mesma.

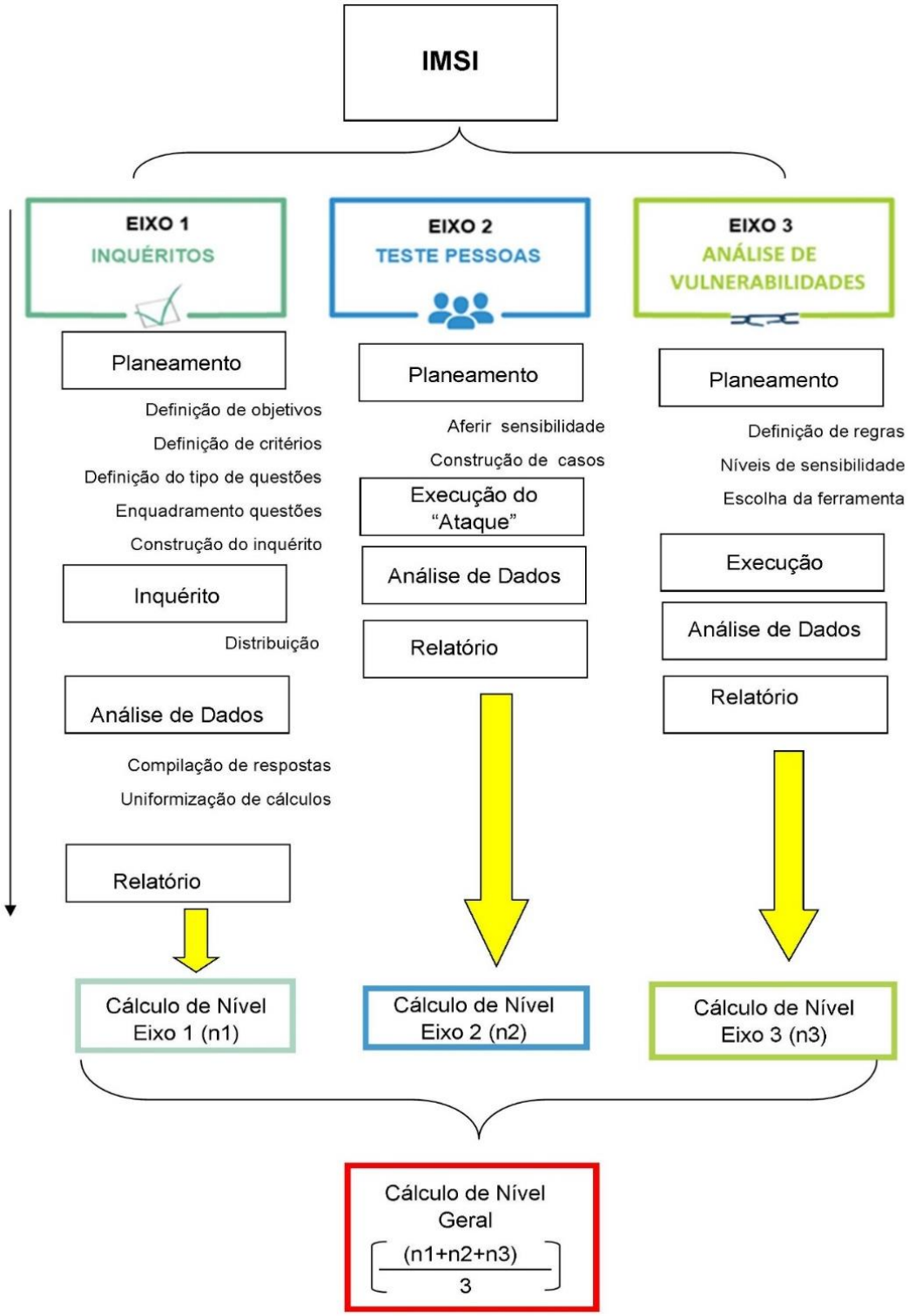


Figura 13: Fluxograma de etapas a executar nos três eixos de análise

Como referido ao longo do documento, a metodologia proposta tem como objetivo ser uma metodologia de "*entry level*", de fácil aplicação, sem necessidade de grandes recursos técnicos e financeiros e capaz de apresentar, no mapeamento das ameaças e gestão do risco, resultados fidedignos e de fácil interpretação pelas organizações. Tais características contrastam com a análise de risco "clássica", que como tivemos oportunidade

de explorar no estado da arte, são de difícil aplicação, requerem recursos técnicos especializados, muitas vezes com custos elevados e com resultados de difícil interpretação por algumas estruturas, nomeadamente pela camada de gestão. De referir que a camada de gestão assume um papel fundamental em toda esta temática, onde não raras vezes, fruto do desconhecimento e da inexistência de avaliações, relativizam esta componente nas várias tomadas de decisão.

No próximo capítulo é apresentado a experimentação da metodologia no terreno.

Capitulo 4

Experimentação da metodologia

Este capítulo comporta a experimentação da metodologia no terreno. Inicialmente, entramos em contacto com as entidades alvo e abordamos a aplicação da metodologia para cada um dos eixos. Em resultado foi acordado uma ordem de execução: eixo 1, eixo 2 e eixo 3. À data de fecho deste relatório só foi possível avançar com o eixo 1 e eixo 2.

Tratando-se de uma metodologia *standard* e transversal a qualquer setor de atividade, começamos por definir os objetivos para cada um dos eixos. Os objetivos deram corpo ao planeamento e consequente execução dos testes. Os resultados obtidos foram analisados e são discutidos também neste capítulo.

4.1 Ações e planeamento do eixo 1

No eixo 1, inquéritos, começamos por efetuar aquilo que poderá ser designado de preparação dos dados. O objetivo desta etapa (preparação de dados) é garantir que as questões colocadas sejam suficientemente amplas e esclarecedoras para uma análise global da organização, na temática da segurança de informação. Para isto será necessário identificar, agrupar e até mesmo corrigir erros.

Ao se começar a usar um conjunto de dados, não raras vezes, encontra-se problemas. Segundo DAVIDSON [52], estima-se que 80% do tempo associado ao processo de prospeção e descoberta de informação será gasto a lidar com esses problemas.

De forma a evitar tais erros e validar a clareza e eficácia do inquérito deverá, sempre que possível, ser efetuada uma prova de conceito para validação do inquérito e respetivos ajustes. Para o efeito e em conjunto com o docente da unidade curricular de Segurança Informática da licenciatura em Sistemas de Informação da ESTGF/IPP (ano 2015/2016), e no âmbito dos objetivos daquela unidade curricular, foi feita uma prova de conceito do mesmo, através da disponibilização dos temas base aos estudantes, no sentido de criarem um formulário de suporte aos inquéritos para os seus trabalhos e desta forma avaliar e/ou sugerir alterações ou inclusões das áreas apresentadas. De salientar que os estudantes tinham como objetivo inquerir um conjunto de empresas, à escolha, sobre os procedimentos relacionados com a segurança de informação.

Esta prova de conceito foi uma mais-valia, na medida em que permitiu efetuar uma avaliação ao fundamento e áreas do inquérito, nomeadamente na correção de alguns erros relacionados com a clareza, tipo, colocação e cruzamento de informação das

questões. Esta validação foi extremamente útil para melhorar o inquérito base constante no Anexo 1. Partindo do inquérito base, foi identificado um sector de atividade para aplicação do mesmo. Para a escolha do sector de atividade considerou-se:

- Organizações que albergassem um número suficiente de colaboradores onde fosse possível experimentar a metodologia nos diversos públicos-alvo;
- Que exercessem atividades similares para comparação entre pares;
- Tivessem uma forte componente tecnológica/informática:
- Fosse possível empregar todos os métodos de análise (pessoas, processos e tecnologias) para determinação do Índice de Maturidade de Segurança Informática.

Face ao planeamento, objetivos definidos e facilidade de contacto a nossa escolha recaiu sobre as autarquias locais. Neste caso, e de forma a termos uma amostra representativa, elegemos quatro autarquias da região.

Após a escolha, seguiu-se o agendamento de reuniões com os responsáveis pelas organizações (presidentes de câmara e/ ou vereadores responsáveis pelo pelouro da sociedade de informação), com o intuito de apresentar o trabalho e os objetivos subjacentes ao mesmo. A avaliação dos aspetos relacionados com a segurança de informação, tendo por base uma metodologia que não é intrusiva na atividade das organizações e é de fácil compreensão foi elogiada e deu frutos. Assim e no final das várias reuniões, com a concordância dos mesmos, foi solicitada uma declaração de autorização para a realização das ações, a qual se dá integralmente reproduzida no Anexo 2 desta dissertação.

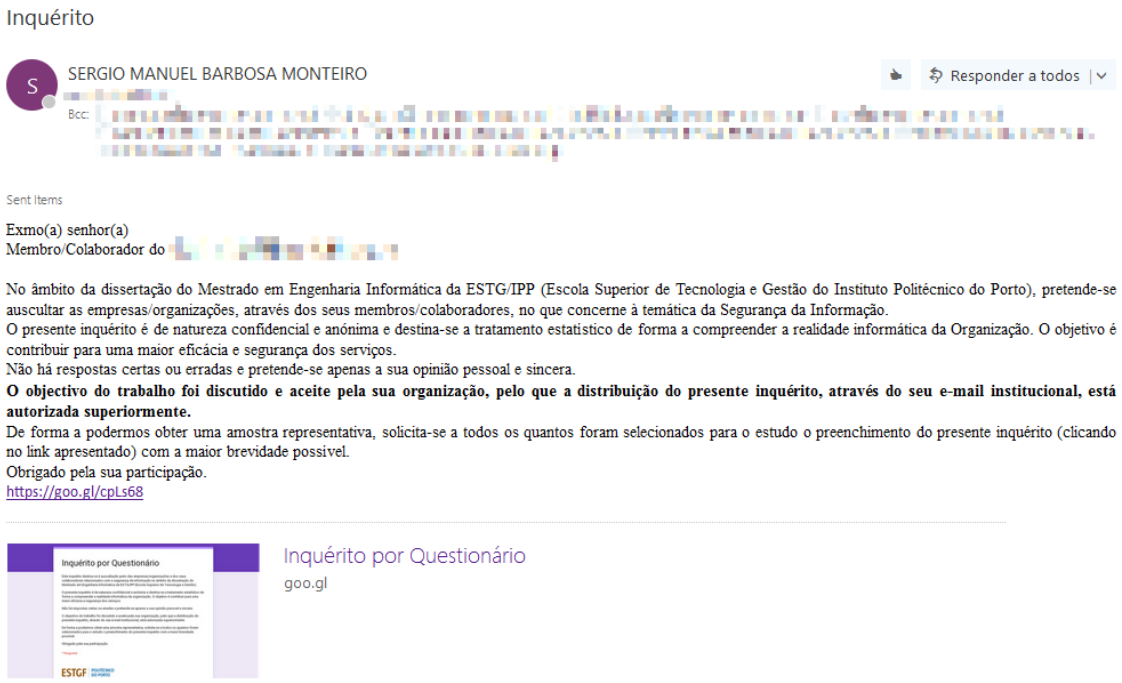
Estas reuniões permitiram ainda recolher informações relativas à atividade das organizações no que se refere à utilização da tecnologia e do relacionamento das mesmas. Esta perceção da realidade foi fundamental, tendo por base as áreas definidas nesta metodologia para enquadramento de nível, para a conceção das questões do inquérito, assim como para aferir as áreas que consideram mais sensíveis/relevantes no contexto do trabalho de forma a classificarmos as questões como do tipo 1 ou 2, isto é, com maior ou menor relevância para a Segurança de Informação. De referir que o âmbito e o tipo das questões, em função do apreendido e acordado nas reuniões iniciais, foi sugerido por nós e aceites por todas as instituições. De acordo com o definido na metodologia, a ponderação/divisão das questões quanto ao grau de importância (tipo 1 ou 2) e atribuição de pesos (proporcionalidade inversa), também foi aceite por todas as partes.

As instituições em que trabalham os inquiridos são autarquias locais da mesma região (Tâmega e Sousa). Por isso, têm atividades e públicos-alvo similares. Em todas existem pessoas com *know-how* mais tecnológico, como é o caso das equipas de

informática. Com Know-how de gestão, como é o caso do executivo e responsáveis de serviços. Existem também os trabalhadores de diferentes serviços. Tal situação proporciona a experimentação da metodologia em pleno, conforme definição dos público-alvo descritos no capítulo 3.

Uma vez percecionada a realidade e o âmbito de distribuição/análise passamos à fase de definição do inquérito a usar. Nesta fase e como referido anteriormente, tivemos em consideração a realidade das organizações, as recomendações para a criação de um inquérito eficaz e o constante na Tabela 3 do presente trabalho.

Após a criação do inquérito, passamos à fase de distribuição. A distribuição foi feita por e-mail para as listas de endereços fornecidas pelas organizações. Para o efeito, foi usado o e-mail da ESTG/IPP com um texto informativo e o link para preenchimento. Para uma maior proteção dos dados da instituição, os endereços de E-mail do destino foram sempre colocados em BCC, conforme evidencia a Figura 14.


Inquérito

SERGIO MANUEL BARBOSA MONTEIRO

Responder a todos

Bcc:

Sent Items

Exmo(a) senhor(a)
Membro/Colaborador do

No âmbito da dissertação do Mestrado em Engenharia Informática da ESTG/IPP (Escola Superior de Tecnologia e Gestão do Instituto Politécnico do Porto), pretende-se auscultar as empresas/organizações, através dos seus membros/colaboradores, no que concerne à temática da Segurança da Informação.
O presente inquérito é de natureza confidencial e anónima e destina-se a tratamento estatistico de forma a compreender a realidade informática da Organização. O objetivo é contribuir para uma maior eficácia e segurança dos serviços.
Não há respostas certas ou erradas e pretende-se apenas a sua opinião pessoal e sincera.
O objectivo do trabalho foi discutido e aceite pela sua organização, pelo que a distribuição do presente inquérito, através do seu e-mail institucional, está autorizada superiormente.
De forma a podermos obter uma amostra representativa, solicita-se a todos os quantos foram selecionados para o estudo o preenchimento do presente inquérito (clicando no link apresentado) com a maior brevidade possível.
Obrigado pela sua participação.
https://goo.gl/cpLs68

Inquérito por Questionário
goo.gl

Figura 14: E-mail para preenchimento de inquérito

A Tabela 9 ilustra, por instituição, o número de inquéritos enviados e quantidade de respostas obtidas. A distribuição foi efetuada em períodos temporais diferentes, por via da disponibilidade da informação, nomeadamente das autorizações e obtenção da lista de E-mails por parte das entidades envolvidas.

Instituição	Nº e-mails fornecidos e enviados	Número de respostas recebidas	%	Período campanha	
				Início	Fim
Município A	144	37	26	17-10-2016	04-11-2016
Município B	213	30	14	10-10-2016	04-11-2016
Município C	224	24	11	03-11-2016	16-11-2016
Município D	114	24	21	10-10-2016	04-11-2016
TOTAIS	**695**	**115**	**16,54**		

Tabela 8: Ações efetuadas e respostas obtidas (Eixo 1)

A análise de resultados será apresentada mais à frente neste capítulo.

4.2 Ações e planeamento do eixo 2

Para a experimentação da metodologia do eixo 2, depois de analisados alguns dos comportamentos/práticas provenientes do eixo 1 (inquéritos), foi selecionada uma campanha por via de phishing simulando um e-mail externo.

