Universidade de Évora

Escola de Ciências Sociais

Mestrado em Gestão

Área de Especialização – Organização e Sistemas de Informação

Dissertação

O comportamento dos utilizadores na segurança dos Sistemas de Informação nas Organizações: um risco ou uma protecção?

Por:

Alexandre Manuel Santareno Pimenta

Orientação:

Prof. Doutor Rui Filipe Cerqueira Quaresma

Évora, Janeiro de 2012

Mestrado em Gestão

Área de Especialização – Organização e Sistemas de Informação

Dissertação

O comportamento dos utilizadores na segurança dos Sistemas de Informação nas Organizações: um risco ou uma protecção?

Por:

Alexandre Manuel Santareno Pimenta

Orientação:

Prof. Doutor Rui Filipe Cerqueira Quaresma

Agradecimentos

A elaboração de um trabalho desta dimensão, não envolve apenas o seu autor, mas uma panóplia de pessoas, que sem o seu precioso contributo seria impossível de realizar.

Agraço especialmente ao meu orientador Prof. Doutor Rui Quaresma a disponibilidade demonstrada e empenho com que acolheu este trabalho bem como toda a sua orientação científica, agradeço ainda todas as preciosas opiniões e sugestões que me permitiram uma melhor execução do trabalho.

À Direcção da Escola Superior de Gestão e Tecnologia de Santarém, a possibilidade que me foi concedida em poder realizar este trabalho.

O apoio prestado pelo Prof. Cláudio Barradas, pela Prof. Emília Pereira e pela Dr.ª Arnaldina Baeta.

Um especial agradecimento a todos aqueles que amavelmente participaram e preencheram o questionário *on-line* que assim possibilitou a realização deste estudo.

À minha família pelo apoio e estímulo dados em todos os momentos da realização deste trabalho.

Finalmente agradeço às minhas filhas Leonor e Matilde pela sua compreensão em relação ao tempo que não lhes dediquei.

A todos o meu muito obrigado.

O comportamento dos utilizadores na segurança dos Sistemas de Informação nas Organizações: um risco ou uma protecção?

Resumo

Numa sociedade cada vez mais global e em constante mutação, onde as organizações necessitam de ter sempre disponível a informação necessária e útil para desenvolver, de uma forma rápida e eficaz, as suas actividades no dia-a-dia, garantir a segurança da informação é um factor do qual depende a sua continuidade e sucesso. O presente trabalho tem como objectivo saber em que medida os comportamentos e as atitudes dos utilizadores constituem um risco ou uma protecção para a segurança dos Sistemas de Informação nas organizações. Para alcançar este objectivo será efectuada uma revisão bibliográfica baseada em fontes secundárias. Numa segunda fase será elaborado um questionário com base nos procedimentos de segurança identificados na revisão da literatura a aplicar aos utilizadores de Sistemas de Informação e Tecnologias de Informação, e posteriormente analisados os resultados e retiradas as conclusões.

A principal conclusão deste estudo revela que os utilizadores, de forma geral, são uma protecção para a segurança dos Sistemas de Informação nas organizações. Existem, no entanto, alguns procedimentos que necessitam de ser melhorados pelos utilizadores, para evitar que o seu comportamento seja considerado de risco

Palavras-chave: Sistemas de Informação, Tecnologias de Informação e Comunicação, Segurança da Informação.

Users' behaviour in Information Systems security in the Organizations: a risk or a protection?

Abstract

In an ever changing and more and more globalized society, in which the organizations need to always have the necessary and useful information available in order to develop, in a fast and accurate way, their daily activities, to ensure the safety of information is a factor on which their continuity and success depend. The goal of the present work is to know to which extent the users' behaviours and attitudes are a risk or a protection for the Information systems' security inside the organizations. In order to reach this goal, a bibliographic revision based on secondary sources will be done. Secondly, a questionnaire will be elaborated based on the safety procedures identified in the literature revision and applied to the Information Systems' users. The results and the conclusions will then be analysed and thought over.

The results of this study show that, in general, users are a protection for the security of the Information Systems inside the organizations. However, there are some procedures that the users have to improve, to avoid what may be considered a risky behaviour.

Keywords: Information Systems, Information and Communication Technologies, Information Security.

Índice

Índice de Figuras

Índice de Tabelas

Lista de Siglas

BS - *British Standard*;

CAE- Rev.3 - Classificação Portuguesa de Actividades Económicas – Revisão 3;

CNPD - Comissão Nacional de Protecção de Dados;

INE – Instituto Nacional de Estatítica;

ISO - *International Organization for Standardization;*

PIN - *Personal Identification Number;*

RFID - *Radio-Frequency IDentification;*

SGSI - Sistema de Gestão da Segurança da Informação;

SI - Sistemas de Informação;

SI/TI - Sistemas de Informação e Tecnologias de Informação;

SPSS - *Statistical Package for the Social Sciences*;

TI - Tecnologias de Informação;

TIC - Tecnologias de Informação e Comunicação;

1. Introdução

Neste capítulo é efectuada uma abordagem preliminar sobre a importância do tema do trabalho e efectuado um enquadramento do mesmo, são definidos os objectivos da investigação e descrita a metodologia para concretizar os mesmos. É apresentada ainda uma descrição sumária da estrutura dos capítulos do trabalho.

1.1 Enquadramento

Num mundo cada vez mais competitivo, onde a informação é vital para todas as organizações, principalmente para a sua subsistência, estas procuram ter sempre disponível a informação de forma rápida e íntegra. Para que isto seja possível, as organizações têm que possuir sistemas de informação e tecnologias de informação (SI/TI) capazes de dar resposta às suas exigências e necessidades. Para que os sistemas de informação (SI) estejam sempre disponíveis e garantam a integridade da informação que recolhem, processam, armazenam e distribuem, há um factor muito importante a ter em consideração, para além da tecnologia propriamente dita e de todos os mecanismos de segurança que se venham a adoptar, que são os utilizadores dos SI/TI. Se estes não tiverem em atenção um conjunto de práticas e regras na utilização dos SI/TI, a informação pode não ser a mais correcta, correndo o risco de se gerar informação incoerente, desfasada da realidade e, consequentemente, levar a tomadas de decisão incorrectas.

Segundo Serrano e Fialho (2005) as tecnologias de informação (TI), a partir do século XX, começaram a exercer uma enorme influência sobre as organizações, alterando nestas as formas de produção, gestão, comercialização e práticas sociais de comunicação. A partir do momento em que uma organização dá os primeiros passos para converter “dados” em “informação”, os seus processos de decisão, a sua estrutura e a sua forma de trabalhar transformam-se.

De acordo com Serrano et al. (2004), o SI organizacional fornece informações sobre a organização e o seu ambiente, não só para os elementos da organização, como também para os elementos do meio envolvente (estado, clientes, fornecedores, etc). O SI da organização deve possibilitar aos responsáveis pela decisão, a informação necessária para as decisões programadas, auxiliando na tomada de decisões não programadas e assegurando também a comunicação entre os elementos da organização.

Para Varajão (1998), a compreensão do papel dos SI nas organizações implica a distinção de dois conceitos relacionados, mas distintos: dados e informação. Dados são factos isolados, ou valores discretos que isoladamente não têm qualquer utilidade e cuja simples posse não assegura a obtenção

de quaisquer benefícios. Informação é tudo aquilo que reduz a incerteza sobre um determinado facto. Face ao descrito, as organizações têm que estar cientes da importância da informação e dos seus SI, pelo que garantir a sua segurança é uma questão fundamental.

Segundo Silva et al. (2003), a segurança, a privacidade e a integridade são conceitos inter-relacionados com que se confronta no dia-a-dia quem manipula informação pessoal, social ou organizacional, particularmente pelas ameaças a que a informação e os SI que a suportam se encontram sujeitos. Emerge assim a necessidade de obter um entendimento concreto dos aspectos adequados para garantir que a informação, independentemente de como e onde vai ser utilizada, a quem pertence ou quem a pode utilizar, apenas é aplicada na prossecução dos objectivos que presidiram à sua criação.