A criação deste tipo de cenários, dependente da identidade assumida tem como abrangência e finalidade na metodologia apresentada:

- Envio de e-mail com um link/anexo para um ficheiro;
- Envio de e-mail a perfis selecionados da empresa (e pela mesma) com e-mails vindo de origens aparentemente válidas e que solicitem ações que violem políticas de segurança;
- E-mail de superior hierárquico a pedir para fazer algo (uma transferência bancária por exemplo ou envio de um relatório com informação de clientes). Caracter urgente;
- E-mail interno a divulgar uma parceria com uma terceira entidade, a solicitar dados do colaborador, nomeadamente o preenchimento de uma ficha. Caracter oportunidade a não perder;
- E-mail de um colaborador a pedir ao outro para lhe fazer algo no computador porque foi ao médico e vai chegar mais tarde. Deixou o utilizador e a *password* para que o colaborador o possa ajudar. Caracter de entreajuda.

Este tipo de e-mails é frequentemente utilizado pelos *hackers* no âmbito das suas ações que visa entre vários:

- A obtenção de dados pessoais dos colaboradores para uso posterior;
- A obtenção de dados sobre o negócio, nomeadamente através do preenchimento de formulários on-line;
- O roubo de credenciais de acesso, pelo simples encaminhamento do utilizador para um *site* fraudulento que lhe pede credenciais comuns;
- Perturbar o normal funcionamento da empresa, enviando informação aparentemente válida, mas que na prática vai levar os colaboradores/operação a ineficiências;
- A instalação de *software* malicioso capaz de, entre vários: cifrar os dados da empresa e pedir regastes monetários em troca da decifra; roubar credenciais de acesso; usar os sistemas informáticos da empresa como meio para atacar terceiros colocando em causa a reputação da própria empresa e eventuais consequências legais por danos causados a terceiros; permitir o acesso remoto aos sistemas da empresa.

Considerando o definido na Tabela 6 do capítulo 3 para a estruturação e planeamento dos cenários, considerámos as entidades envolvidas e sugerimos uma campanha de *phishing* que avaliasse o comportamento dos utilizadores a vários níveis. A campanha apresentada e aceite por todos tinha como base os seguintes prossupostos:

- Envio de um e-mail a 50 colaboradores escolhidos de forma aleatória entre os e-mails fornecidos pelas instituições;
- Assumisse uma identidade externa e desconhecida, isto é, sem semelhança a nenhuma entidade/organização conhecida pelo setor;
- Contivesse links no corpo do e-mail e fosse possível quantificar os cliques;
- Remetesse para uma página com *links* a apontar para um ficheiro (2 º nível)
- Ficheiro em Excel com uma macro que quando aberta executasse uma ação (3 º nível).

Em fase de preparação da ação e de acordo com as etapas da metodologia a campanha resume-se ao constante na Tabela 10.

Complexidade	Média	Tipo Ação	Phishing	Template	Simples
Objectivo	Avaliar se o colaborador é vulnerável ao *download* de ficheiros potencialmente maliciosos.				
Alvo	50 Colaboradores (aleatórios) de cada instituição				

Descrição	Este exercício utiliza um ambiente de contexto para convencer um colaborador a clicar num *link* para aceder a uma página e a partir dai, abrir um documento potencialmente malicioso.
Pré-Requisitos	Base de dados dos colaboradores
Meios de Comunicação	E-mail
Contexto	Revisão de Carreiras Descongelamento de Carreiras Contagem de tempo de serviço para progressão na carreira Simulação de rendimento/salários
Output	O relatório de ação contém a taxa de cliques relativamente ao número total de colaboradores que abriram o e-mail, clicaram no *link* e abriram o ficheiro anexo, e ações recomendadas.

Tabela 9: Campanha de Phishing

Com esta ação, pretendemos avaliar se os colaboradores abrem e-mails de desconhecidos, clicam em *links* desconhecidos e procedem à abertura/download de ficheiros, potencialmente maliciosos.

Para dar corpo à campanha, utilizamos a ferramenta "Gophish", disponível em https://get**gophish**.com/ que após configuração de todos os parâmetros, permite-nos operacionalizar a campanha e obter relatórios quanto ao número de e-mails enviados, e-mails abertos e links clicados. O número de ficheiros abertos, é obtido através da própria macro, que procede ao envio de um e-mail sempre que é ativada.

No Gophish, foi necessário proceder às seguintes configurações:

- "Sending Profile" – Configuração do e-mail que assume o envio da campanha.
- "Landing Pages" – Configuração de uma página clone, que alberga os *links* e ficheiros maliciosos (Controlada pela origem/ *hackers)*
- *"E-mail Tempaltes" – Criação do e-mail, com definição de links e estrutura a enviar*
- *"Users & Groups" – Criação dos grupos de utilizador a ser alvo do ataque*

Para aplicação do caso em estudo, foi necessário, entre outros: proceder ao registo de um domínio www.dlap-tamegasousa.pt, com o propósito de assumir a identidade de "Direção local da Administração Pública do Tâmega e Sousa"; alugar um servidor (Amazon AWS) e proceder às respetivas configurações. Foi também necessário proceder à criação de um ficheiro em excel, com macros autoexecutaveis, que apesar de neste caso não acarretarem qualquer tipo de risco para a instituição, poderia conter código malicioso e colocar a organização em perigo.

Tal como dito acima, a macro criada e que se dá como reproduzida no anexo 3, faz com que à abertura do ficheiro e activação da macro, seja enviado um e-mail com um texto pré-definido.

4.3 Análise de resultados

Eixo 1

Tendo em consideração o acordado com as entidades e a metodologia apresentada, procedemos à fase de análise de resultados do eixo 1. A Figura 15 ilustra a relação entre as questões instanciadas a partir do inquérito (Anexo 1) e a divisão e enquadramento das questões nos dois tipos, determinados em fase prévia, de acordo com a metodologia. No que se refere à relação das questões, referidas no capitulo 3, pontos 3.1.3 e 3.1.4, cuja cotação e ponderação final advém do cruzamento de dados com mais questões, salientamos que para o rigor do cálculo contabilizamos esse grupo/conjunto de questões como sendo apenas uma questão, conforme ilustra a mesma figura. Assim e para cada conjunto de questões/grupo-alvo temos as questões iniciais e o respetivo agrupamento/análise.

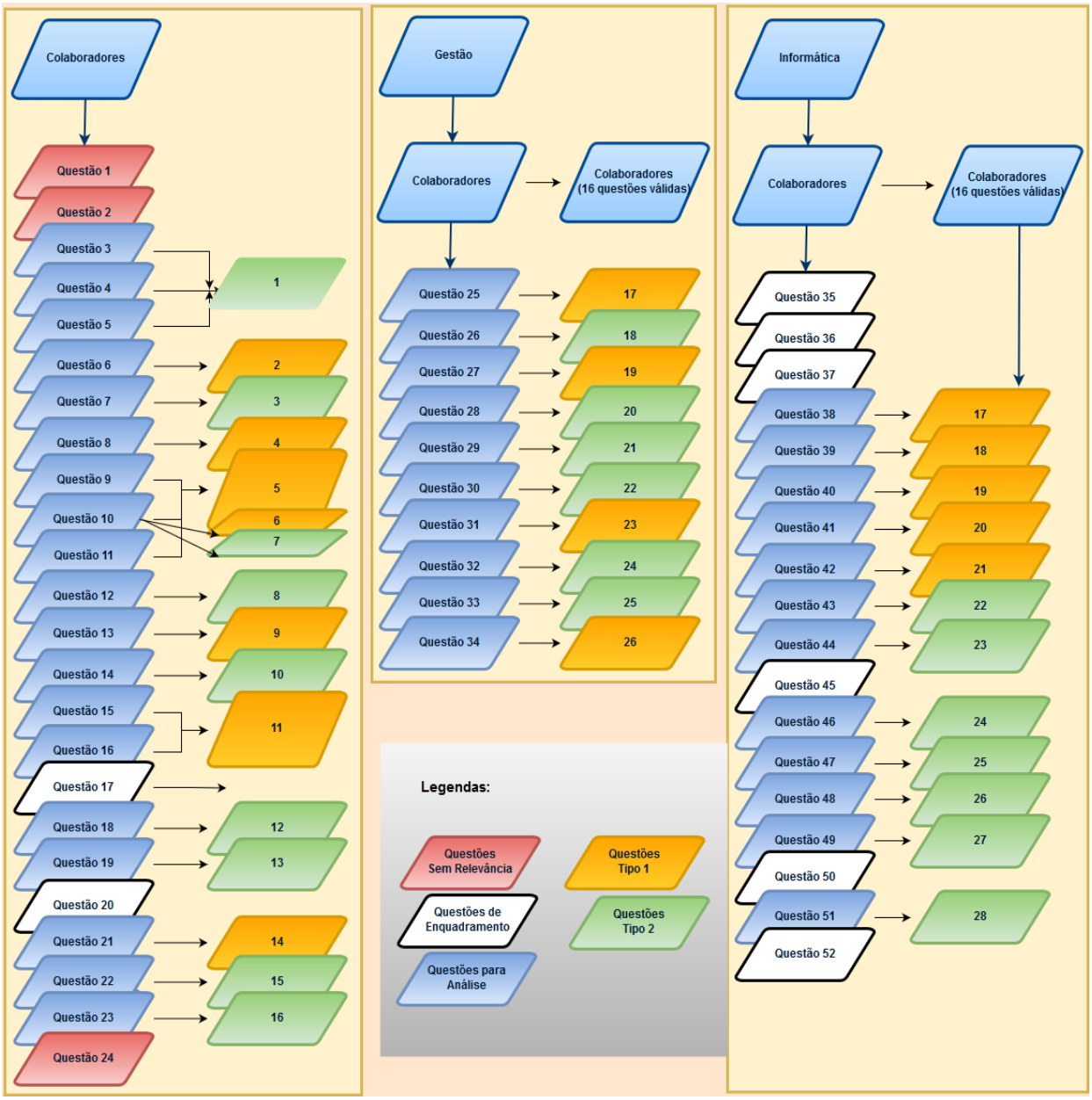


Figura 15: Questões – Relação e Tipo

Face ao disposto na metodologia e descrito no capítulo 3, a Figura 16 ilustra o número e percentagem de questões por tipo, a atribuição de cotações (pesos) baseada na regra da proporcionalidade inversa.

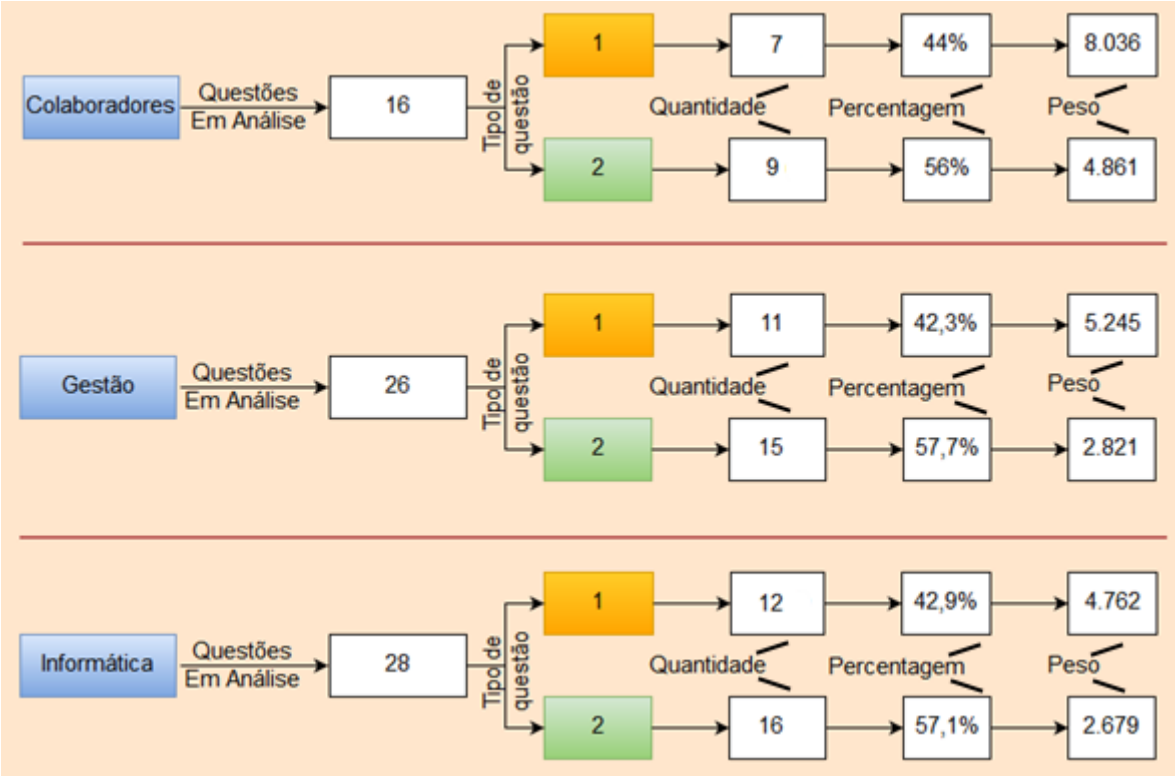


Figura 16: Número e Percentagem de Questões por tipo e atribuição de pesos

Os valores apresentados na Figura 15 são uniformes a todas as organizações em teste. O número de questões resultou das reuniões prévias. A classificação do tipo foi feita por nós a pedido das organizações e discutida antes de ser feita a análise dos inquéritos.

De seguida são apresentados os resultados por instituição. Para a análise e cálculo das questões foram empregues os métodos constantes no Capítulo 3. Na descrição dos resultados obtidos as questões mencionadas aludem ao resultante do tratamento efetuado na Figura 15 e não ao número da questão do inquérito.

Instituição A

<u>Grupo Alvo: Colaboradores</u>

Ao nível dos colaboradores, nomeadamente naquilo que são as práticas do dia-a-dia, dos conhecimentos e preocupações com a segurança de informação, a pontuação obtida (55,16%), de acordo com a curva de nível adotada e apresentada na Figura 5 do capítulo 3 coloca a organização no nível 2 (dois), conforme ilustra a Figura 17.

Colaboradores Instituição A

Questões	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Resultados (%)	0,884	0,839	0,968	0,135	0,337	0,387	0,452	0,258	0,756	0,387	0,290	0,872	0,903	0,802	0,757	0,194
Peso	4,861	8,036	4,861	8,036	8,036	8,036	4,861	4,861	8,036	4,861	8,036	4,861	4,861	8,036	4,861	4,861
Final	3,324	6,740	4,704	1,084	2,705	3,111	2,195	1,254	6,073	1,882	2,333	4,239	4,391	6,447	3,731	0,941

Resultado: 55,16 % Nível 2

Figura 17: Análise Inquéritos da Instituição A – Colaboradores

A Figura 17 resulta da aplicação da metodologia descrita no capítulo 3. Pela análise, pode-se observar que a maioria dos inqueridos utiliza *passwords* de acesso ao computador, questão 2 da figura. Apesar deste ser um requisito fundamental no âmbito da segurança de informação, verifica-se a inexistência de uma politica relacionada com as mesmas, pois como podemos constatar, a maioria dos inqueridos afirma não alterar as passwords, questão 4, para além de usarem expressões e/ou datas com sentido semântico e normalmente inferior a 8 caracteres, questão 5, o que torna as passwords de "força fraca".

Em média, apenas 25,8% dos inquiridos (questão 8) afirma não usar dispositivos de armazenamento USB e só 75,6% (questão 9) bloqueia a sessão de trabalho nas ausências do posto de trabalho.

Outro fator que merece destaque nesta análise, é o facto de a grande maioria dos inqueridos não ter conhecimento da existência de um plano de boas práticas e normas de segurança (questão 11) não havendo por isso uma definição clara da política de segurança da organização nem uma definição das responsabilidades dos colaboradores.