As pessoas utilizam a informação a que têm acesso porque possuem a percepção de que essa utilização lhes permitirá um melhor desempenho. A informação tornou-se então o factor crítico de sucesso, exigindo por isso uma protecção adequada, principalmente no contexto actual de turbulência do meio organizacional e social.

Serrano e Jardim (2007) referem que com a crescente utilização e difusão das TI, o recurso informação apresenta-se estratégico para a organização, potenciando o desenvolvimento ou a alteração das suas actividades operacionais. A capacidade de penetração das novas TI em todos os âmbitos da actividade humana, provoca alterações e mudanças a nível económico, social e organizacional. As organizações têm que acompanhar estas mudanças de modo a direccionarem o seu desenvolvimento e o seu destino. A sociedade em que vivemos apresenta-se muito dinâmica, instável, desafiadora e evolutiva, pelo que as organizações têm que encontrar nos SI a informação relevante para as suas tomadas de decisão. As organizações enfrentam ameaças reais que podem a qualquer momento provocar um incidente com origem em fontes distintas, pelo que qualquer perda na sua capacidade de processamento pode ter consequências devastadoras, dependendo do tempo de inoperacionalidade que se verifique. A informação denomina-se como um activo económico para as organizações, visto tratar-se de uma das matérias-primas mais desejada. Os dados recolhidos pela organização, associado ao significado que lhes é atribuído, representam informação especializada para as organizações. Nas organizações, a informação é utilizada para processar registos, planear, monitorizar as actividades, para controlar e comunicar. A informação é um recurso estratégico, pelo que as organizações devem efectuar uma gestão eficiente desta com o objectivo de incrementar as capacidades de aprendizagem bem como a sua adaptação às mudanças no meio ambiente. Independentemente do nível hierárquico na organização, a informação, face à sua natureza e

importância para apoio à tomada de decisão, é um recurso importante, pelo que é pertinente garantir a sua protecção de modo a permitir a continuidade do negócio em qualquer circunstância. Implementar e manter um eficaz sistema de controlo interno nas organizações passou a ser um factor fundamental para o sucesso, para identificar, gerir os riscos e adequar os procedimentos internos. Não basta às organizações aplicarem meios de segurança técnica, é necessário também implementar normas e controlos internos, que são identificados através da sistemática avaliação dos riscos de segurança.

Serrano e Fialho (2005) referem que dentro das organizações a área das tecnologias de informação tem como desafio identificar, encontrar, desenvolver e implementar SI/TI que permitam a partilha, a comunicação e a troca de informação entre os utilizadores, de modo a que estes trabalhem de forma integrada e em rede e promovam o conhecimento colectivo. As TI fornecem o acesso a diversas fontes de informação, o que permite melhorar a capacidade para analisar, gerir, aplicar e distribuir a informação dentro da estrutura da organização, conduzindo-a a estar mais informada, flexível e orgânica.

Segundo Kruger e Kearney (2008), não basta apenas ter soluções tecnológicas para eliminar as vulnerabilidades e ameaças, é necessário ter em consideração as acções dos utilizadores na segurança da informação. Os utilizadores devem ser sensibilizados para as questões de segurança, nomeadamente para os efeitos negativos que uma falha ou quebra de segurança podem provocar. As acções de sensibilização procuram verificar se os utilizadores estão cientes das ameaças à segurança, das suas responsabilidades e obrigações, e se aplicam as políticas de segurança da organização no desenvolvimento das suas actividades diárias.

De acordo com Furnell e Thomson (2009), um dos grandes problemas e ameaças verificados na implementação de práticas e procedimentos na segurança da informação são os utilizadores. Por este facto, torna-se necessário promover dentro da organização uma cultura de segurança e assegurar que as boas práticas são uma componente natural do comportamento dos utilizadores.

Albrechtsen (2007) refere que as medidas de segurança da informação revelam-se ineficientes pelo facto de os utilizadores não estarem informados de quais os comportamentos seguros a adoptar e qual o contributo da adopção desses comportamentos.

1.2 Objectivos

As organizações dispõem de SI que precisam de estar sempre disponíveis para a análise e tomada de decisão por parte dos gestores, tratamento de informação por parte dos serviços administrativos e

consulta de informação por parte dos clientes e fornecedores. São os utilizadores os elementos dentro da organização que operam e manuseiam a maior parte da informação nos SI, pelo que têm uma quota-parte de responsabilidade na integridade e fidedignidade da informação gerada. Os utilizadores são, portanto, um dos elementos que pode provocar vulnerabilidades e eventuais danos nos SI, pelo que é pertinente verificar se estão sensibilizados para a utilização de práticas correctas e seguras no desempenho das suas tarefas.

Face ao exposto anteriormente, o objectivo geral deste trabalho é saber em que medida os comportamentos e as atitudes dos utilizadores constituem um risco ou uma protecção para a segurança dos SI nas organizações.

Objectivos Específicos

1. Identificar e descrever, com base na literatura, os procedimentos de segurança que os utilizadores das Tecnologias de Informação e Comunicação (TIC) devem adoptar para garantir a segurança dos SI;
2. Construir e aplicar um questionário sobre a segurança dos SI junto de utilizadores das organizações que utilizam as TIC;
3. Analisar os resultados obtidos através do questionário, para verificar se o comportamento e as atitudes dos utilizadores constituem um risco ou uma protecção para a segurança dos SI nas organizações;
4. Apresentar um conjunto de recomendações que os utilizadores de TIC nas organizações podem adoptar para melhorar a segurança dos SI.

1.3 Metodologia

Para concretizar o objectivo do trabalho, será efectuada, em primeiro lugar uma pesquisa bibliográfica exploratória com base em fontes secundárias (artigos científicos, livros, teses, etc.). Em seguida, é realizada a revisão da literatura, onde vão ser explanados os tópicos relacionados com a segurança da informação, normalização existente e legislação aplicável. A revisão da literatura vai permitir identificar os procedimentos que os utilizadores devem adoptar para garantir a segurança dos SI dentro das organizações. Para saber em que medida os comportamentos e as atitudes dos utilizadores constituem um risco ou uma protecção para a segurança dos SI nas organizações, será efectuada uma recolha de dados primária. O instrumento utilizado na recolha de dados será o questionário, e terá como população alvo os utilizadores dos SI/TI nas organizações. O questionário conterá um conjunto de questões de tipo fechado, suficientemente abrangentes sobre os

procedimentos de segurança nos SI, identificados na revisão da literatura. A recolha dos dados será efectuada com um questionário *on-line*, através de um sítio *Web* criado especificamente para esse fim, tendo uma base de dados associada que vai permitir o armazenamento das respostas. Para realizar e aplicar o questionário, será utilizada uma amostra não probabilística por conveniência. Será enviada uma mensagem de correio electrónico aos utilizadores das TIC nas organizações a apelar à participação e divulgação do questionário. Depois de terminar a recolha dos dados, estes serão quantificados através de escalas não comparativas para permitir a sua análise e apurar os resultados com recurso à aplicação informática SPSS.

A análise aos resultados obtidos no questionário vai permitir verificar se o comportamento e as atitudes dos utilizadores constituem um risco ou uma protecção para a segurança dos SI nas organizações.

1.4 Estrutura e organização do trabalho

Para que exista uma melhor percepção do trabalho, o mesmo foi desenvolvido não de forma desordenada, mas segundo uma estrutura lógica e divida em capítulos.

Capítulo 1 - Introdução: neste capítulo é efectuado um enquadramento do tema do trabalho, identificado o problema de investigação e a relevância do mesmo, identificados os objectivos do trabalho e efectuada a descrição da estrutura da dissertação.

Capítulo 2 - Enquadramento teórico: neste capítulo são elencados e descritos os conceitos de organização, tecnologias de informação e comunicação, de informação, de segurança da informação bem como a descrição dos principais perigos a que está sujeita, e no fim do capítulo é feita a referência aos utilizadores e aos principais incidentes que estes podem provocar na segurança da informação.