Apesar da maioria dos inqueridos classificar a sua apetência para o uso das tecnologias elevado (questão 12), e de considerarem as tecnologias de informação, nomeadamente o uso da Internet como fundamental para o rendimento e qualidade do trabalho (questão 15) denota-se a inexistência de um programa de formação (formação, avaliação de conhecimentos, entre outros) no que respeita à segurança de informação (questão 16).

Grupo Alvo: Gestão

Ao nível da gestão, de acordo com a curva de nível adotada e apresentada na Figura 5 do capítulo 3, o enquadramento de nível mantem-se no segundo nível, pese embora a percentagem suba ligeiramente (61,91%).

Gestão Instituição A

Questões	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Resultados (%)	0,70	1	1	0,095	0,933	0,50	0,250	0,000	0,930	0,250	0,500	0,775	0,500	0,930	0,750	0,000
Peso	2,821	5,245	2,821	5,245	5,245	5,245	2,821	2,821	5,245	2,821	5,245	2,821	2,821	5,245	2,821	2,821
Final	1,974	5,245	2,821	0,498	4,891	2,622	0,705	0,00	4,878	0,705	2,622	2,186	1,410	4,878	2,115	0,000

Questões	17	18	19	20	21	22	23	24	25	26
Resultados (%)	1	0,950	0,968	0,750	0,000	0,250	0,840	1	0,000	0,250
Peso	5,245	2,821	5,245	2,821	2,821	2,821	5,245	2,821	2,821	5,245
Final	5,245	2,679	5,074	2,115	0,000	0,705	4,406	2,821	0,000	1,311

Resultado: 61,91 % Nível 2

Figura 18:Análise de Inquéritos Instituição A – Gestão

Pela análise da Figura 18, pode-se observar que as questões da segurança de informação ainda assumem um papel secundário, apesar de afirmarem que as novas tecnologias suportarem uma grande parte das decisões, questão 18.

Quando questionados se “são realizadas auditorias de segurança de informação na instituição” (questão 25) 50% dos inqueridos afirma que não e os restantes 50% dizem que não sabem ou não querem responder. Importa ainda evidenciar:

- Que a política de segurança de informação não é partilhada fora da instituição, nomeadamente com parceiros/fornecedores (questão 26);
- Não existe um custo atribuído a cada ativo crítico ou função (questão 21);
- 75% afirma não conhecer ou não existir um plano para a continuidade do negócio em caso de desastre (questão 22).

Ao nível das questões comuns, não se verificam grandes alterações entre este grupo e os colaboradores, excetuando a temática das *passwords* (questão 5) onde é visível um aumento significativo de preocupação e importância no uso das mesmas. Apesar desta preocupação, 75% afirma não ter por habito alterar as *passwords* e 25% refere que altera um vez por ano (questão 4). Todos os inqueridos afirmam ainda, que costumam usar

dispositivos de armazenamento USB no computador (questão 8). Outro aspeto a realçar é que 50% dos inqueridos neste grupo, já foi alvo de ataque informático (questão 13).

Apesar do grupo em análise ter poder de decisão, todos os inqueridos responderam não saber (25%) ou não existir (75%) um programa de formação em segurança de informação na instituição, questão 16.

Grupo Alvo: Informática

Ao nível do departamento informático, foram rececionadas 2 respostas e conforme ilustra a Figura 19 não existe alteração de nível (60,520%).

Informática
Instituição A

Questões	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Resultados (%)	0,750	1	1	0,750	1	0,500	0,500	1	0,840	1	0,600	1	1	0,840	0,223	0,500
Peso	2,679	4,762	2,679	4,762	4,762	4,762	2,679	2,679	4,762	2,679	4,762	2,679	2,679	4,762	2,679	2,679
Final	1,974	5,245	2,821	0,498	4,891	2,622	0,705	0,00	4,878	0,705	2,622	2,186	1,410	4,878	2,115	0,000

Questões	17	18	19	20	21	22	23	24	25	26	27	28
Resultados (%)	0,500	0,000	0,000	0,750	0,500	0,000	1	0,000	0,000	0,000	0,750	0,930
Peso	4,762	4,762	4,762	4,762	4,762	2,679	2,679	2,679	2,679	2,679	2,679	2,679
Final	1,974	5,245	2,821	0,498	4,891	2,622	0,705	0,00	4,878	0,705	2,622	2,186

Resultado:
60,52 %
Nível 2

Figura 19: Análise de Inquéritos Instituição A - Informática

Na análise deste departamento, as questões relacionadas com a possibilidade de instalação de *software* e utilização de dispositivos de armazenamento USB foram cotadas de forma diferente dos restantes grupos (valorizou-se a possibilidade de instalação/uso como de nível 5, isto é, cotação máxima), em virtude do definido em sede de reunião prévia face ao conteúdo funcional exercida por este grupo.

No que concerne às questões comuns a todos os grupos, além de uma maior preocupação e melhores resultados no que concerne ao uso e politica de *passwords* e conhecimentos e praticas com o uso das tecnologias (questão 5) a maior diferença, e que contrasta com os restantes grupos, é a totalidade dos inqueridos afirmar ter conhecimento da existência de um plano de boas práticas e normas de segurança informática da organização, apesar de atribuírem uma cotação média no que respeita à sua acessibilidade, disponibilidade, atualização e compreensão de responsabilidades atribuídas em caso de negligência por parte dos utilizadores (questão 11).

Apesar de existir uma preocupação ao nível da tecnologia, nas questões direcionadas a este grupo é ainda possível extrair que:

- Não é comum usar cláusulas de salvaguarda das políticas de segurança nos contratos que dispõem com terceiros (questão 18);
- Não sabem ou não respondem se a estratégia de Segurança de Informação escrita incluem planos que visam reduzir os riscos a um nível aceitável, com interrupções mínimas para operações (questão 22);
- Não sabem ou não respondem se são realizadas auditorias de segurança de informação na instituição (questão 24);
- Não sabem ou não respondem se existem algum procedimento em vigor na instituição para atuação em caso de ataque (questão 26);
- Não sabem ou não respondem se a instituição foi alvo de algum tipo de ataque.

Para além destas, e face a contrariedade e/ou falta de conhecimento de alguns elementos nas restantes respostas às questões deste grupo, denota-se a ausência de uma eventual politica daquilo que são as normas e/ou cultura da organização, no âmbito da segurança de informação, para este setor em especifico.

Se considerarmos uma análise conjunta de todos os grupos, podemos verificar a existência de algumas dificuldades/*deficit* e ausência de planos e regras ao nível da segurança de informação, o que justifica o enquadramento de todos os grupos em análise no nível 2, conforme ilustra a Figura 20.

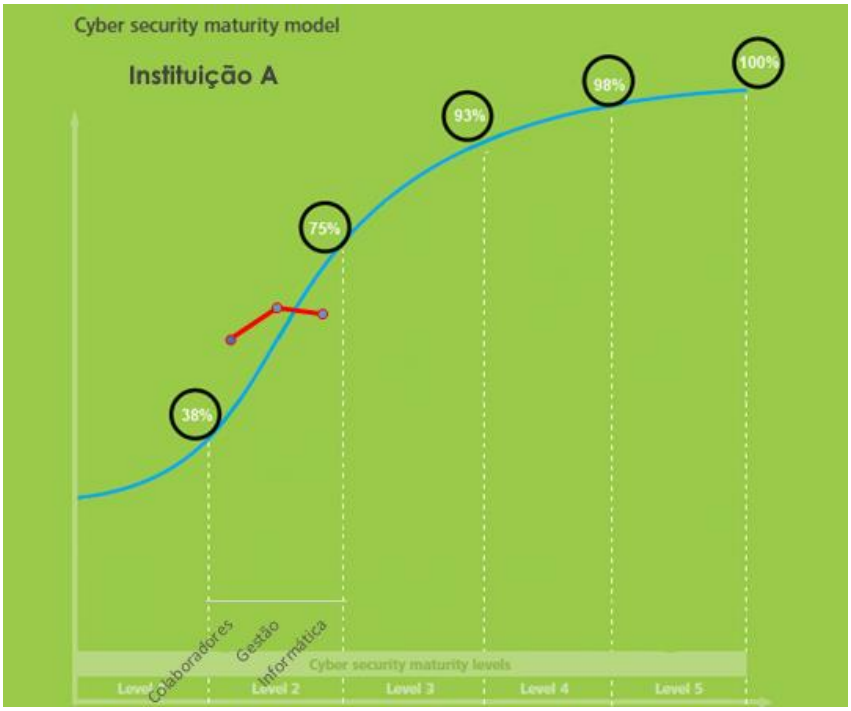


Figura 20: Enquadramento de Nível da Instituição A (inquéritos)

Instituição B

Grupo Alvo: Colaboradores

À semelhança da anterior e tendo por base a metodologia e a curva de nível adotada e apresentada na Figura 5 do capítulo 3 a pontuação obtida na instituição B, no que respeita à análise das práticas do dia-a-dia, dos conhecimentos e preocupações com a segurança de informação por parte dos colaboradores, coloca a organização no nível 2 (59,68%), conforme ilustra a figura 21 e 22.

Colaboradores Instituição B

Questões	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Resultados (%)	0,547	1	0,867	0,272	0,898	0,267	0,467	0,400	0,780	0,700	0,333	0,876	0,867	0,846	0,087	0,200
Peso	4,861	8,036	4,861	8,036	8,036	8,036	4,861	4,861	8,036	4,861	8,036	4,861	4,861	8,036	4,861	4,861
Final	2,657	8,036	4,213	2,188	7,212	2,143	2,269	1,944	6,268	3,403	2,679	4,258	4,213	6,798	0,425	0,972

Resultado: 59,68 % Nível 2

Figura 21: Análise de Inquéritos Instituição B – Colaboradores

De salientar, que nesta instituição não houve lugar a respostas por parte da gestão e do departamento informático, pelo que será impossível fazer deduções e comparação, com as demais instituições envolvidas, sobre estes dois grupos.

Pela análise do inquérito e como justificação de enquadramento de nível, denota-se alguma falta de clareza e/ou politicas no que respeita à segurança de informação. Quando questionados sobre a existência de alguma pessoa ligada às tecnologias de informação, uma parte substancial dos inqueridos não reconhece e/ou não sabe da sua existência e as que responderam afirmativamente, não são unanimes quanto ao número de pessoas afetas ao departamento, questão 1.

Pela questão 6 verifica-se que 73,30% diz que cederia a sua *password* de acesso a um colega e na questão 7, 53,30% afirma ter conhecimento dessa prática.

O desconhecimento (66,7%) da existência de um plano de boas práticas e normas de segurança informática na organização (questão 11) é outro aspeto merecedor de realce nesta análise e que remete para uma definição pouco clara da política de segurança da organização e da definição das responsabilidades dos colaboradores.

Como ponto positivo, salienta-se o cuidado existente com a possibilidade de instalação de *softwares* e com o uso das *passwords*, onde 100% dos inqueridos (questão 2) afirma usar passwords de acesso. Apesar da maioria dos inqueridos afirmar que as altera semestralmente ou trimestralmente, ainda há uma larga maioria (questão 4) que afirma não ter por hábito proceder à sua alteração. A força das *passwords* (questão 5) é outro aspeto a realçar, pois pela análise é possível observar que 83,4% são inferiores a 8 caracteres, 76,70 % não usa símbolos na sua composição e 33,3% inclui informação pessoal, o que fragiliza a sua eficácia/proteção.

Apesar da maioria dos inqueridos classificar a sua apetência para o uso das tecnologias elevado (questão 12) e de considerarem as tecnologias de informação, nomeadamente o uso da Internet, como fundamental para o rendimento e qualidade do trabalho, denota-se a inexistência (questão 16) de um programa de formação (formação, avaliação de conhecimentos, entre outros) no que respeita à segurança de informação

Face aos resultados obtidos e à curva de nível adotada, este grupo de utilizadores posiciona-se no nível 2, conforme ilustra a Figura 22.

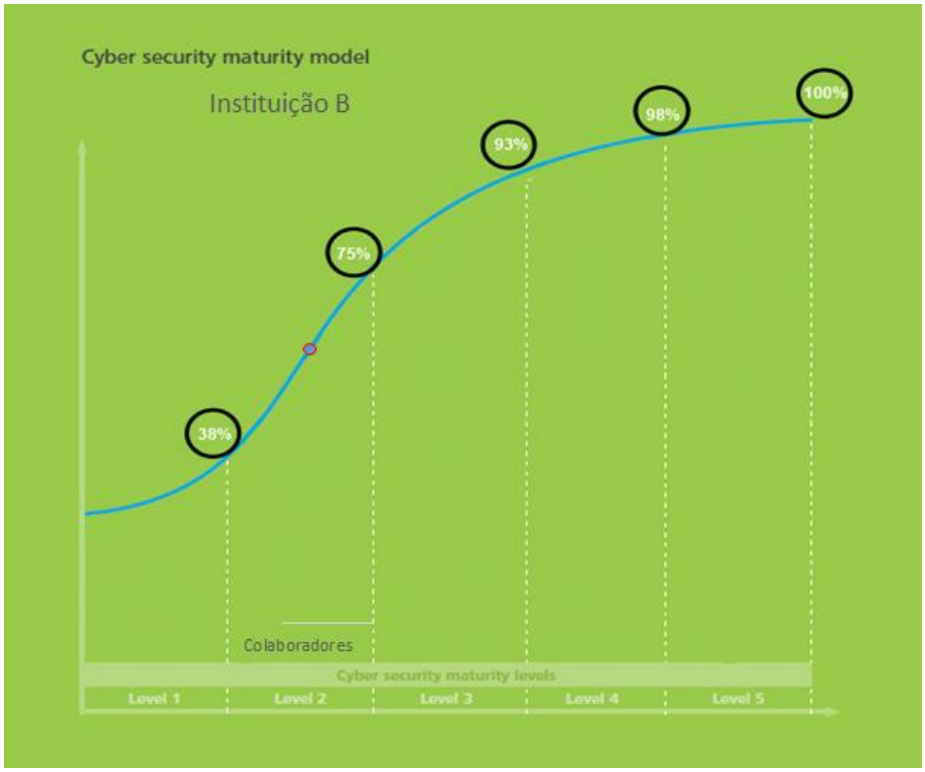


Figura 22: Enquadramento de nível Instituição B (Inquéritos)

Instituição C

Grupo Alvo: Colaboradores

Pela análise dos inquéritos, verificou-se que ao nível dos colaboradores, nomeadamente naquilo que são as práticas do dia-a-dia, dos conhecimentos e preocupações com a segurança de informação, a pontuação obtida (42,46%) coloca a organização no mesmo nível das anteriores, conforme ilustra a Figura 23.

Colaboradores Instituição C

Questões	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Resultados (%)	0,700	0,533	0,600	0,127	0,359	0,467	0,667	0,133	0,087	0,333	0,200	0,906	0,600	0,858	0,383	0,063
Peso	4,861	8,036	4,861	8,036	8,036	8,036	4,861	4,861	8,036	4,861	8,036	4,861	4,861	8,036	4,861	4,861
Final	3,403	4,286	2,917	1,018	2,887	3,750	3,241	0,648	0,702	1,620	1,607	4,404	2,917	6,895	1,863	0,304

Resultado: 42,46 % Nível 2

Figura 23: Análise de iquéritos Instituição C - Colaboradores

No grupo de colaboradores, denota-se alguma falta de clareza e/ou politicas no que respeita à segurança de informação. Quando questionados sobre a existência de um plano de boas práticas e normas de segurança informática na organização (questão 11) uma larga maioria afirma não existir o que remete para uma definição pouco clara da política de segurança da organização e da definição das responsabilidades dos colaboradores.

Quando questionados sobre o bloqueio da sessão de trabalho nas ausências, questão 9, 27% afirma que não o faz porque ninguém disse para fazer, 40% diz que não tem por hábito faze-lo e 33,33 % só bloqueia em ausências perlongadas (questão 4). 53,3% diz que cederia a sua password de acesso a um colega e 33,33% afirma ter conhecimento dessa prática entre os colaboradores da organização (questão 6).

A utilização de *passwords* para acesso ao posto de trabalho (questão 2) é feito apenas por 53,33% dos inqueridos. Apesar de fazerem uso das *passwords* pela análise de algumas das alíneas da questão 5, é possível extrair que 80% dos inqueridos não tem por hábito proceder à sua alteração, 73,3% não fazem uso de símbolos e 80% têm 8 ou menos caracteres, o que fragiliza a sua eficácia/proteção.

Apesar da maioria dos inqueridos classificar a sua apetência para o uso das tecnologias elevado e de considerarem as tecnologias de informação, nomeadamente o uso da Internet, como fundamental para o rendimento e qualidade do trabalho, 93,3% dos inquiridos (questão 16) considera não existir um programa de formação (formação, avaliação de conhecimentos, entre outros) no âmbito da segurança de informação.

Grupo Alvo: Gestão

Ao nível da gestão o enquadramento de nível mantem-se no segundo nível (56,09%), conforme evidencia a Figura 24. Este grupo foi respondido por 7 elementos.

Gestão Instituição C

Questões	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Resultados (%)	0,762	0,714	1	0,109	0,370	0,857	0,571	0,143	0,355	0,429	0,571	0,904	0,286	0,827	0,776	0,000
Peso	2,821	5,245	2,821	5,245	5,245	5,245	2,821	2,821	5,245	2,821	5,245	2,821	2,821	5,245	2,821	2,821
Final	2,149	3,746	2,821	0,569	1,942	4,496	1,612	0,403	1,863	1,209	2,997	2,551	0,806	4,338	2,188	0,000

Questões	17	18	19	20	21	22	23	24	25	26
Resultados (%)	0,875	0,945	0,827	0,429	0,000	0,429	0,776	0,857	0,143	0,286
Peso	5,245	2,821	5,245	2,821	2,821	2,821	5,245	2,821	2,821	5,245
Final	4,589	2,665	4,338	1,209	0,000	1,209	4,068	2,418	0,403	1,499

Resultado: 56,09 % Nível 2

Figura 24 - Análise de Inquéritos Instituição C – Gestão

Ao nível da gestão, pode-se observar que as questões da segurança de informação ainda assumem um papel secundário, apesar de afirmarem que as novas tecnologias suportarem uma grande parte das decisões.

Quando questionados se “são realizadas auditorias de segurança de informação na instituição” (questão 25) 57,10% dos inqueridos afirma que não e 28,60% dizem que não sabem ou não querem responder. Importa ainda evidenciar:

- Que 71,40 % dos inqueridos diz não saber se a política de segurança de informação é partilhada fora da instituição, nomeadamente com parceiros/fornecedores (questão 26);
- Não existe um custo atribuído a cada ativo crítico ou função (questão 21);

- 57,10% (questão 22) afirma não conhecer ou não existir um plano para a continuidade do negócio em caso de desastre.

Ao nível das questões comuns, não se verificam grandes alterações entre este grupo e os colaboradores, excetuando a temática das passwords (questão 5), onde é visível um aumento significativo de preocupação e importância no uso das mesmas. Apesar desta preocupação, pela análise da questão 4, verifica-se que 71,5% dos inqueridos não tem por habito alterar as *passwords* e os restantes 28,5% apenas o fazem uma vez por ano.

Apesar do grupo em análise ter poder de decisão, todos os inqueridos responderam que não existe um programa de formação em segurança de informação na instituição (questão 16) e considerarem o nível de alfabetização dos seus utilizadores e dos recursos com experiencia e qualificação para as questões de Segurança de Informação como médio (questão 23).

Grupo Alvo: Informática

Ao nível do departamento informático, conforme ilustra a Figura 25, foram rececionadas 2 respostas e não existe alteração de nível (59,23%).

Informática
Instituição C

Questões	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Resultados (%)	0,800	1	1	0,750	0,023	1	0,500	1	0,955	1	0,000	0,750	0,000	0,038	0,750	0,000
Peso	2,679	4,762	2,679	4,762	4,762	4,762	2,679	2,679	4,762	2,679	4,762	2,679	2,679	4,762	2,679	2,679
Final	2,143	4,762	2,679	3,572	0,110	4,762	1,340	2,679	4,548	2,679	0,000	2,009	0,000	0,181	2,009	0,000

Questões	17	18	19	20	21	22	23	24	25	26	27	28
Resultados (%)	1	0,5	0,000	0,840	1	1	0,500	0,000	0,500	0,500	0,954	0,223
Peso	4,762	4,762	4,762	4,762	4,762	2,679	2,679	2,679	2,679	2,679	2,679	2,679
Final	4,762	2,381	0,000	4,000	4,762	2,679	1,340	0,000	1,340	1,340	2,556	0,597

Resultado:
59,23 %
Nível 2

Figura 25: Análise de Inquéritos Instituição C – Informática

Na análise deste departamento, à semelhança das outras instituições, as questões relacionadas com a possibilidade de instalação de *software* e utilização de dispositivos de armazenamento USB foram cotadas de forma diferente dos restantes grupos (valorizou-se a possibilidade de instalação/uso como de nível 5, isto é, cotação máxima), em virtude do definido em sede de reunião prévia e ao conteúdo funcional exercida por este grupo.

No que concerne às questões comuns a todos os grupos, também nesta instituição, não existe alterações significativas. De salientar a fraca pontuação obtida por este grupo na temática relativa às *passwords* (questão 5) ao afirmarem que incluem informação pessoal na sua password (ex.: Nome, data, etc), palavras conhecidas e/ou com sentido semântico e não fazem uso de símbolos.

Pelo lado positivo, destacamos o facto de assinalarem que:

- As questões da segurança de informação são consideradas nas decisões da organização (questão 17);
- A monitorização das redes, sistema e aplicações para acessos não autorizados (questão 21);
- A existência de uma estratégia de SI escrita que inclui planos que visam reduzir os riscos a um nível aceitável, com interrupções mínimas para as operações (questão 22).

Apesar de existir uma preocupação ao nível da tecnologia, nas questões direcionadas a este grupo é ainda possível extrair que:

- Não são realizadas auditorias de segurança de informação na instituição (questão 24);
- Não são construídos relatórios com alertas de potenciais ameaças e exposição para os superiores (questão 19).

Para além destas, e face a contrariedade e/ou falta de conhecimento de alguns elementos nas restantes respostas às questões deste grupo, denota-se a ausência de uma eventual politica daquilo que são as normas e/ou cultura da organização, no âmbito da segurança de informação, para este setor em especifico, pois em questões de âmbito global, como seja a existência de uma pessoa ou organização que tenha a segurança de informação como o seu principal dever (questão 23), o conhecimento do uso de clausulas de segurança de informação nos contratos com fornecedores (questão 18), a existência ou conhecimento de algum procedimento na instituição em caso de ataque (questão 26), entre outras, verifica-se que 50% responde sim e os outros 50% não.

Face aos resultados obtidos e à curva de nível adotada, se considerarmos uma análise conjunta de todos os grupos, podemos verificar a existência de algumas dificuldades/*deficit* e ausência de planos e regras ao nível da segurança de informação, o que justifica o enquadramento do nível da instituição no nível 2, conforme ilustra a Figura 26.

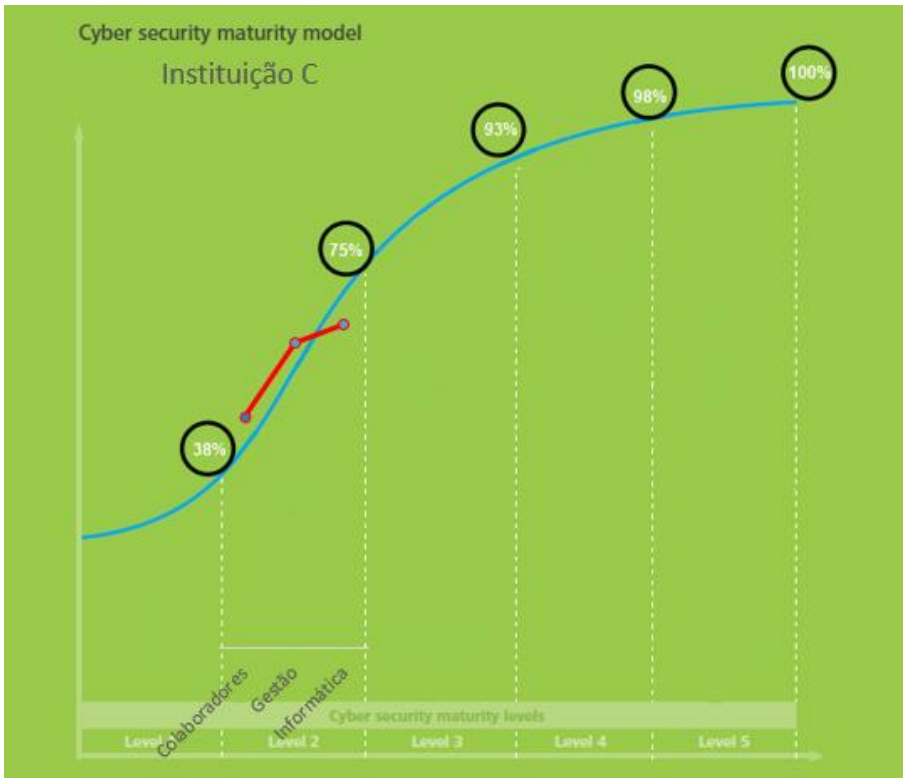
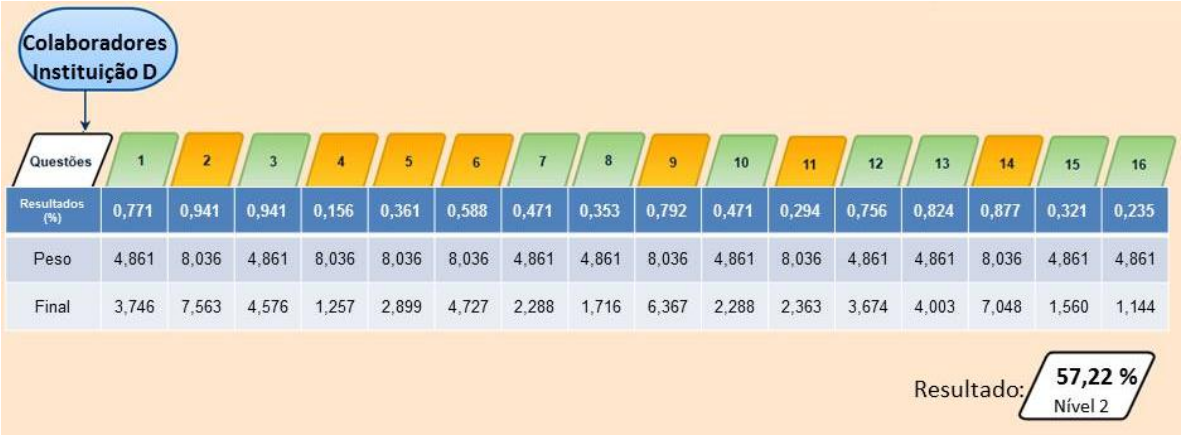


Figura 26: Enquadramento de Nível Instituição C (Inquéritos)

<u>Instituição D</u>

Grupo Alvo: Colaboradores

À semelhança das análises anteriores e da curva de nível adotada e descrita no capítulo 3, a pontuação obtida por este grupo (57,22%) coloca a organização no nível 2 (dois), conforme ilustra a Figura 27.



Colaboradores Instituição D

Questões	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Resultados (%)	0,771	0,941	0,941	0,156	0,361	0,588	0,471	0,353	0,792	0,471	0,294	0,756	0,824	0,877	0,321	0,235
Peso	4,861	8,036	4,861	8,036	8,036	8,036	4,861	4,861	8,036	4,861	8,036	4,861	4,861	8,036	4,861	4,861
Final	3,746	7,563	4,576	1,257	2,899	4,727	2,288	1,716	6,367	2,288	2,363	3,674	4,003	7,048	1,560	1,144

Resultado: 57,22 % Nível 2

Figura 27: Análise de Inquéritos Instituição D - Colaboradores

Pela análise dos inquéritos verificou-se alguma falta de clareza e/ou politicas no que respeita à segurança de informação. Quando questionados (questão 11) sobre a existência

de um plano de boas práticas e normas de segurança informática na organização, 70,59% diz não existir o que remete para uma definição pouco clara da política de segurança da organização e da definição das responsabilidades dos colaboradores.

Pela questão 9, sobre o bloqueio da sessão de trabalho nas ausências, verificou-se que 58,8% só bloqueia em ausências perlongadas e 17,6 % dos inqueridos nunca o faz.

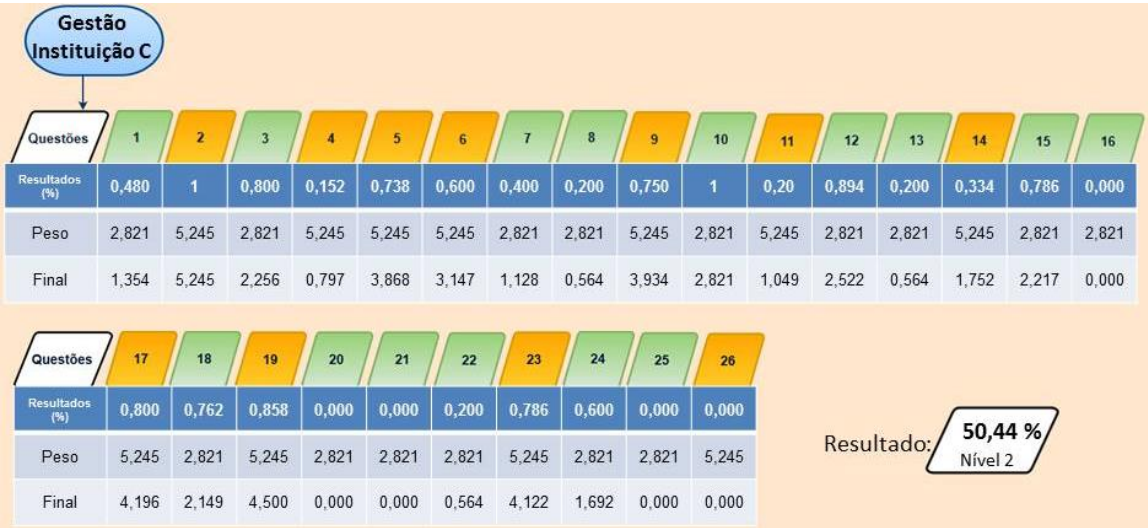
Pela análise da questão 6 é possível extrair que 41,2% dos inqueridos cederia a sua *password* de acesso a um colega e 52,94% (questão 7) afirma ter conhecimento dessa prática entre os colaboradores da organização.

A utilização de *passwords* para acesso ao posto de trabalho, questão 2, é feito por 94,12% dos inqueridos. Apesar de a maioria fazer uso das *passwords*, pela análise das questões 4 e 5 é possível extrair que 64,7% não tem por hábito proceder à sua alteração e que na sua composição, 82,4% não fazem uso de símbolos e 76,5% têm 8 ou menos caracteres, o que fragiliza a sua eficácia/proteção.