Capítulo 3 - Políticas e procedimentos de segurança: neste capítulo é apresentado o conceito de políticas de segurança bem como o seu processo de criação e implementação na organização, são também identificados um conjunto de procedimentos de segurança que os utilizadores devem adoptar para que seja garantida a segurança da informação. É efectuada também uma referência às principais Leis existentes a nível nacional relacionadas com a segurança da informação, e por último identificadas as principais normas internacionais relacionadas também com a segurança da informação.

Capítulo 4 - Metodologia: neste capítulo é descrito todo o desenho da investigação que permite atingir os objectivos do trabalho, desde a escolha da população e amostra, aos dados que inclui o

instrumento escolhido para a recolha de dados, o pré-teste efectuado, o processo de recolha dos dados e por fim como é efectuado o tratamento e análise dos dados.

Capítulo 5 – Resultados e discussão: neste capítulo são apresentados os resultados obtidos através do tratamento estatístico dos dados recolhidos na investigação e retiradas as ilações com base nos procedimentos identificados na revisão da literatura.

Capítulo 6 – Considerações finais: neste capítulo são apresentadas as conclusões desta investigação, analisadas as suas implicações e limitações e sugestões para investigações futuras.

2. Enquadramento Teórico

No capítulo dois é efectuada uma revisão da literatura, onde são apresentados os conceitos chave para o desenvolvimento da investigação. Na primeira parte deste capítulo é efectuada a definição e realçada a importância na organização, dos sistemas de informação, das tecnologias de informação e comunicação e da informação. A segunda parte do capítulo retrata a importância da segurança da informação e identifica as principais ameaças, vulnerabilidades, ataques e riscos a que a mesma está sujeita. O último ponto de capítulo descreve o papel e a problemática dos utilizadores na segurança dos SI nas organizações.

2.1 A Organização, os Sistemas de Informação, as Tecnologias de Informação e Comunicação e a Informação

2.1.1 A Organização

Devido às constantes mudanças que ocorrem no seu meio ambiente, como a globalização dos mercados e a evolução das TI, as organizações deparam-se com novas realidades e formas de realizar o seu negócio, pelo que, de acordo com Serrano e Jardim (2007), têm necessidade de adaptar a sua estrutura, organização, planificação, tomada de decisão e SI capazes de dar resposta aos novos desafios e aumento da competitividade. As organizações debatem-se num ambiente de negócio que se caracteriza:

- Pela globalização dos mercados cada vez mais competitivos e internacionalizados com a crescente abolição de barreiras económicas e sociais;
- Pela constante mudança, turbulência e instabilidade, o que "obriga" as organizações a possuírem uma grande flexibilidade e capacidade de adaptação às novas situações, além de rapidez nas respostas;
- Pelo facto de o cliente ser o ponto central no processo de negócio da organização.

Neste contexto, Serrano et al. (2004) consideram a organização como um sistema aberto em permanente evolução e adaptação às alterações do meio ambiente, sendo constituída por um conjunto de elementos humanos, materiais e abstractos, que actuam e relacionam-se de uma forma dinâmica entre si e com o meio ambiente, na prossecução da sua missão e objectivos.

Segundo Mukherji (2002), a necessidade das organizações se adaptarem ao seu meio envolvente é uma questão estratégica que tem repercussões na sua sobrevivência, crescimento e aumento da performance. As organizações proactivas utilizam uma estrutura descentralizada e estratégias

diferentes de acordo com o surgimento de novas TI, enquanto as reactivas usam uma estrutura centralizada. Os factores como o meio envolvente, a gestão e o desempenho dos trabalhadores afectam a forma e a estrutura de funcionamento da organização, facilitando a comunicação dentro da organização através da utilização dos SI, não apenas a nível interno, mas também a nível externo com clientes, fornecedores e parceiros. Para que esta estrutura organizacional funcione correctamente, as organizações têm que se equipar com SI/TI e redes de comunicação capazes de responder de forma rápida e eficaz às suas necessidades de informação.

Para Serrano et al. (2004), as organizações recorrem aos SI/TI para suportar as suas actividades, visto estes permitirem um aumento significativo da produtividade, uma vez que armazenam, tratam e transmitem a informação em tempo real permitindo uma melhoria nas tomadas de decisão.

2.1.2 Os Sistemas de Informação

Rodrigues (2002) define um SI como um conjunto de procedimentos, actividades, pessoas e tecnologias envolvidos na recolha de dados relevantes, armazenamento enquanto necessário, processamento dos dados e na disponibilização de informação a quem necessite da mesma.

Para Serrano et al. (2004), o SI de uma organização tem objectivos definidos, fornecendo informações sobre a organização e o seu ambiente, não só para os seus elementos, mas também para os do meio envolvente (clientes, fornecedores, fisco). Na organização, os SI devem proporcionar aos decisores informações necessárias para as tomadas de decisão programadas e auxiliar nas não programadas e assegurar a comunicação entre todos os elementos da organização.

Segundo Laudon e Laudon (2007), existem três funcionalidades que caracterizam um SI, as entradas, o processamento e as saídas. Os dados recolhidos no interior e exterior da organização correspondem às entradas. Após a recolha, os dados são processados de modo a terem um significado e serem úteis para a organização. Os dados, após o processamento são informação que é canalizada para as actividades ou pessoas que dela necessitem. A funcionalidade de feedback tem como função controlar se a informação produzida está de acordo com o pretendido pela organização, se não estiver coloca-a de novo no processo de entrada para ser processada, como demonstrado na figura 1.

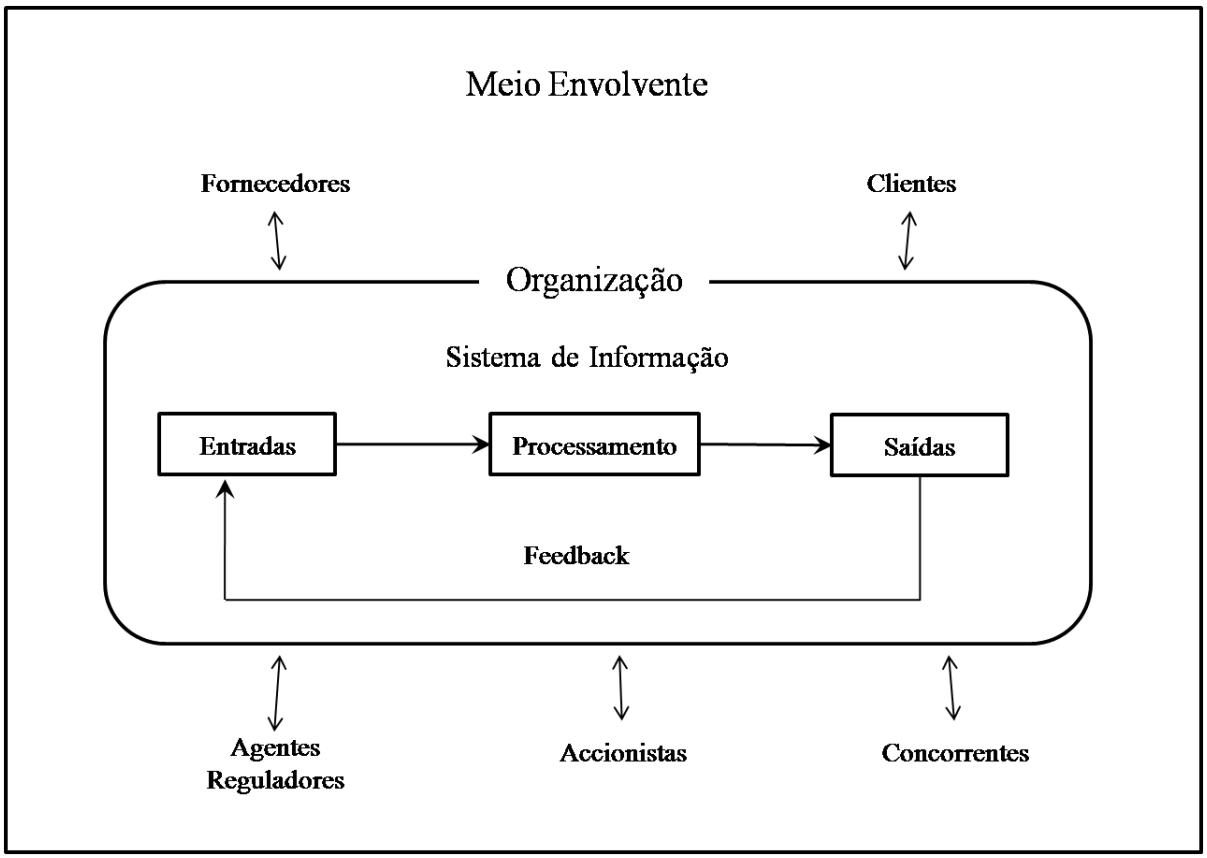

Figura 1 - Actividades de um SI (adaptado de Laudon e Laudon, 2007)

De acordo com Mukherji (2002), os SI permitiram às organizações adoptarem uma estrutura descentralizada ao invés da centralizada, uma vez que permitem uma maior fluidez das comunicações, controlo e distribuição da informação. Deste modo, deixa de existir uma unidade central de controlo, cada unidade desenvolve as suas actividades, tem os seus recursos e as suas responsabilidades, ficando a parte de troca de dados e comunicações da responsabilidade dos SI, o que se traduz num aumento da qualidade, fiabilidade, quantidade e capacidade de processar a informação.

Laudon e Laudon (2007) referem que os SI para serem eficazes devem promover o aumento da produtividade dos trabalhadores e da capacidade produtiva das organizações.

Segundo Choo (2003), os SI têm que facilitar, simplificar e estruturar a informação para o utilizador final, dar-lhe um significado, para que seja possível às organizações saber o que está a mudar quer no seu ambiente interno quer no externo, nomeadamente o que os outros estão a fazer e qual o seu comportamento.

Para Laudon e Laudon (2007), o valor de um SI para uma organização, bem como a decisão de investimento em SI, está condicionada pela expectativa nos benefícios que estes introduzirão na

organização em termos da flexibilidade, da eficiência, dos ganhos, dos proveitos e melhoria da tomada de decisão.

Dhillon (2005) refere que a implementação de um SI na organização não cria por si só benefícios nem resolve todos os problemas, é necessário ter em atenção também a formação dos utilizadores, a alteração de rotinas, regras e responsabilidades. O processo de implementação de SI/TI na organização para ser eficiente tem que provocar mudanças não apenas tecnológicas, mas também de gestão, na estrutura da organização e na sua cultura, contribuindo deste modo para o aumento dos seus factores de sucesso e para a concretização dos objectivos de negócio.

2.1.3 As Tecnologias de Informação e Comunicação

No contexto deste trabalho, e especialmente neste ponto, os termos TI e TIC representam a mesma realidade.

Para garantirem a sua eficácia e competitividade, as organizações têm que acompanhar as constantes evoluções das TIC. De acordo com Zorrinho et al. (2007), as TIC permitem às organizações:

- Generalização do acesso às redes de informação;
- Troca de todo o tipo de informação em tempo real;
- Possibilidade de trabalho colectivo mesmo estando em localizações diferentes;
- Partilha de informação armazenada em bases de dados;
- Facilidade de selecção e memorização de informação.

Esta visão consagra a importância que as TIC representam para as organizações, pelo que é importante proceder à sua definição.

Segundo Serrano et al. (2004), as TI são um conjunto de processos de *software* e *hardware* necessários para a realização de actividades de recolha, processamento, armazenamento e emissão de informação.

Já Laudon e Laudon (2007), definem as TIC como um conjunto de *hardware* e *software* que as organizações necessitam de adoptar de forma a alcançar os seus objectivos.

A capacidade das organizações em se adaptarem às novas TIC define o seu destino e projecta-as para a transformação e mudança dos seus processos de fabrico, de gestão e comercialização. As TIC

potenciaram uma nova revolução nas organizações, com um incremento da capacidade de utilização e processamento da informação, como referem Zorrinho et al. (2007).

De acordo com Serrano et al. (2004), sem as TIC não era possível a inovação, a flexibilização e a globalização dos mercados, uma vez ser necessário para que estes factos ocorram obter e processar grandes quantidades de informação. Só com a adopção de novas tecnologias e uma gestão adequada da informação, é que as organizações conseguem obter vantagens que lhes permitem a sua continuidade e sobrevivência. A introdução das TIC está a originar profundas alterações na vida das pessoas, da sociedade, da economia e nas organizações, nomeadamente com a introdução de novos processos de produção, comercialização e gestão.

Ainda de acordo com Serrano et al. (2004), as TIC proporcionam às organizações uma melhor gestão, distribuição e aplicação da informação, isto porque todos os elementos dentro da organização com acesso às novas tecnologias manipulam e potenciam a geração de informação, que depois é difundida por toda a estrutura organizacional.

Dhillon (2008) refere que as TI, conjugadas com os recursos e competências das organizações, têm o potencial de reduzir custos, criar a diferenciação e proporcionar o ganho de vantagens competitivas em relação aos concorrentes, se fomentarem algum tipo de mudança inovadora na estrutura da indústria onde se inserem, permitindo obter e colocar em prática novos tipos de informação e conhecimento. Como resultado, a organização consegue obter vantagens competitivas duradouras.

2.1.4 A Informação

Segundo Rodrigues (2002), a informação é entendida como um conjunto de dados que quando fornecidos de forma e a tempo adequado melhora o conhecimento de quem a recebe. Os dados são factos isolados, representações não estruturadas cuja utilização e interpretação resultará em informação.

Para Varajão (1998), a informação pode ser entendida como um conjunto de dados que quando colocados num contexto útil e de grande significado têm um valor real e percebido nas acções ou decisões de quem os utiliza.

De acordo com Serrano e Fialho (2005), os dados referem-se a um conjunto de factos discretos e objectivos sobre acontecimentos. Depois de lhe atribuir um significado e um sentido segundo a percepção de cada um, é que os dados passam a informação que permite tirar ilações sobre um determinado facto ou situação.

Para Serrano e Jardim (2007), as organizações que desenvolvem as suas actividades com base na informação recolhida, procuram uma melhor distribuição e aplicação desta com o intuito de explorar os conhecimentos existentes na organização e no seu meio ambiente, enquanto nas organizações tradicionais a incidência reside no processo de armazenamento da informação e na optimização da gestão da informação operacional, criada pelo funcionamento diário da organização.

Gaivéo (2008) refere que o importante é que a informação seja integrada nos diversos sectores da organização, independentemente da sua origem. No entanto, há a necessidade de garantir que esta se apresenta de forma precisa, consistente e útil para os que a vão utilizar.

Segundo Rodrigues (2002), para que a organização não caia no excesso de busca de informação que depois terá pouca utilidade, é necessário efectuar uma gestão da informação de forma efectiva e eficiente, permitindo o acesso a esta atempadamente. A destruição da que não tem qualquer valor, e a identificação e retenção num formato acessível da relevante e necessária, vai permitir à organização utilizá-la como arma estratégica na obtenção de vantagens competitivas.

Choo (2003) refere que as necessidades de informação emergem de problemas, incertezas e ambiguidades que ocorrem no seio das organizações e que estão relacionadas com: os objectivos que se pretendem atingir, o grau de risco, as normas profissionais, os constrangimentos e os estilos organizacionais. A aquisição de informação é realizada de acordo com regras definidas ou convencionadas junto de fontes previamente definidas. A informação é organizada e armazenada de acordo com uma estrutura definida de forma a facilitar a sua partilha e posterior consulta.