Apesar da maioria dos inqueridos classificar a sua apetência para o uso das tecnologias elevado (questão 12), e de considerarem as tecnologias de informação, nomeadamente o uso da Internet, como fundamental para o rendimento e qualidade do trabalho (questão 15), 82,4% dos inquiridos (questão 16) considera não existir um programa de formação (formação, avaliação de conhecimentos, entre outros) no âmbito da segurança de informação.

<u>Grupo Alvo: Colaboradores</u>

Neste grupo, o enquadramento de nível mantem-se no segundo nível (50,44%), conforme evidencia a Figura 28. Este grupo foi respondido por 5 elementos.



Questões	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Resultados (%)	0,480	1	0,800	0,152	0,738	0,600	0,400	0,200	0,750	1	0,20	0,894	0,200	0,334	0,786	0,000
Peso	2,821	5,245	2,821	5,245	5,245	5,245	2,821	2,821	5,245	2,821	5,245	2,821	2,821	5,245	2,821	2,821
Final	1,354	5,245	2,256	0,797	3,868	3,147	1,128	0,564	3,934	2,821	1,049	2,522	0,564	1,752	2,217	0,000

Questões	17	18	19	20	21	22	23	24	25	26
Resultados (%)	0,800	0,762	0,858	0,000	0,000	0,200	0,786	0,600	0,000	0,000
Peso	5,245	2,821	5,245	2,821	2,821	2,821	5,245	2,821	2,821	5,245
Final	4,196	2,149	4,500	0,000	0,000	0,564	4,122	1,692	0,000	0,000

Figura 28: Análise de Inquéritos Instituição D – Gestão

Pela análise global deste grupo pode-se observar que as questões da segurança de informação ainda assumem um papel secundário.

Quando questionados (questão 25) se “são realizadas auditorias de segurança de informação na instituição”, 60 % dos inqueridos afirma que não e os restantes 40% dizem que não sabem ou não querem responder. Importa ainda evidenciar:

- Que a política de segurança de informação não é partilhada fora da instituição, nomeadamente com parceiros/fornecedores (questão 26);
- Não existe um custo atribuído a cada ativo crítico ou função (questão 21);
- 80% afirma não conhecer ou não existir um plano para a continuidade do negócio em caso de desastre (questão 22).

Ao nível das questões comuns, não se verificam grandes alterações entre este grupo e os colaboradores, excetuando a temática das *passwords* (questão 5), onde é visível um aumento significativo de preocupação e importância no uso das mesmas. Apesar desta preocupação pela análise da questão 4 verifica-se que 80% não tem por habito alterar as *passwords*.

Apesar do grupo em análise ter poder de decisão, todos os inqueridos responderam não saber (20%) ou não existir (80%) um programa de formação em segurança de informação na instituição (questão 16).

<u>Grupo Alvo: Informática</u>

Conforme ilustra a Figura 29, ao nível do departamento informático, foram rececionadas 2 respostas e não existe alteração de nível (66,54%).

Informática
Instituição D

Questões	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Resultados (%)	0,750	1	1	0,750	0,813	1	0,000	1	0,930	0,500	0,500	0,750	0,500	0,223	0,038	0,500
Peso	2,679	4,762	2,679	4,762	4,762	4,762	2,679	2,679	4,762	2,679	4,762	2,679	2,679	4,762	2,679	2,679
Final	2,009	4,762	2,679	3,572	3,872	4,762	0,000	2,679	4,429	1,340	2,381	2,009	1,340	1,062	0,102	1,340

Questões	17	18	19	20	21	22	23	24	25	26	27	28
Resultados (%)	1	1	0,500	0,930	1	0,500	0,500	0,000	0,500	0,000	0,930	0,223
Peso	4,762	4,762	4,762	4,762	4,762	2,679	2,679	2,679	2,679	2,679	2,679	2,679
Final	4,762	4,762	2,381	4,429	4,762	1,340	1,340	0,000	1,340	0,000	2,491	0,597

Resultado:
66,54 %
Nível 2

Figura 29: Análise de Inquéritos Instituição D – Informática

Na análise deste grupo, as questões relacionadas com a possibilidade de instalação de *software* e utilização de dispositivos de armazenamento USB foram cotadas de forma diferente dos restantes grupos (valorizou-se a possibilidade de instalação/uso como de nível 5), em virtude do definido em reuniões prévios e daquilo que é o conteúdo funcional exercida por este grupo.

No que concerne às questões comuns a todos os grupos, além de uma maior preocupação e melhores resultados nas politicas e uso *passwords* (questão 5), um dos aspetos curiosos e que contrasta com os restantes grupos, é a totalidade dos inqueridos afirmar ter conhecimento de colegas que divulgam a password a outros colegas (questão 7).

Pelo lado positivo, destacamos o facto de assinalarem que:

- As questões da segurança de informação são consideradas nas decisões da organização (questão 17);
- O uso de cláusulas de salvaguarda das políticas de segurança nos contratos com terceiros (questão 18).

Apesar de existir uma preocupação ao nível da tecnologia, pela análise da questão 26 é possível extrair que não existem procedimentos em vigor na instituição para atuação em caso de ataque.

Para além destas, e face a contrariedade e/ou falta de conhecimento de alguns elementos nas restantes respostas às questões deste grupo, denota-se a ausência de uma eventual politica daquilo que são as normas e/ou cultura da organização, no âmbito da segurança de informação, para este setor em especifico, pois em questões de âmbito global, como seja a criação de relatórios com alertas de potenciais ameaças (questão 19), a existência de uma pessoa ou organização que tenha a segurança de informação como o seu principal dever (questão 23), a realização de auditorias de segurança de informação (questão 24), o uso de clausulas de salvaguarda das politicas nos contratos com terceiros (questão 18), entre outras, verifica-se que 50% responde sim e os outros 50% não.

Se considerarmos uma análise conjunta de todos os grupos, podemos verificar a existência de algumas dificuldades/*deficit* e ausência de planos e regras ao nível da segurança de informação, o que justifica o enquadramento do nível da instituição no nível 2, conforme ilustra a Figura 30.

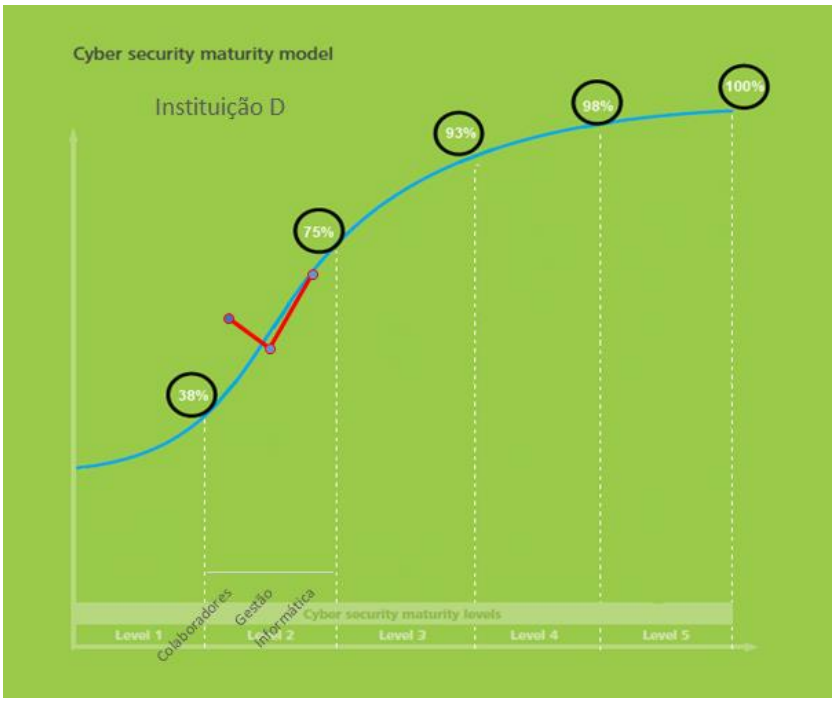


Figura 30: Enquadramento de Nível da Instituição D (Inquéritos)

Uma das possibilidades que emerge da presente metodologia é a possibilidade de comparação entre *peers*. A Figura 31 ilustra a posição/comparação das organizações. Para uma facilidade de leitura, interpretação e congruência da estratégia adotada e dos resultados obtidos usamos a curva de nível adotada, mas de forma invertida.

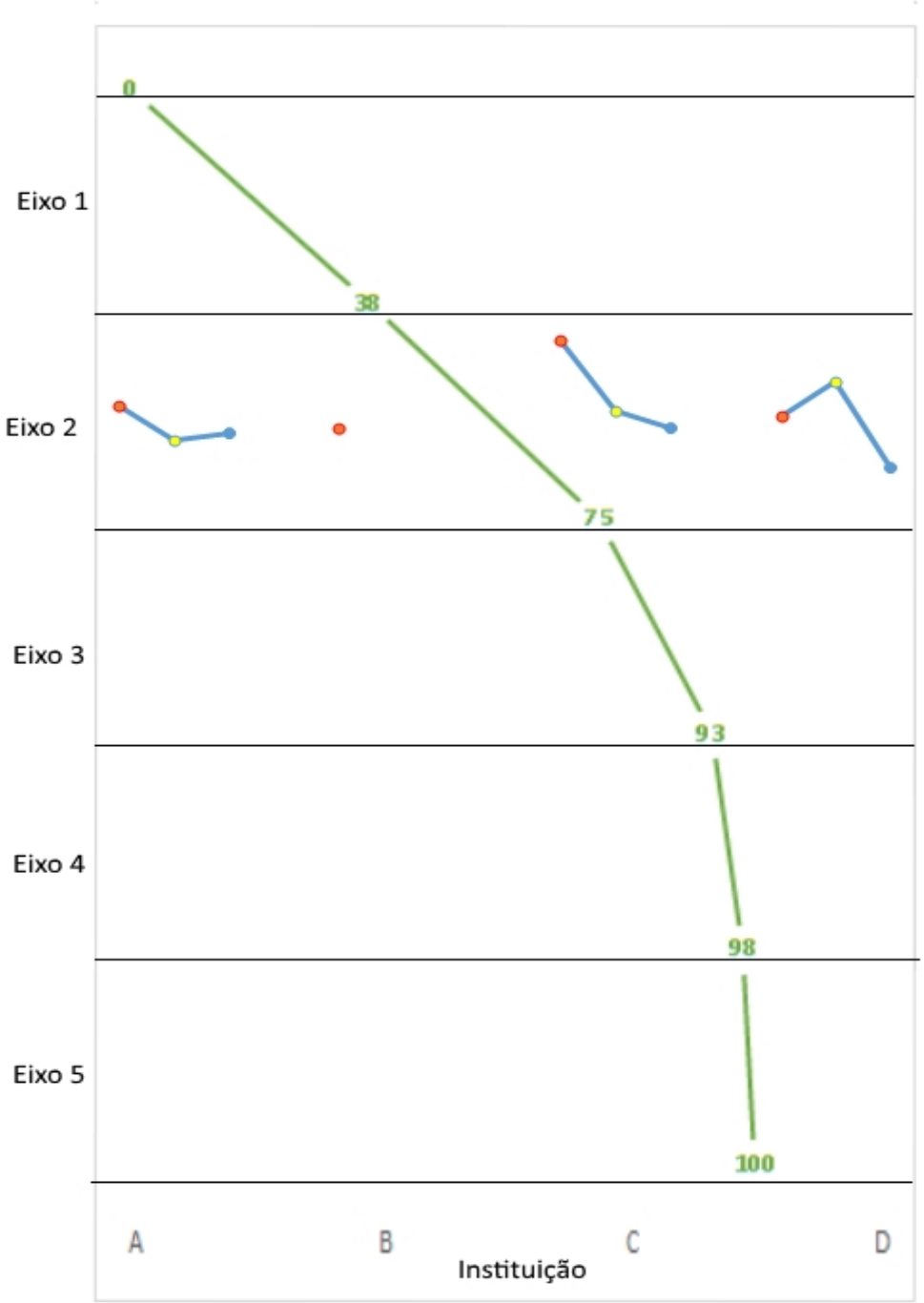


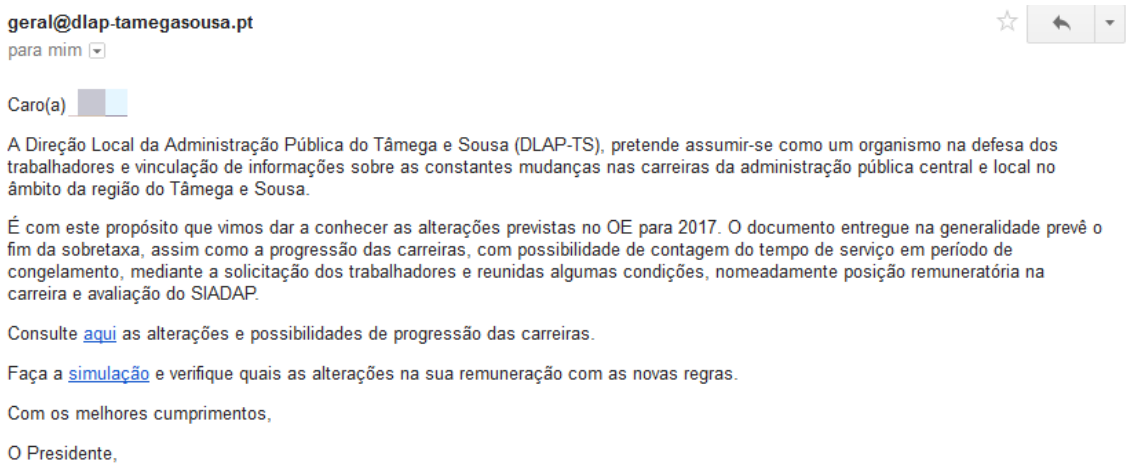
Figura 31: Posição/comparação das organizações (Eixo 1)

Conforme ilustra a figura, todas as organizações e grupos em análise ficam posicionados no nível 2, numa escala de 1 a 5 onde o nível 1 é o mais baixo e o 5 o mais forte. Pela análise da mesma figura, pode-se ainda observar a existência de uma ligeira alteração sobre a compreensão dos comportamentos de risco entre as várias estruturas em análise.

Eixo 2

Ao longo desta subseção procedemos a fase de análise e apresentação dos resultados do eixo 2. A campanha foi planeada/executada, tendo em consideração o acordado com as entidades e o constante na metodologia. Seguidamente apresentamos uma síntese da ação seguido da análise de resultados.

Número de Instituições:	4
Número de funcionários sob teste:	50 x 4
Data de início:	17/11/2016
Data de término:	21/11/2016
Número de envios de *e-mail*:	50 x 4
Use Case:	E-mail com link direcionável para uma página sob controlo do atacante. Uma vez clicado e a pagina acedida, o colaborador é convidado a clicar em mais um link (2º nível) para download (3º nível) de um ficheiro em excel, com macros autoexecutáveis
E-mail enviado:	Foi emitido um e-mail aos colaboradores das instituições com indicação das alterações previstas no OE 2017, relativo às Carreiras da Administração Pública. O e-mail enviado contém um link que permite efetuar uma simulação sobre as diferenças salariais. A Figura 32 ilustra o e-mail recebido pelos colaboradores



geral@dlap-tamegasousa.pt
para mim

Caro(a)

A Direção Local da Administração Pública do Tâmega e Sousa (DLAP-TS), pretende assumir-se como um organismo na defesa dos trabalhadores e vinculação de informações sobre as constantes mudanças nas carreiras da administração pública central e local no âmbito da região do Tâmega e Sousa.