2.2 Segurança da Informação

A proliferação de redes de computadores permite transmitir, processar e armazenar grandes quantidades de informação. Esta mudança na forma de comunicar e realizar as tarefas veio também trazer novas preocupações, nomeadamente ao nível da segurança e integridade da informação, que é essencial para a actividade das organizações. Proteger e salvaguardar a informação tornou-se mais difícil do que resolver determinados problemas técnicos, como por exemplo falhas nos SI, tanto a nível de *software* como de *hardware*, que possam surgir. Para melhorar a segurança da informação, as organizações têm que ajustar a sua estrutura, visto existir uma enorme quantidade de partilha de informação e interligação com diversos elementos exteriores à organização, para evitar o uso inadvertido e abusivo da sua rede por parte de utilizadores internos, ou em casos extremos, de intrusão de elementos externos.

Devido à multiplicidade e diversidade de SI/TI que as organizações necessitam para realizarem as suas operações, existe um ambiente com enormes fragilidades, com vulnerabilidades a vírus, roubo de dados, intercepção de comunicações e intrusões nos SI. Estas situações podem ser desencadeadas a partir do interior ou do exterior das organizações. Um dos principais problemas apontados à segurança prende-se com o facto de as organizações não acompanharem a evolução tecnológica no que respeita a tomar atitudes pró-activas e melhorar a sua postura em relação às questões de segurança, como refere Mamede (2006).

Para Dlamini et al. (2009), a segurança da informação não é olhar para os ataques que aconteceram no passado, não é olhar para o presente com receio de ser atacado e não é olhar para o futuro com a incerteza sobre os ataques que poderão acontecer. A segurança da informação exige que a organização esteja sempre alerta e a sua necessidade surgiu desde que a informação começou a ser transmitida, armazenada e processada.

Segundo Dhillon (2004), embora as organizações invistam em sistemas de segurança da informação, as agressões e violações à informação têm vindo a aumentar. Não se tem revelado suficiente as organizações investirem quantias avultadas em mecanismos de protecção física, uma vez que as violações continuam a acontecer. A pergunta impõe-se: o que é necessário para fazer face a tal situação?

De acordo com Dhillon (2000), face à competitividade e constantes mudanças que imperam no mercado empresarial, as organizações vêem-se na necessidade de investir em SI sem que exista um planeamento e um cuidado com a segurança destes. Quando se fala em segurança da informação, normalmente as pessoas associam-na às TI, esquecendo um dos elementos mais sensíveis e provocadores de danos, os utilizadores dos SI/TI.

Para Ng et al. (2009), uma violação na segurança dos SI é definida como um acontecimento adverso relativo à sua segurança, onde existe a perda de confidencialidade da informação, perda da integridade e distorção da informação, indisponibilidade do sistema e a violação das regras de segurança dos SI.

Neste contexto, Mamede (2006) define segurança como a existência de capacidade para se tomarem medidas preventivas que, mesmo que não sejam suficientes para impedir as ocorrências indesejadas, maliciosas ou inesperadas, pelo menos as prevejam e tentem minimizar o seu impacto. Isto implica a identificação dos elementos mais vulneráveis do sistema e o desenho de soluções adequadas que tenham em consideração os riscos e os custos associados à protecção dos dados da organização.

Já a ISO (2009) define segurança como a tentativa de minimizar a vulnerabilidade de valores e recursos, sendo a vulnerabilidade qualquer ocorrência em que terceiros penetram num SI informatizado sem autorização, com o objectivo de obter proveitos do seu conteúdo ou das suas características.

De acordo com o exposto acima, e segundo Dhillon (2004), a definição de segurança da informação abarca:

- Confidencialidade - procurar garantir que o acesso à informação é feito apenas por aqueles que têm autorização;
- Integridade - manter o significado original da informação que foi manipulada e armazenada;
- Responsabilidade - regras que devem ser conhecidas por todos os colaboradores de uma organização, para que estes possam desenvolver as suas actividades com base nas suas responsabilidades;
- Honestidade das pessoas - revela-se uma componente importante para as organizações, visto que são estas que manipulam o bem mais precioso, a informação, pelo que deve-se tomar especial atenção a qualquer mudança de atitude ou comportamento por parte destes, de modo a evitar qualquer tipo de fraude;
- Confiança - tem que ser mútua entre a organização e os colaboradores, de acordo com as normas, regras e padrões de comportamento aceites, e funcionar como um elemento de coesão por toda a organização;
- Ética - está ligada às práticas que cada um tem, não existindo regras que possam ser aplicadas neste campo, simplesmente tem a ver com a percepção que cada um tem sobre a prática de determinado acto, se é correcto ou não.

Ainda de acordo Dhillon (2004), têm que se considerar também aspectos relacionados com o controlo de acesso aos equipamentos informáticos, as ligações seguras e a necessidade de estabelecer programas de formação para os colaboradores sobre segurança da informação e comportamentos de risco a evitar. A organização tem que desenvolver e implementar políticas de segurança da informação. Normalmente estas são aplicadas apenas depois de se ter sofrido um ataque, o que é uma atitude passiva e reactiva não desejada. Existe um conjunto de regras e padrões, como por exemplo o ISO 17799[1] (Dhillon, 2004), que podem ser adoptados pelas organizações. No

[1] ISO/IEC 17799:2005 - *Code of Practice for Information Security Management*

entanto, cada caso é um caso, pelo que as organizações devem construir políticas de acordo com a sua realidade, e não reger-se por políticas generalizadas que apenas são guias de orientação para ajustarem à sua realidade. Por último, compreender o comportamento e os aspectos sociais da organização. A segurança da informação passa também pela forma como as pessoas comunicam umas com as outras, pelo que estas devem ser educadas no sentido de terem uma responsabilidade social em relação à informação que levam para fora da organização

Mamede (2006) refere ainda os seguintes elementos a considerar na definição de segurança da informação:

- Registo – recolher e armazenar informações sobre a utilização dos SI, garantindo a existência de dados para a realização de auditorias e identificação dos responsáveis em caso de incidentes;
- Fiabilidade – procurar garantir que os dados que são introduzidos não são alterados pelo SI devido a falhas ou faltas, e que se mantém sempre íntegros enquanto o SI os armazenar;
- Segurança – procurar garantir que os dados que são introduzidos não são alterados pelo SI, nomeadamente ao nível do impacto que as falhas ou faltas provocam no seu ambiente. Procura dar confiança ao utilizador na utilização do SI.

Ainda segundo Mamede (2006), o processo de segurança numa organização não é um processo com princípio, meio e fim, mas sim um processo contínuo ao longo do tempo sem espaço para tréguas, sob pena de se ficar sujeito a vulnerabilidades. A segurança tem como objectivo proteger bens, que têm que ser identificados e ser conhecido o seu valor. Esta identificação permite-nos tomar as seguintes acções:

- Prevenção – procura determinar o valor de cada recurso e quais os riscos a que está sujeito, para encontrar formas de os eliminar ou minimizar;
- Detecção (quando, como e quem) – monitoriza e acompanha em permanência as operações, para poder determinar com exactidão quando sucedeu o incidente, como sucedeu e quem foi o responsável;
- Reacção (recuperação de danos) – são as acções que podem ser tomadas no sentido de repor a situação antes do incidente, tomando as medidas necessárias para que este tipo de incidente não volte a desencadear-se.

Laudon e Laudon (2007) referem que o armazenamento de informação com o recurso às TI provoca maiores vulnerabilidades e um vasto conjunto de ameaças do que quando tudo era processado de forma manual. Devido ao facto de a informação circular através de redes, que podem ser locais ou estarem geograficamente distantes, existe um conjunto sério de ameaças a que esta está sujeita e que podem acontecer em qualquer ponto da rede. As ameaças podem ser de natureza técnica, organizacional ou do meio envolvente, muitas das vezes por decisões de gestão inadequadas.

Segundo Gaivéo (2008), associado às questões de segurança da informação, existem ameaças, vulnerabilidades, ataques e riscos que podem afectar a actividade dos SI nas organizações, pelo que é essencial proceder à sua identificação e caracterização para uma melhor resposta e protecção dos SI no caso de se verificar alguma destas ocorrências.

2.2.1 Ameaças

Segundo Workman et al. (2008), uma ameaça é definida como uma antecipação psicológica, física ou sociológica de uma violação ou dano contra a organização. A ameaça da segurança dos SI inclui intercepção, modificação e divulgação não autorizadas da informação a terceiros e a destruição de *hardware*, *software* e informação. Quando uma ameaça é percebida, as pessoas ajustam os seus comportamentos de acordo com o risco que essa ameaça representa. As pessoas alteram o seu comportamento para uma maior ou menor cautela, de acordo com a sua percepção dos perigos e dos estragos que uma ameaça pode provocar. A avaliação e percepção da gravidade de uma ameaça e a aceitação de comportamentos de risco a ela associados têm por base as seguintes premissas:

- Os valores intangíveis que as pessoas têm sobre a vida, a liberdade e a propriedade;
- A linha limite do nível de risco que as pessoas aceitam, toleram, preferem, desejam e escolhem;
- O nível máximo de risco que é aceite até serem adoptadas medidas, depende da relação custo-benefício, vantagens e desvantagens que as medidas de segurança proporcionarão;
- A avaliação do risco determina o grau de exposição a uma ameaça ou perigo, antes de tomarem as medidas e comportamentos necessários para extinguir as ameaças.

De acordo com Silva et al. (2003), a organização pode proceder à identificação das ameaças através de cenários ou de listagens de tipos de ameaças. As listagens das ameaças por tipo facilitam a obtenção de informação sobre as ameaças que ocorreram no passado, o que permite uma melhor

análise sobre os riscos que essas ameaças representaram. As principais ameaças a que a organização está sujeita têm origem em:

- Fenómenos naturais – estão relacionados com ocorrências de origem natural como terramotos, inundações, tornados;
- Incêndios – podem ser de origem natural, acidental ou provocados deliberadamente;
- Explosões – podem ocorrer devido a falhas ou acidentes e eventualmente provocar a destruição ou perturbar o normal funcionamento dos SI/TI;
- Falhas de energia – em caso de falha pode provocar danos nos SI/TI da organização, podendo esta parar se não existir um sistema alternativo de energia;
- Falhas mecânicas – podem ocorrer em algum dos componentes que compõe os SI/TI, provocando paragens ou um funcionamento deficitário;
- Falhas infra-estruturais – podem ter origem em falhas nos equipamentos que controlam as condições do meio ambiente, como por exemplo a temperatura ou a refrigeração;
- Distúrbios sociais – têm a sua origem em tumultos, manifestações e em casos extremos de guerra;
- Erros humanos – provocados devido ao manuseamento deficiente dos SI/TI;
- Crimes – quando provocados por alguém de forma premeditada contra os SI/TI da organização;
- Acidentes biológicos ou químicos – quando determinados produtos, devido à sua composição, provocam danos nos SI/TI da organização;
- Impactos de veículos terrestres, aéreos ou navais – devido à sua localização, as organizações podem estar sujeitas a incidentes provocados por estes tipos de meio de transporte.

Carneiro (2002) classifica as ameaças da seguinte forma:

- Incidental – sem intenção premeditada, muitas vezes inerente às operações quotidianas, por exemplo, a ausência de cópias de segurança e as falhas de energia;
- Intencional – intrusão não autorizada com a intenção de aproveitamento dos recursos com fins alheios à organização proprietária;

- Passiva – embora a sua origem possa ser de natureza incidental ou intencional, não corresponde nem a nenhuma modificação da informação, nem à alteração dos recursos ou do funcionamento do SI;
- Activa – provoca a modificação da informação dos SI ou nos seus processos de funcionamento.

2.2.2 Vulnerabilidades

De acordo com Gaivéo (2008), uma vulnerabilidade é definida como uma fraqueza ou falha num sistema ou mecanismo de protecção, que expõe activos de informação a ataques ou danos.

Segundo Silva et al. (2003), a identificação das vulnerabilidades tem como objectivo calcular a probabilidade de uma potencial ameaça se concretizar. Para se proceder à identificação das vulnerabilidades podem-se utilizar listagens de tipos de vulnerabilidades.

Já Mamede (2006) refere que as vulnerabilidades representam a probabilidade de ocorrência de uma quebra ou incidente de segurança, e que podem ocorrer quando se verificam determinadas condições.

Laudon e Laudon (2007) referem que as vulnerabilidades existem em todo o percurso que a informação percorre nas redes de computadores, e podem ter origem nos acessos não autorizados provocados pelos utilizadores devido à introdução de vírus ou *spyware*, estes por sua vez acedem, roubam e alteram a informação a que têm acesso. Uma vulnerabilidade pode surgir devido ao mau funcionamento ou configuração do *hardware*, a erros ou falhas de programação no *software*, à má instalação ou configuração do *software* e a acessos não autorizados. A generalização da utilização do correio electrónico e dos serviços de mensagens instantâneas, que muitas das vezes contém anexos com *software* malicioso, que pode provocar danos ou facultar acessos não autorizados, são apontados como um dos principais elementos susceptíveis de criar vulnerabilidades nos SI.

Para Arbaugh et al. (2000), as vulnerabilidades apresentam os seguintes estados:

- Nascimento – ocorre de uma forma não intencional, na fase de desenvolvimento de um projecto de SI/TI devido a uma má especificação ou falta de testes adequados;
- Descoberta – quando alguém descobre que um SI/TI tem uma falha de segurança, ou seja, uma vulnerabilidade, não sendo importante se quem a descobriu é mal-intencionado ou não. O importante é assegurar que ela não é divulgada;

- Divulgação – acontece quando quem efectuou a descoberta da falha no SI/TI procede à sua divulgação. Aqui podem acontecer dois cenários: no primeiro a divulgação é efectuada a quem forneceu o SI/TI, para este proceder à sua correcção; no segundo a divulgação é feita com intenções maliciosas de provocar abusos e intrusões nos SI/TI;
- Correcção – a vulnerabilidade é considerada corrigida quando o fornecedor do SI/TI o altera ou modifica com o intuito de reparar a falha encontrada;
- Publicação – a vulnerabilidade torna-se conhecida a partir do momento que a divulgação é efectuada em larga escala, normalmente acontece quando a intenção é maliciosa;
- Exploração – após o conhecimento da existência da vulnerabilidade os *Hackers* e os *Crackers*, desenvolvem técnicas no sentido de a explorar com o intuito de aceder ilicitamente aos SI/TI;
- Morte – uma vulnerabilidade morre a partir do momento em que a falha do SI/TI é solucionada e aplicada por todos aqueles onde esta se verificou.

2.2.3 Ataques

Segundo Carneiro (2002), qualquer SI da organização está sujeito a ataques, que podem ser à sua existência, à sua manutenção, à sua propriedade ou à sua integridade. Por razões de concorrência, cópia, espionagem tecnológica, por questões individuais ou proveitos próprios, os SI das organizações estão sujeitos a acções que ameaçam, perturbam e afectam a estabilidade e os seus níveis de operacionalidade.

Para Mamede (2006), nenhuma organização pode afirmar que tem implementado os controlos e medidas de segurança necessárias que garantem a completa segurança dos seus SI. Devido à enorme quantidade e tipos de ataques que existem, e outros que irão surgir, que exploram as vulnerabilidades dos SI das organizações, estas têm que estar constantemente alerta e proceder ao ajustamento das medidas e controlos de segurança consoante os riscos detectados, não podendo cair na falácia do completamente seguro. Para desencadear um ataque a um SI, normalmente é seguida uma metodologia que é constituída pelas seguintes passos:

- Recolha – neste passo o atacante recolhe informação de uma forma sistematizada sobre o alvo a atacar;
- Reconhecimento – aqui o atacante procura validar a informação recolhida e identificar os dispositivos que bloqueiam a intrusão e quais os serviços que se podem efectuar a partir do

exterior. No fundo, o atacante efectua um mapa do alvo com os sistemas disponíveis e a ser utilizados, quais os que estão a ser executados no sistema e tenta introduzir-se nestes;

- Intrusão – é o passo em que é desencadeado o ataque, tentando superar as defesas e procurando uma forma ilegítima de acesso aos SI da organização.