É com este propósito que vimos dar a conhecer as alterações previstas no OE para 2017. O documento entregue na generalidade prevê o fim da sobretaxa, assim como a progressão das carreiras, com possibilidade de contagem do tempo de serviço em período de congelamento, mediante a solicitação dos trabalhadores e reunidas algumas condições, nomeadamente posição remuneratória na carreira e avaliação do SIADAP.

Consulte aqui as alterações e possibilidades de progressão das carreiras.

Faça a simulação e verifique quais as alterações na sua remuneração com as novas regras.

Com os melhores cumprimentos,

O Presidente,

Figura 32: E-mail Campanha Phishing

Antes de se apresentar os resultados e considerando a sensibilidade do assunto e a gravidade que pode representar para uma organização a leitura de e-mails e o acesso a *links* desconhecidos, importa salientar que em momento algum será feita, nesta análise, qualquer referência aos colaboradores que tiveram um comportamento de risco.

Para a análise e cálculo foram empregues os métodos constantes no capítulo 3. Em função do acordado em reuniões prévias, os resultados referem-se às primeiras 24 horas, após o envio da campanha. A lista de consequência e critérios de análise (Ação – Consequência – Nº de ocorrências), foi feita por nós a pedido das organizações e discutida antes do lançamento da campanha. A organização fica posicionada no nível, analisado do mais baixo (1) para o mais alto (5), onde se observe um ou mais dos comportamentos/consequência definidos em cada nível. A lista de consequências ficou organizada da seguinte forma: nível 1: abriu o e-mail, clicou nos link´s, abriu o ficheiro e ativou a macro; nível 2: abriu o e-mail e clicou no link; nível 3: abriu e descartou o e-mail; nível 4: abriu e reencaminhou para a equipa de Informática; nível 5: não abriu o e-mail.

De seguida são apresentados os resultados por instituição.

Instituição A

Na Figura 33 são ilustradas as estatísticas gerais da campanha. Como se pode verificar foram carregados na aplicação de engenharia social da instituição A 50 endereços únicos de e-mail, escolhidos aleatoriamente da lista de endereços fornecidos pela própria. Durante a execução da campanha foram enviados 50 e-mails separados por pequenos períodos temporários. Este desfasamento temporal, deve-se ao facto do servidor de e-mail

fazer throttling. Dos 50 E-mails, 39 e-mails saíram de imediato e houve 11 que por razões de e-mail throttling deram erro, tendo sido necessário proceder ao seu reenvio. Face às aplicações de gestão de correio utilizada pela organização, onde maioritariamente o e-mail é lido em modo de "pré-visualização" não é possível obter o número de e-mail abertos (a imagem que faz o tracking não é ativada). De salientar ainda que 22 colaboradores clicaram no *link* incluído no corpo do e-mail de simulação de *phishing*, correspondendo assim a 44% dos e-mails enviados e uma utilizador não só abriu o ficheiro como correu a macro.

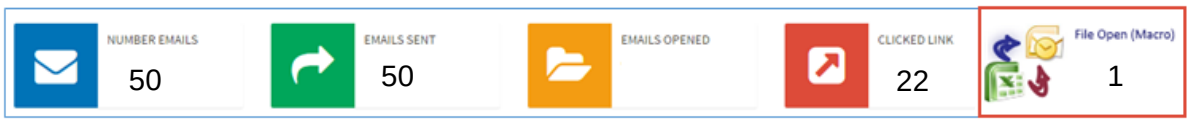


Figura 33: Estatísticas globais da campanha – Instituição A

Os resultados da campanha mostram que os colaboradores da Instituição A têm um grau de maturidade baixo relativamente às técnicas de engenharia social utilizadas em ciber ataques. É de salientar que, de acordo com o definido e estipulado na metodologia, para uma empresa/organização estar em risco basta apenas que um utilizador tenha um comportamento de risco.

No caso da Instituição A esse risco é exponenciado pelo facto de 44% dos colaboradores terem clicado no link do e-mail que numa situação real levaria ao extravio de dados ou à instalação de malware. Apesar de não ser possível quantificar o número de pessoas que clicou no link do 2º nível (Note-se que a macro envia um e-mail com a informação "ficheiro aberto pela instituição …", razão pela qual apenas é possível identificar o numero de ficheiros com a macro ativa e não o numero de cliques do 2º nível e/ou ficheiros abertos sem ativação da macro), este risco torna-se ainda mais critico ao se verificar que um dos utilizadores ativou a macro, mesmo depois dos avisos de segurança, pré-definidos pela ferramenta do office, colocando a organização em risco eminente caso se tratasse de uma situação real. O baixo tempo entre o envio de e-mails e os primeiros resultados é também um elemento a considerar. Os colaboradores abriram o e-mail, clicaram nos links e abriram o ficheiro de forma muito proactiva, sendo que neste caso a proatividade não beneficia a instituição.

Face aos resultados obtidos, pelo emprego do algoritmo e o previamente acordado com a organização, a instituição enquadra-se no nível de maturidade de segurança de informação mais baixo, isto é, no nível 1.

Instituição B

Na Figura 34 são ilustradas as estatísticas gerais da campanha. À semelhança da instituição anterior, foram carregados e enviados 50 endereços únicos de e-mail, escolhidos aleatoriamente da lista de endereços fornecidos pela própria. Dos 50 E-mails, 46 e-mails saíram de imediato e houve 4 que por razões de e-mail throttling deram erro, tendo sido necessário proceder ao seu reenvio. Também aqui e pelas mesmas razões da anterior, não é possível obter o numero de e-mail abertos. Pelos resultados obtidos, podemos aferir que 26 colaboradores clicaram no *link* incluído no corpo do e-mail de simulação de *phishing*, correspondendo assim a 52% dos e-mails enviados. 50% dos utilizadores que clicaram no link do e-mail, não só clicaram no link do segundo nível, como abriram o ficheiro e ativaram as macros.

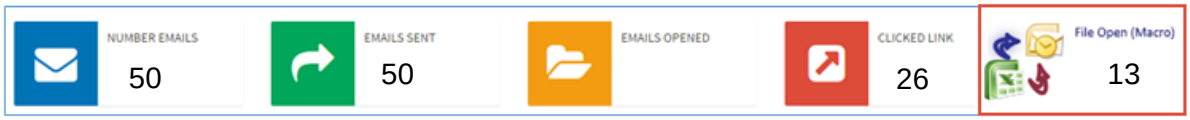


Figura 34: Estatísticas globais da campanha

Os resultados da campanha mostram que os colaboradores da Instituição B têm um grau de maturidade muito baixo relativamente às técnicas de engenharia social utilizadas em ciber ataques. Este risco é exponenciado pelo facto de 52% dos colaboradores terem clicado no link do e-mail e 50% desses terem aberto o ficheiro e ativado as macros, depois dos avisos de segurança, pré-definidos pela ferramenta do office, o que numa situação real levaria ao extravio de dados ou à instalação de malware. O baixo tempo entre o envio de e-mails e os primeiros resultados é também um elemento a considerar. Os colaboradores abriram o e-mail, clicaram nos links e abriram o ficheiro de forma muito proactiva, sendo que neste caso a proatividade não beneficia a instituição.

Face aos resultados obtidos, pelo emprego do algoritmo e acordado previamente, a instituição enquadra-se no nível de maturidade de segurança de informação mais baixo, isto é, no nível 1.

Instituição C

Na Figura 35 são ilustradas as estatísticas gerais da campanha. O procedimento adotado foi o mesmo das instituições anteriores. Dos 50 E-mails, 31 e-mails saíram de imediato e houve 19 que por razões de e-mail throttling deram erro, tendo sido necessário proceder ao seu reenvio. Assim como nas anteriores, verificou-se a impossibilidade de

obtenção do número de e-mails abertos, pelas razões supra transcritas. Da campanha resulta que 21 colaboradores clicaram no *link* incluído no corpo do e-mail de simulação de *phishing*, correspondendo assim a 42% dos e-mails enviados. 47,6% dos cliques no link do e-mail, não só clicaram no link do segundo nível, como abriram o ficheiro e ativaram as macros.

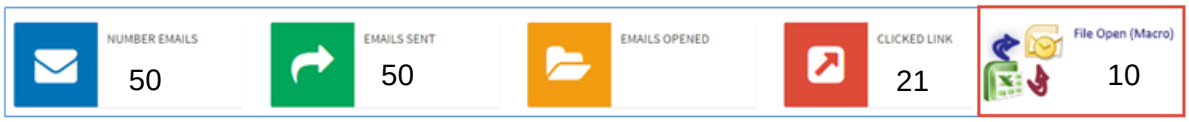


Figura 35: Estatísticas globais da campanha

Os resultados da campanha mostram que os colaboradores da Instituição C têm um grau de maturidade bastante baixo relativamente às técnicas de engenharia social utilizadas em ciber ataques. No caso da Instituição C esse risco é exponenciado pelo facto de 42% dos colaboradores terem clicado no link do e-mail e 47,6% desses terem aberto o ficheiro e ativado as macros, depois dos avisos de segurança, pré-definidos pela ferramenta do office, o que numa situação real levaria ao extravio de dados ou à instalação de malware, colocando a organização, numa situação real, em risco eminente. O baixo tempo entre o envio de e-mails e os primeiros resultados continua a ser um elemento a considerar. Os colaboradores abriram o e-mail, clicaram nos links e abriram o ficheiro de forma muito proactiva, sendo que também neste caso a proatividade não beneficia a instituição.

Face aos resultados obtidos, pelo emprego do algoritmo e o previamente acordado com a organização, a instituição enquadra-se no nível de maturidade de segurança de informação mais baixo, isto é, no nível 1.

Instituição D

Na Figura 36 são ilustradas as estatísticas gerais da campanha. À semelhança das anteriores, por razões de e-mail throttling, dos 50 E-mails enviados, 43 e-mails saíram de imediato e houve 7 que deram erro, tendo sido necessário proceder ao seu reenvio. Também aqui se verifica a impossibilidade de obter o numero de e-mail abertos. Da análise da campanha, resulta que 25 colaboradores clicaram no *link* incluído no corpo do e-mail de simulação de *phishing*, correspondendo assim a 50% dos e-mails.

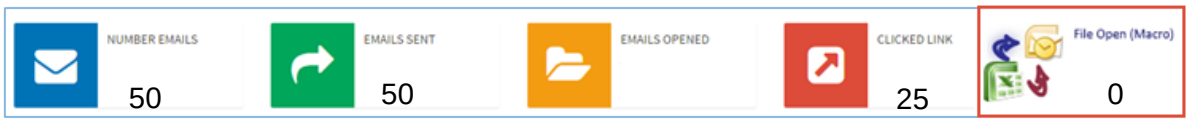


Figura 36: Estatísticas globais da campanha

Os resultados da campanha mostram que os colaboradores da Instituição D têm um grau de maturidade baixo relativamente às técnicas de engenharia social utilizadas em ciber ataques. No caso da Instituição D esse risco é exponenciado pelo facto de 50% dos colaboradores terem clicado no link do e-mail que numa situação real levaria ao extravio de dados ou à instalação de *malware*. O baixo tempo entre o envio de e-mails e os primeiros resultados continua a ser um elemento a considerar.

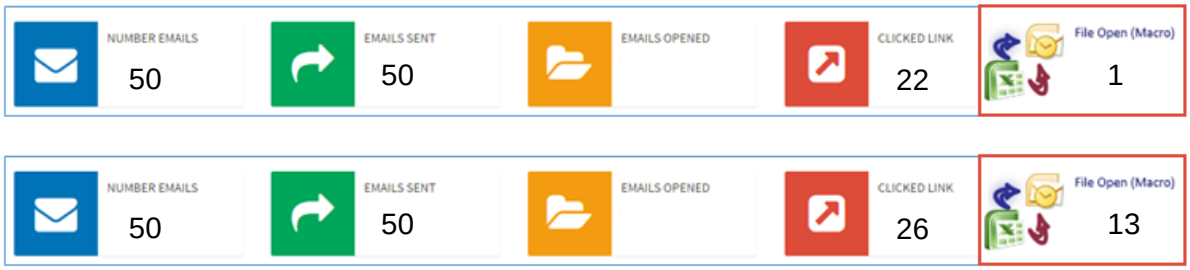
Apesar de 50% dos utilizadores terem clicado no link, verificou-se que nenhum dos utilizadores ativou a macro do ficheiro.

Face aos resultados obtidos, neste eixo e ao descrito no algoritmo do capítulo 3 a instituição enquadra-se no nível 2 de maturidade de segurança de informação

Resultados gerais

A Figura 37 apresenta os resultados combinados e por isso, a comparação das instituições em análise. Pela análise, é possível afirmar que todas as instituições são suscetíveis ao risco face ao comportamento dos seus colaboradores, o que numa situação real levaria ao extravio de dados ou à instalação de malware, colocando a organização em risco eminente. De salientar que estes resultados referem-se às primeiras 24 horas após o lançamento da campanha.

A campanha de phishing criada apresentava um cenário com vários níveis. Ainda que não tenha sido possível avaliar o número de e-mails abertos, verificou-se que uma grande parte dos utilizadores de todas as instituições (+ 40%) clicaram no link do e-mail e, por isso, acederam à página indicada pela origem. Apesar de também não ser possível avaliar o número de pessoas que clicaram nos links existentes na página (2º nível) e que remetiam para um ficheiro com macros autoexecutáveis, em 3 das 4 instituições verificou-se a ativação das macros apesar da mensagem do office a alertar para o risco do ficheiro. Reforça-se novamente que a macro enviava um e-mail com a informação “ficheiro aberto pela instituição …”, razão pela qual apenas é possível identificar o numero de ficheiros com a macro ativa e não o numero de cliques do 2º nível e/ou ficheiros abertos sem ativação da macro.



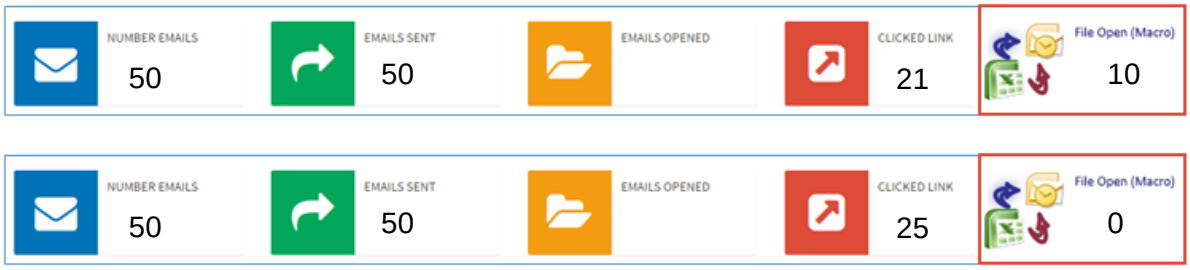


Figura 37: Resultados comparativos (eixo 2)

Apesar da existência de um comportamento incorreto ser o suficiente para por toda a organização em risco as organizações B e C são as que apresentam a maior exposição ao risco, seguido da A e por último a C. Apesar de não se verificar a ativação da macro por parte da organização C, não poderemos afirmar que a mesma não comporte riscos, pois como se pode verificar 50% dos utilizadores clicaram no link de um e-mail desconhecido, situação que poderia acarretar riscos.

Face aos resultados deste eixo, a instituição A, B e C, ficam posicionadas no nível 1 e a instituição C no nível 2.