Ainda de acordo com Carneiro (2002), os principais tipos de ataques aos SI são:

- Mascarados – quando uma entidade pretende assumir o papel de outra;
- *Replay* – quando os dados são reenviados para produzir um efeito não autorizado;
- Modificação de dados – quando a transmissão de dados é alterada sem ser detectada;
- Recusa de serviço – quando uma entidade num SI não exerce a sua função ou impede que outras exerçam as suas funções;
- Internos – quando os utilizadores de um dado sistema assumem comportamentos não autorizados;
- Externos – quando são utilizadas técnicas que incluem a captação de dados, a intercepção de emissões e o contorno dos controlos de acesso;
- *Trapdoor* – quando um SI é alterado com o intuito de permitir a um intruso um efeito não autorizado num dado evento;
- Vírus e Cavalos de Tróia – quando um SI, além das suas funções normais, produz acções não autorizadas que podem auxiliar terceiros a introduzir-se no SI.

2.2.4 Análise do Risco

Segundo Mamede (2006), existem diferentes métodos utilizados na segurança das organizações, uns são reactivos outros pró-activos:

- No método reactivo, a organização só toma as acções necessárias após a ocorrência de um problema. Esta situação pode revelar-se catastrófica, podendo ocorrer a perda de dados, danos e interrupções nos SI e, no pior dos cenários, ter que repor toda a informação por ausência de cópias de segurança.
- No método pró-activo, procura-se eliminar os pontos vulneráveis antes que sejam explorados.

É importante estar consciente que a segurança absoluta não existe, mas podemos criar capacidades e conhecimentos que permitam efectuar uma gestão adequada do risco. Para se proceder à análise do risco deve-se começar por identificar o estado actual:

- Das políticas de segurança, caso existam;
- Da segurança na rede informática;
- De segurança do sistema como um todo;
- De segurança das aplicações de rede;
- De sensibilização dos funcionários da organização;
- De segurança da informação e dos esforços de formação.

Ainda de acordo com Mamede (2006), a organização tem que identificar qual o objecto ameaçado (*hardware*, *software*, informação, processo ou equipamento controlado pelos dados), o grau de risco do mesmo (danos que podem ser causados), o nível de ameaça (probabilidade de ocorrer um ataque ou exploração de uma vulnerabilidade) e as limitações com que temos que trabalhar (todos os constrangimentos que são colocados, desde os legais, orçamentais e de investimento). Após esta identificação, é necessário verificar quais as medidas mais eficazes a serem adoptadas e quais os seus custos, como se pode visualizar na figura 2.

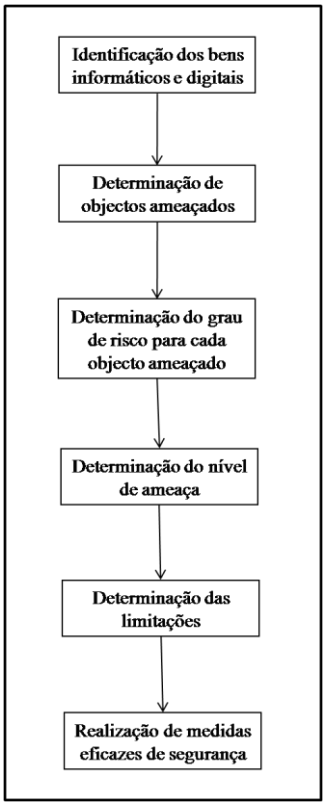

Figura 2 - A análise do risco na organização (adaptado de Mamede 2006)

A análise do risco deve conter um conjunto de características que incrementam os respectivos benefícios, nomeadamente:

- Auto-análise – a análise do risco deve ser simples o suficiente para permitir a sua utilização sem ter conhecimentos profundos de segurança ou na área tecnológica;
- Consciência da segurança – a análise do risco deve ser horizontal e envolver activamente o maior número de colaboradores, contribuindo para a tomada de consciência e sensibilização para as questões de segurança;
- Direccionamento da segurança – deve ser orientada de forma apropriada para reduzir as potenciais ameaças e vulnerabilidades;
- Linha base da segurança e políticas – a análise do risco deve contemplar a utilização de padrões como a legislação, política da organização e controlos regulatórios;
- Consciência e comunicação – ao obter informação nos vários sectores da organização, a análise do risco auxilia a comunicação e ajuda na tomada de decisão.

A análise do risco pode dividir-se em duas categorias:

- Quantitativa – neste tipo de análise são utilizados dois elementos fundamentais, a probabilidade de um evento ocorrer e a perda associada à ocorrência do evento;
- Qualitativa – é a análise mais utilizada, apenas é considerada a perda potencial estimada. Neste tipo de análise são usados, após a sua correcta identificação, os seguintes elementos inter-relacionados:
  - Ameaças – é tudo aquilo que pode falhar ou atacar o sistema;
  - Vulnerabilidades – são componentes dos sistemas que apresentam falhas que podem ser aproveitadas para desencadear ataques;
  - Controlos – são as contra-medidas para as vulnerabilidades.

O inter-relacionamento dos elementos descritos é ilustrado na figura 3:

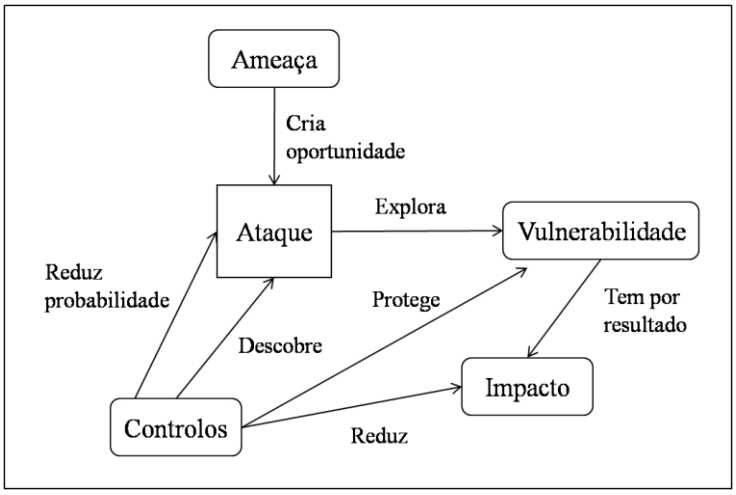

Figura 3 - Elementos a considerar na análise do risco (extraído de Mamede 2006)

Ainda de acordo com Mamede (2006), e como se pode observar na figura 3, existem ameaças que criam oportunidades de ataques através das vulnerabilidades, que por sua vez provocam impactos nos sistemas da organização. Por este motivo, têm de existir controlos que descubram antecipadamente os ataques e reduzam a sua probabilidade de ocorrência, protejam contra as vulnerabilidades detectadas, com a finalidade de reduzir o impacto destes acontecimentos adversos para a organização.

2.3 Os Utilizadores

A informação tornou-se no recurso mais precioso para a organização, pelo que garantir a sua segurança é um dos maiores desafios com que as organizações têm que lidar. Frequentemente são

aplicadas grandes quantidades de dinheiro e tempo em soluções técnicas, não considerando o factor humano. Segundo Kruger e Drevin (2010), as soluções técnicas são necessárias para resolver vulnerabilidades como ataques de vírus ou de *hackers*. No entanto, os utilizadores que manipulam informação são, em muitos casos, o elemento gerador de ataques contra a segurança da informação.

Já Ng et al. (2009) referem que os utilizadores nas organizações têm um papel crucial na prevenção e detecção das violações de segurança. Para que exista uma segurança realmente eficaz, os utilizadores têm que agir de uma forma consciente, cumprir as políticas de segurança da organização e adoptar comportamentos que não comprometam a segurança dos SI.