4.4. Resultados inter-eixos

Tendo em consideração os resultados obtidos nos dois eixos experimentados e o constante na Figura 13, através do emprego da média aritmética simples, a instituição A, B e C, ficam posicionadas no nível 1 e a instituição D no nível 2, conforme ilustra a Tabela 11.

	Eixo 1	Eixo 2	Eixo 3	Resultado combinado (média)
Organização A	Nível 1	Nível 2		Nível 1
Organização B	Nível 2	Nível 2		Nível 1
Organização C	Nível 3	Nível 2		Nível 1
Organização D	Nível 2	Nível 2		Nível 2

Tabela 10: Resultados inter-eixos

De acordo com a metodologia, cada eixo em análise tem validade por si só. A tabela não só apresenta o nível obtido em cada eixo como também o resultado combinado dos eixos. Tal representação permite a comparação e avaliação dos resultados entre as diferentes entidades nas múltiplas comparações e/ou inferências desejadas.

Capitulo 5

Conclusões e Trabalho Futuro

Neste capítulo, apresentamos um resumo do trabalho realizado e referem-se as principais contribuições para a área da segurança de informação. São também tecidas algumas recomendações sobre os resultados obtidos e trabalho futuro.

O objetivo principal deste trabalho era criar uma metodologia de fácil aplicação e interpretação para o cálculo do Índice de Maturidade de Segurança Informática das Organizações (IMSI). A metodologia está distribuída por três eixos: (1) Inquéritos. (2) Engenharia Social e (3) Analise de Vulnerabilidades/Auditoria e contempla três áreas funcionais: (1) Pessoas, (2) processos e (3) Tecnologia.

O trabalho desenvolvido com vista à apresentação desta tese começou, por uma revisão do estado-da-arte na área da Segurança de Informação, estendeu-se no desenvolvimento e apresentação de uma metodologia para o cálculo do IMSI e acabou na sua experimentação.

A metodologia consiste num guia de referência no qual estão elencados o conjunto de procedimentos a realizar. Está dividida em três áreas de análise às quais damos o nome de eixo. No eixo 1 (inquéritos), começa-se por elucidar o planeamento e desenho do questionário e abordam-se, entre outros, a conceção das questões, o desenho do questionário e os métodos de recolha e análise de dados. No eixo 2 (engenharia social), além de explorarmos os conceitos de engenharia social e as suas manifestações mais populares, apresentamos um conjunto de procedimentos para avaliar a maturidade das organizações no que diz respeito à resiliência deste tipo de ataques. Abordam-se, entre outros, a conceção e desenho de campanhas de phishing e os métodos de recolha e análise de dados. No eixo 3 (análise de vulnerabilidades), sob a ótica de que para gerir o risco é preciso conhecer as vulnerabilidades, exploramos os conceitos de análise de vulnerabilidades e apresenta-se um algoritmo para a recolha e análise de dados.

O estudo sobre a segurança de informação e as suas várias formas de manifestação permitiu desenvolver uma metodologia de fácil compreensão e aplicação sem necessidade de especialistas nem grandes recursos técnicos. Tal abordagem diferencia-a do existente no mercado, na medida em que pretende ser uma metodologia de "*entry level*", pelo que se espera que seja de mais simples acesso e aceitação capaz de apresentar, no mapeamento das ameaças e gestão do risco, resultados fidedignos e de fácil interpretação pelas várias estruturas das organizações. Tais características contrastam com a análise de risco "clássica", que como apresentado no estado da arte, são de difícil aplicação, requerem

recursos técnicos especializados, muitas vezes com custos elevados e com resultados de difícil interpretação por algumas estruturas, nomeadamente pela camada de gestão.

A metodologia assenta num conjunto de prossupostos, com métricas e algoritmos definidos, que depois de analisados e avaliados permite enquadrar a instituição num dos 5 níveis de maturidade propostos. Tal avaliação contribui para a perceção das fragilidades/vulnerabilidades das organizações e consequente modelação do processo de gestão e manutenção da informação ao nível dos processos, pessoas e tecnologias.

Para validação e exequibilidade da metodologia foi feita uma experimentação no terreno (prova de conceito). Começou-se por identificar o público-alvo, seguiu-se o agendamento de reuniões na apresentação do trabalho, obtenção de autorizações e definição de objetivos de aplicação para cada um dos eixos. Os objetivos deram corpo ao planeamento e consequente execução dos testes.

A prova de conceito e experimentação da metodologia permiti-nos, com base nos resultados, aferir que as organizações priorizam os aspetos funcionais que atendem a área de negócios, enquanto os requisitos de segurança (principalmente ao nível da pessoas e da definição de politicas e procedimentos), muitas vezes por falta de informação e desconhecimento ficam em segundo plano. Tal situação coloca as organizações num nível de exposição ao risco elevado.

A existência de meios tecnológicos com vista a proteção e segurança de informação por parte das organizações envolvidas é uma realidade. Esta realidade ainda que necessária para manter o ambiente seguro, em funcionamento e com desempenho favorável, no cômputo geral é muito deficitária, sendo necessário, em relação à segurança de informação, um programa estruturado que contemple não só a parte tecnológica e física, mas também a humana e de processos, vertentes onde se verificam as maiores lacunas.

A avaliação da criticidade que emerge dos resultados dos vários eixos propostos e da aplicação da metodologia, não é substancialmente inalterada entre os vários setores da organização e organizações em análise.

Com o trabalho agora apresentado, pensamos contribuir para uma mais simples estruturação e formalização do conhecimento das organizações sobre a temática da segurança de informação e das suas vulnerabilidades com vista à preservação da disponibilidade, confiabilidade e integridade da informação, o que facilitará a tomada de decisão e a proteção das pessoas e do negócio.

No curto prazo, com base nos resultados obtidos, as organizações podem: definir/redefinir políticas de segurança; promover programas de educação e treino; definir um reforço por via da tecnologia; aprofundar uma análise de risco mais minuciosa.

5.1 Trabalho Futuro

Todo o trabalho de investigação feito, que culmina com a apresentação da presente tese, permite sugerir algumas orientações de trabalho futuro que, dando continuidade ao apresentado aqui, poderão trazer contributos importantes para o refinamento da metodologia aqui proposta.

O tempo para a realização do trabalho foi uma limitação. Tal limitação foi agravada, pelo facto da experimentação da metodologia no terreno necessitar de autorizações, concordância e dados de entidades externas, o que nem sempre foi fácil ou fornecido nos tempos adequados e/ou acordados pelas partes.

No seguimento deste trabalho, uma primeira abordagem pode ser a operacionalização do eixo 3, na criação de, por exemplo, planos de formação e planos de segurança passiveis de darem resposta às vulnerabilidades que emergem dos eixos 1 e 2.

Seria também interessante verificar a aplicação das técnicas desenvolvidas no âmbito deste trabalho, num sistema colaborativo de aplicação, com o envolvimento das equipas de gestão, com vista a uma maior focalização e uniformização das formas de análise dos vários eixos.

Uma outra questão no âmbito desta investigação, que apesar de ter sido considerada inicialmente, por requisitos de tempo não foi devidamente explorada, tem a ver com a necessidade da criação de métricas que aprofundem a forma como as várias estruturas das organizações, priorizam ou relativizam determinados aspetos ou áreas da segurança de informação.

Um trabalho futuro, que emerge do agora apresentado é a necessidade da metodologia, ser mais testada e afinada no sentido de se tornar uma referência na área da análise de risco, em particular como instrumento de *first/fast assessment*.

Referências bibliográficas

[1] Reuters, Global Internet population grows to 3.2 billion: study, http://www.dailymail.co.uk/sciencetech/article-3458733/Global-Internet-population-grows-3-2-billion-study.html, consultado em 2016-07-18

[2] Marktest, Bareme Internet relatório 2015 (2016, 22 jul.), disponível em www.marktest.com

[3] Abraham Y., What Happens in an Internet Minute?, disponível em http://www.excelacom.com/resources/blog/what-happens-in-an-Internet-minute-how-to-capitalize-on-the-big-data-explosion, consultado em 23/07/2016

[4] PORDATA (2016) , Base de Dados de Portugal Contemporâneo, Fundação Francisco Manuel dos Santos, disponível em www.pordata.pt

[5] McAfee, (2013 Julho), The Economic Impact of Cybercrime and Cyber Espionage, disponível em http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

[6] Juniper Research, Cybercrime will Cost Businesses Over $2 Trillion by 2019, Hampshire**,** UK **-** 12th May 2015**,** disponível **em** https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion, consultado em 09/11/2016

[7] Dekker, M., Karsberg, C., & Lakka, M. (2012). Annual Incident Reports 2012. Crete, Greece: European Union Agency for Network and Information Security (ENISA).

[8] Deloitte, (2013) The cyber security imperative, disponível em http://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-13-3694-cyber-security-pov-fin.pdf

[9] Armaghan, B. & Rafhana, A.R., A Survey of information Security Risk Analysis, Smart Computing Review, vol. 2, no. 1, 2012

[10] MAI - Ministério da Administração interna - Governo de Portugal, (2014) Relatório Anual de Segurança Interna 2014, disponível em http://www.portugal.gov.pt/media/6877606/20150331-rasi-2014.pdf

[11] CNCS - Centro Nacional de Cibersegurança, (2016, 5 Jan), disponível em http://www.cncs.gov.pt/sobre-cncs/index.html

[12] ISO - International Organization for Standardization, (2016, 5 jan.) ISO 31000 – Risk Management, disponível em https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

[13] ISO - International Organization for Standardization, (2016, 5 jan.) ISO 27001 – Information security management, disponível em https://www.iso.org

[14] ISO - International Organization for Standardization, (2016, 5 jan) ISO 27002 – Information technology -- Security techniques -- Code of practice for information security controls, disponível em https://www.iso.org

[15] SO/IEC. (2009b). ISO/IEC 27000:2009, Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva, Switzerland: International Commission Organization for Standardization/International Electrotechnical.

[16] REZENDE, Denis Alcides. Planeamento de Sistemas de Informação e Informática: guia prático para planear a tecnologia da informação integrada ao planeamento estratégico das organizações. 4. ed. São Paulo: Atlas, 2011.)

[17] FERREIRA, F.; ARAÚJO, M. Política de Segurança de Informação - Guia Prático para Elaboração e Implementação. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

[18] Dantas, M. Segurança de informação: uma abordagem focada em gestão de riscos. 1 ed. Olinda: livro rápido, 2011 citado por Cardoso F, Oliveira P., Politica de Segurança de Informação nas Empresas, disponível em https://s.profissionaisti.com.br/wp-content/uploads/2013/06/Politica-de-Seguran%C3%A7a-nas-Empresas.pdf

[19] Project Management Institute. A guide to the project management body of knowledge – PMBOK Guide. Newtown Square: PMI, 2004, citado por ROVAI R. Modelo Estruturado para a Gestão de Riscos ewm Projetos: Estudos de Múltiplos Casos, Escola politécnica da Universidade se São Paulo, 2005

[20] GAIVEO N.(2016), Análise e Gestão do Risco em Segurança de Informação, SINFIC - Sistemas de Informação Industriais e Consultoria, SA, disponível em http://www.sinfic.pt/SinficWeb/displayconteudo.do2 ?numero=24868#

[21] NAKAMURA, E.and PAULO L. *Segurança de redes*. Berkeley, 2002

[22] ISACA. **COBIT 5** - Enabling Processes. Meadows, 2012.

[23] STUTTARD, Dafydd; PINTO, Marcus. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. 2. ed. Indianapolis: Wiley, 2011 citado por Reinaldo F et all, Information Security Framework, disponível em www.contecsi.fea.usp.br

[24] Natário R. "O CIBERESPAÇO E A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS: Contributos para um Modelo Nacional de Análise e Gestão do Risco Social", Academia Militar, Tese de mestrado, Lisboa, 2014]

[25] NIST (National Institute of Standards and Tecnhlogy) (2016, 27 jun.) Cybersecurity Framework (CSF), disponível em http://www.nist.gov/cyberframework/csf_reference_tool.cfm

[26] SCHNEIER, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2. ed. New York: Wiley, 1996.

[27] Ming-Chang L., Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method, international Journal of Computer Science & Information Technology (IJCSIT) Vol 6, No1, 2014

[28] Macedo, F. (2009) *Models for Assessing Information Security Risk* (Tese de Mestrado). Universidade Técnica de Lisboa, Portugal

[29] Software Engineering Institute (SEI) - Carnegie Mellon University (2016, 5 jan) OCTAVE, disponível em: http://www.cert.org/octave/octavemethod.html

[30] Federal Ofice for Information Security (2016, 6 jan), IT-Grundschutz, disponível em https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

[31] Club de la Sécurité Informatique Français (CLUSIF). MARION (2016, 5 jan) Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau, disponível em <https://www.clusif.asso.fr/en/clusif/present/

[32] ISACA (Information Systems Audit and Control Association (2016, 5 Jan.) COBIT (Control Objectives for Information and related Technology, disponível em https://cobitonline.isaca.org/

[33] ENISA - European Union Agency for Network and Information Security (2016, 16 jun.), disponível em https://www.enisa.europa.eu/

[34] Information Security Assessment & Monitoring Method (2016, 7 Jan) ISAMM, disponível em http://www.telindus.com

[35] Gobierno de Espanha (2016, 7 jan) MAGERIT v.3: Methodology of analysis and risk management information systems, disponível em http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en#.VpvWb1L-s7g

[36] Club de la Sécurité Informatique Français (CLUSIF). MEHARI (2016, 5 jan) MEthod for Harmonized Analysis of RIsk, disponível em <https://www.clusif.asso.fr

[37] Information Security Forum, (2016, 7 jan) IRAM, disponível em https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/

[38] Barão A., IT Governance - Risco e Segurança dos SI no sector financeiro – Prova de Conceito no regulador Portugues, Escola Superior de Ciências Empresariais, IPS, 2015 dispopnivel em, https://comum.rcaap.pt/bitstream/

[39] Alves N., Investigação por Inquérito, Lic. Em Matemática Aplicada, Universidade dos Açores (2005/2006)

[40] PSE – Produtos e Serviços de estatistica, lda (2016, 16 jun) - Um guião para ajudá-lo a poupar tempo e dinheiro quando planeia, desenvolve e executa um inquérito, disponível em http://www.pse.pt/wp-content/uploads/2011/08/PSE-Survey-Tips.pdf

[41] GOODE, W., HATT, P. (1979). *Métodos em Pesquisa Social* (pp. 171-235), 7ª Edição. São Paulo, Brasil: Companhia Editora Nacional

[42] GHIGLIONE, R. e MATALON, B. (1992), *O Inquérito, Teoria e Prática*, Oeiras, Celta Editora, citado por Ferreira M, Campos P. Uma introdução à elaboração de questionários, amostragem, organização e apresentação de resultados, disponível em http://homepage.ufp.pt/cmanso/ALEA/Dossier11.pdf (2016, 27 jun).

[43] Force password, disponível em http://www.passwordmeter.com/, consultada em 18/07/2016

[44] Force password, https://password.kaspersky.com/, consultada em 18/07/2016

[45] R. Pais et all, Engenharia Social (ou o carneiro que afinal era um lobo), Almedina, 2013 disponivel em http://hdl.handle.net/1822/26251

[46] Mitnick, K., Simon, W., Wozniak, S., “The Art of Deception”, John Wiley & Sons (2002), citado por Pais R. Moreira F., Varajão J. Engenharia Social (ou o carneiro que afinal era um lobo), Universidade do Minho, disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/26251/1/ntmi2013-2.pdf

[47] Methodology social engineering, disponível em http://www.7-network.com, consultada em 24/07/2016

[48] CAMPOS, A. Sistemas de Segurança de Informação. 2 ed. Florianopolis: Visual Books, 2007 citado por Cardoso F, Oliveira P., Politica de Segurança de Informação nas Empresas, disponível em https://s.profissionaisti.com.br/wp-content/uploads/2013/06/Politica-de-Seguran%C3%A7a-nas-Empresas.pdf

[49] OWASP - Open Web Application Security Project, (2016, 6 jan), disponível em https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

[50] Ecommerce Europe – B2C Ecommerce Report Central Europe 2014 FULL, disponivel em https://www.ecommerce-europe.eu, consultado em 16 de julho de 2016

[51]gartner Institut, “Cybersecurity at the Speed of Digital Business” . Exsecutive Summary: The Advantages, Economics and value of reuse, disponivel em https://gartner.com/doc/1406319/executive-summary-advantages-economics-value, consultado em 13 de julho de 2016

[52] DAVIDSON, I., SOUKUP, T. (2002). *Visual Data Mining: Techniques and tools for data visualization and mining.* Danvers, USA: John Wiley & Sons, citado por Alves N., Investigação por Inquérito, Lic. Em Matemática Aplicada, Universidade dos Açores (2005/2006)

[53] GITMAN, L. J. Principles of managerial finance: brief 2 ed. Reading, Mass: Addison Wesley, 2000

[54] Ohtoshi P. Análise comparativa de metodologias de gestão e de Análise de riscos, Universidade de Brasilia, 2008

[55] SÊMOLA, Marcos. Gestão da Segurança de Informação - Uma Visão Executiva. Rio de Janeiro : Campus, 2003 disponivel em [54]

[56] Symantec, *Norton Cibersecurity insights Report, 2016 disponivel em http://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt*

Anexo I | Inquérito por Questionário

Este inquérito destina-se à auscultação junto das empresas/organizações e dos seus colaboradores relacionados com a segurança de informação no âmbito da dissertação do Mestrado em Engenharia Informática da ESTG/IPP (Escola Superior de Tecnologia e Gestão).

O presente inquérito é de natureza confidencial e anónima e destina-se a tratamento estatístico de forma a compreender a realidade informática da organização. O objetivo é contribuir para uma maior eficácia e segurança dos serviços.

Não há respostas certas ou erradas e pretende-se apenas a sua opinião pessoal e sincera.

O objetivo do trabalho foi discutido e aceite pela sua organização, pelo que a distribuição do presente inquérito, através do seu e-mail institucional, está autorizada superiormente.

De forma a podermos obter uma amostra representativa, solicita-se a todos os quantos foram selecionados para o estudo o preenchimento do presente inquérito com a maior brevidade possível.

Obrigado pela sua participação.

1) **Concelho?**

Amarante
Baião
Castelo de Paiva
Celorico de Basto
Cinfães
Felgueiras
Lousada
Marco de Canaveses
Paços de Ferreira
Penafiel
Resende

2) **Dimensão da Empresa /Organização (Colaboradores)?**

< 10

10 a 49

50 a 249

250 a 500

mais de 500

3) **Existe alguma pessoa ou departamento ligado às Tecnologias de Informação?**

Sim

Não (Passe para a pergunta 6).

NS/NR

Uma vez que respondeu afirmativamente indique:

4) **Quantas pessoas estão afetas ao departamento?**

5) **Têm formação base na área?**

Sim

Não

6) **Utiliza passwords/credenciais de acesso para se ligar ao seu posto de trabalho (PC)?**

Sim

Não

7) **Utiliza passwords/credenciais de acesso às aplicações que considera importantes para o seu trabalho?**

Sim

Não

8) **Com que frequência altera as suas passwords? (Assinale uma das opções)**

Não tenho por hábito alterar a password

Uma vez por ano

Semestralmente

Trimestralmente

Mensalmente

9) **Qual o tamanho típico da sua password?**

<= 5 caracteres

<= 8 caracteres

<= 12 caracteres

> 12 caracteres

10) **Assinale de acordo com o solicitado: (Sim ou Não)**

Inclui Informação Pessoal na sua password (ex.: Nome, data, etc)?

Inclui palavras conhecidas e/ou com sentido semântico?

Intercala letras, números e/ou símbolos na formulação da password?

De forma a facilitar o trabalho da organização, cederia a sua password de acesso a um colega?

Tem conhecimento de colegas que divulgam a password a outros colegas para facilitar o trabalho?

11) **Quantifique por tipo o número de caracteres que normalmente usa nas suas passwords? (de 1 a 10)**

Número de Letras minúsculas

Número de Letras maiúsculas

Quantidade de números

Quantidade de Símbolos

12) **Costuma usar dispositivos de armazenamento USB no seu PC?**

Sim

Não

13) **Bloqueia a sessão de trabalho do seu computador quando se ausenta?**

Não, nunca ninguém me disse para o fazer.

Não tenho por hábito faze-lo.

Bloqueio mas apenas em asências prolongadas.

Bloqueio frequentemente

Bloqueio sempre

14) **No contexto do seu ambiente de trabalho existe a possibilidade de instalar algum tipo de *software* que considere relevante para a realização das suas tarefas?**

Sim

Não

15) **Tem conhecimento da existência de um plano de boas práticas e normas de segurança informática na organização?**

Sim (*Passa para a pergunta 16*).

Não (*passa para a pergunta 17*)

16) **Uma vez que respondeu afirmativamente, indique: (de 1 a 5)**

(sendo 1 nada claro/indisponível e 5 perfeitamente claro/disponível)

Acessibilidade do plano

Disponibilidade e atualização do plano

Clareza das políticas de Segurança definidas no plano

Compreensão das responsabilidades atribuídas aos colaboradores/ departamentos relacionado com a negligência informática

17) **Classifique, assinalando na coluna correspondente, a dependência dos sistemas informáticos e da Internet para a atividade normal da Organização/instituição. (de 1 a 5)**

(*Sendo 1 nada dependente e 5 fortemente dependente*)

18) **Como classifica a sua apetência relativamente ao uso das tecnologias? (de 1 a 5)**

(*Sendo 1 fraca e 5 Avançada*)

19) **No contexto do seu ambiente de trabalho existe a possibilidade de instalar algum tipo de *software* que considere relevante para a realização das suas tarefas?**

Sim

Não

NS/NR

20) **Dos seguintes serviços assinale os que consulta no seu computador de trabalho?**

(Marcar tudo o que for aplicável.)

E-mail Institucional

E-Mail Pessoal

Redes sociais pessoal

Redes sociais relacionadas com a organização

Motores de pesquisa (Google, etc)

Fóruns de debates

Portais on-line (home banking, finanças, etc)

21) **Quando recebe um e-mail de um remetente desconhecido, que tipo de tratamento lhe dá?**

Abro e avalio o conteúdo

Só abro se o assunto for do meu interesse

Não abre

Descarto sem ler

Leio rapidamente e descarto

22) **Se ficasse sem Internet durante 4 horas, qual seria o impacto no rendimento e qualidade do seu trabalho**

Nenhum

Baixo impacto

O serviço ficaria atrasado

Teria de compensar com horas extraordinárias durante a semana

Teria de compensar com horas extraordinárias no próprio dia

23) **Na sua opinião considera que a instituição possui um programa de formação em segurança de informação (P.ex: Formação, avaliação de conhecimentos)**

Sim

Não

NS/NR

24) **Escolha a resposta que melhor define as suas funções na instituição**

Dirigente/membro do executivo (Passe para a pergunta 24)

Departamento de Informática (Passe para a pergunta 35)

Colaborador (Termina o Inquérito)

Questões dirigidas aos dirigentes/executivo

25) **As questões de segurança de informação são considerados nas decisões da organização?**

Sim

Não

NS/NR

26) **Quanto ao nível de apoio aos gestores, os sistemas de informação da organização suportam:**

As decisões operacionais

Decisões táticas

Decisões estratégicas

Todas as anteriores

Não suportam as decisões

27) **Numa escala de 1 a 5, considera que a sua organização dispõe de recursos com experiência e qualificações necessárias para as questões de segurança informática?**

(Sendo 1 baixa e 5 elevada)

28) **A sua organização alguma vez realizou uma avaliação de risco para identificar fragilidades e eventuais correções?**

Sim

Não

NS/NR

29) **Tem um custo atribuído à perda de cada ativo crítico ou função?**

Sim

Não

30) **Existe um plano para a continuidade de negócios em caso de desastre (dentro ou fora)?**

Sim

Não

NS/NR

31) **Como classifica o nível de alfabetização tecnológico dos seus utilizadores (de 1 a 5)**

(sendo 1 fraca e 5 Elevado)

32) **Existe uma pessoa ou organização que tenha a segurança de informação como seu principal dever?**

Sim: Interna

Sim. Externa

Não

33) **São realizadas auditorias de segurança de informação na instituição?**

Sim

Não

NS/NR

34) **É usual contemplar a inserção de cláusulas de segurança de informação em contratos com fornecedores?**

Sim

Não

NS/NR

Equipa de Informática

35) Assinale as opções que melhor caracterizam a forma de comunicação na sua organização:

Uso exclusivo de servidores internos

Aplicações na Cloud

Aplicações em servidores internos e cloud

Ligações via web pública a serviços/espaços desconcentrados

Ligação através de VPN a serviços/espaços desconcentrados

36) Identifique o número de computadores com acesso à rede?

37) Assinale as alíneas que melhor a definem a sua organização

Todos os colaboradores internos têm acesso a computador com ligação à Internet

A maioria dos colaboradores internos tem acesso a computadores e Internet

Os colaborados apenas usam a intranet, sendo pouco os que têm acesso à Internet.

Inexistência de restrições no acesso à Internet

O acesso à Internet é livre, mas com restrições de sites/conteúdos

38) As questões de segurança de informação são considerados nas decisões da organização?

Sim

Não

NS/NR

39) É comum usar cláusulas de salvaguarda das políticas de segurança nos contratos que dispõe com terceiros?

Sim

Não

NS/NR

40) São construídos relatórios com alertas de potenciais ameaças e exposição para os superiores?

Sim

Não

41) Numa escala de 1 a 5, como considera a existência de meios para gerir e garantir os processos relacionados com a segurança de informação?

(Sendo 1 nada adequado e 5 muito adequado)

42) Existe uma monitorização das suas redes, sistemas e aplicações para acesso não autorizado e comportamento anómalo, como vírus, códigos maliciosos inserção e/ou tentativas de intrusão?

Sim

Não

NS/NR

43) A estratégia de segurança de informação escrita incluem planos que visam reduzir os riscos a um nível aceitável, com interrupções mínimas para operações?

Sim

Não

NS/NR

44) Existe uma pessoa ou organização que tenha a segurança de informação como seu principal dever?

Sim: Interna

Sim: Externa

Não

45) Assinale quais os mecanismos de controlo/segurança dispõe na organização?

Antivírus

Firewalls

Lista de Controlo de acessos (log´s de acesso)

Varredura de Vulnerabilidades

Sistemas de Prevenção de Intrusão

Controlo de acesso à rede

Autenticação a vários níveis.

Outra

46) São realizadas auditorias de segurança de informação na instituição?

Sim

Não

NS/NR

47) Tem conhecimento de ser usual a instituição contemplar a inserção de cláusulas de segurança de informação em contratos com fornecedores?

Sim

Não

NS/NR

48) Existe ou conhece algum procedimento em vigor na instituição para atuação em caso de ser vítima de ataque?

Sim

Não

NS/NR

49) Para que tipo de incidentes entende que a instituição tem capacidade para detetar e responder em tempo útil?

Incidentes complexos

Incidentes simples

A instituição não tem capacidade para responder a incidentes

NS/NR

50) Nos últimos dois anos a instituição foi alvo de algum tipo de ataque informático?

Sim

Não

NS/NR

51) No seu entender, qual a probabilidade da instituição ser vítima de ataque no próximo ano?

(sendo 1 nada provável e 5 extremamente provável)

52) Classifique, do mais preocupante para o menos preocupante para a instituição, os seguintes temas? (1 - menos preocupante; 5 - mais preocupante)

(sendo 1 nada provável e 5 extremamente provável)

Ataques de hackers ou organizações criminosas

Cloud computing

Cumprimento com legislação e outras obrigações regulamentares

Desconhecimento das ameaças de Vulnerabilidades

Disseminação pública não autorizada de informação da instituição

Proteção de dados pessoais e dados pessoais sensíveis

Falta de capacidade de deteção de ataques

Anexo II | Declaração de autorização

AUTORIZAÇÃO

O Município de _____, com o NIPC , _____ representado por _____, na qualidade de _____ , declara autorizar o aluno Sérgio Manuel Barbosa Monteiro, sob orientação do Prof. Doutor João Paulo Magalhães, do mestrado em Engenharia Informática da ESTGF/IPP, a realizar as ações necessárias para o desenvolvimento do projeto de investigação tendo tomado conhecimento dos objetivos do estudo e cujos testes a realizar assentam nos processos, tecnologias e pessoas, nomeadamente na:

- Resposta a inquéritos.
- Engenharia Social – Teste aos procedimentos efectuados por parte das pessoas, cuja proveniência de identidade pode assumir o nome da instituição ou de terceiros/desconhecidos e em momento algum acarretará perigo ou prejuízo para a instituição, pretendendo apenas avaliar o comportamento das pessoas.

Fica ainda salvaguardado que todos os dados a serem recolhidos serão para uso exclusivo ao nível da investigação e que será mantido o anonimato.

Paços do Concelho, _____ de _____ de 2016

O Presidente da Câmara,

_____

Assinatura e carimbo

Anexo III | Macro auto-executável (eixo 2)

```
Private Sub Workbook_Open()
Dim iMsg, iConf, Flds
'Seta as variáveis, lembrando que o objeto Microsoft CDO deverá estar habilitado em
Ferramentas->Referências->Microsoft CDO for Windows 2000 Library
   Set iMsg = CreateObject("CDO.Message")
   Set iConf = CreateObject("CDO.Configuration")
   Set Flds = iConf.Fields

   'Configura o componente de envio de e-mail
   schema = "http://schemas.microsoft.com/cdo/configuration/"
   Flds.Item(schema & "sendusing") = 2
   'Configura o smtp
   Flds.Item(schema & "smtpserver") = "smtp-pt.xxxxxxxxx.xxx"
   'Configura a porta de envio de e-mail
   Flds.Item(schema & "smtpserverport") = 465
   Flds.Item(schema & "smtpauthenticate") = 1
   'Configura o e-mail do remetente
   Flds.Item(schema & "sendusername") = "geral@dlap-tamegasousa.pt"
   'Configura a senha do e-mail remetente
   Flds.Item(schema & "sendpassword") = "XXXXXXXXX"
   Flds.Item(schema & "smtpusessl") = 1
   Flds.Update

   With iMsg
      'E-mail do destinatário
      .To = "xxxxxxxxxxx@gmail.com"
      'Seu e-mail
      .From = "seuemail@gmail.com"
      'Título do e-mail
      .Subject = "Ficheiro aberto por"
      'Mensagem do e-mail, você pode enviar formatado em HTML
      .HTMLBody = "Mensagem enviada com o gmail."
      'Seu nome ou apelido
      .Sender = "Teste"
      'Nome da sua organização
      .Organization = "Empresa Teste"
      'e-mail de responder para
      .ReplyTo = "xxxxxxxx@gmail.com"
      'Anexo a ser enviado na mensagem
      '.AddAttachment ("c:\fatura.txt")
      'Passa a configuração para o objeto CDO
      Set .Configuration = iConf
      'Envia o e-mail
      .Send
   End With

   'Limpa as variáveis
   Set iMsg = Nothing
   Set iConf = Nothing
   Set Flds = Nothing
End Sub
```