Para Rhee et al. (2009), o aumento e a sofisticação com que as ameaças se afiguram para as organizações, coloca a segurança da informação como um dos factores críticos dentro desta. Por outro lado, as organizações afectam os seus recursos para controlar as ameaças à segurança da informação através da utilização de *software* antivírus e *anti-spyware*, *firewalls*, sistemas de prevenção e detecção de intrusos e *software* de filtragem de conteúdos. No entanto, todos estes mecanismos de segurança aplicados podem revelar-se inúteis face à forma como os utilizadores manuseiam os SI. Muitas das falhas geradas pelos utilizadores derivam das suas acções, como por exemplo abrir uma mensagem de correio electrónico ou efectuar um *download* de um site que contém um vírus ou outro *software* malicioso, representando uma das grandes ameaças à segurança da informação. Posteriormente, infiltram-se no sistema e provocam danos neste, ou eventualmente permitem o acesso não autorizado de utilizadores externos aos SI da organização. Destes factos, conclui-se que os comportamentos dos utilizadores têm uma influência directa na segurança da informação na organização. A segurança da informação tem sido interpretada como um problema técnico, descurando talvez o factor mais frágil neste processo, que são os utilizadores.

Dhillon (2001) refere que os colaboradores que pratiquem actos ilícitos podem ser desonestos ou estar descontentes com o seu posto trabalho e copiam, roubam ou danificam a informação, em proveito próprio ou não, e as suas acções podem eventualmente passar despercebidas.

De acordo com Albrechtsen (2007), os utilizadores são considerados o factor ou a barreira mais fraca na segurança da informação. Os mecanismos para prevenção de perdas devido ao comportamento dos utilizadores resultam da combinação de factores como: as características pessoais, a estrutura da organização, os aspectos tecnológicos e físicos e as normas sociais.

Segundo Stanton et al. (2005), o aumento exponencial das interligações dos equipamentos potenciou as intrusões, os roubos, a destruição ou outras formas de perda. Esta situação leva a que

as organizações se preocupem essencialmente com as vulnerabilidades e ameaças externas. No entanto, uma grande quantidade dos incidentes tem a sua origem dentro da organização. Embora as organizações adoptem um número considerável de tecnologias para eliminar as vulnerabilidades, estas não conseguem controlar o comportamento dos utilizadores que utilizam, administram e mantém os recursos da informação.

Para Dhillon (2000), os utilizadores procuram a oportunidade mais vantajosa, não olhando a meios, podendo eventualmente vir a cometer crimes dentro da própria organização. Assim, as organizações têm que desenvolver acções, e adaptar a sua estrutura para evitar atitudes fraudulentas, corrupção, dano e distorção da informação pelos utilizadores. Para garantir a privacidade e integridade da informação, as organizações têm que considerar princípios sociais e humanos, uma vez que se tratam de colaboradores que utilizam e manipulam a informação.

Já Leach (2003) refere que as ameaças internas abrangem os erros, as omissões, a negligência e os actos contra a organização efectuados deliberadamente, englobando os seguintes comportamentos:

- Ausência de práticas de segurança - os utilizadores têm atitudes que sabem que podem provocar quebras na segurança, como por exemplo abrir ficheiros anexos a mensagens de correio electrónico ou a partilha da palavra-passe com outros utilizadores;
- Os utilizadores esquecem-se de aplicar os procedimentos de segurança - por exemplo, não efectuar as cópias de segurança ou alterar e revelar a palavra-passe;
- Os utilizadores adoptam um comportamento de risco - porque não percebem o nível de risco a que estão sujeitos, como por exemplo ausentarem-se do posto de trabalho sem bloquear o seu acesso;
- Actos deliberados de negligência - os utilizadores não adoptam os procedimentos de segurança deliberadamente, como por exemplo, enviar informação sensível sobre a organização sem qualquer tipo de protecção como a criptografia, ou não aplicam as actualizações de segurança porque é difícil;
- Ataques deliberados - os utilizadores agem contra os interesses da organização porque estão irritados com a entidade patronal, como por exemplo, fornecer informações sensíveis a organizações concorrentes ou divulgar uma vulnerabilidade de segurança a pessoas externas à organização.

De acordo com Albrechtsen e Hovden (2009) a organização visualiza de formas diferentes o papel dos utilizadores na segurança da informação, como se pode verificar na figura 4.

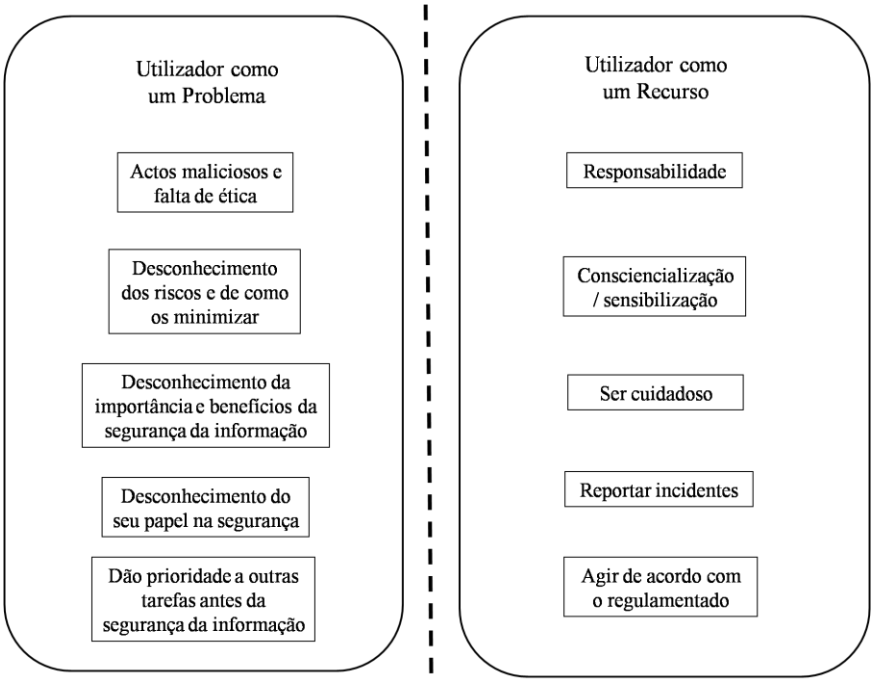

Figura 4 - O papel que os utilizadores representam na segurança da informação (adaptado de Albrechtsen e Hovden 2009)

Ainda de acordo com Albrechtsen e Hovden (2009), têm de existir diferentes tipos de acessos à informação para os utilizadores, de acordo com as suas habilidades, o âmbito da utilização, a autonomia e a capacidade para aproveitar a tecnologia ao máximo para atingir os objectivos. Segundo uma perspectiva social e técnica, os perfis diferentes estão relacionados com os conhecimentos, as competências, as percepções, as normas sociais, as relações interpessoais, que em conjunto podem fazer a diferença na performance da segurança da informação.

Rhee et al. (2009) referem que os utilizadores reconhecem que têm um papel importante a desempenhar na segurança da informação, mas afirmam que não têm os conhecimentos e as habilidades necessárias para agir de acordo com as políticas de segurança implementadas, devido principalmente à falta de treino e formação. Os responsáveis pela segurança nas organizações não podem esquecer o papel, a opinião, os comportamentos e as práticas de segurança dos utilizadores. É necessário fomentar um programa de treino e sensibilização para aumentar a eficácia dos comportamentos e práticas na segurança da informação. Não basta apresentar uma listagem com os comportamentos a evitar e com as penalizações da sua adopção, é necessário realizar acções de treino e sensibilização com ênfase nas vulnerabilidades existentes, quais as ameaças que daqui podem advir e quais os procedimentos a tomar para as eliminar e garantir a segurança dos SI.

Segundo Herath e Rao (2009), a aplicação de sanções só é possível se a organização possuir mecanismos que detectem as acções negligentes dos utilizadores. A realização de auditorias é um dos mecanismos que permitem analisar o comportamento dos utilizadores. Quanto maior for o nível de punição, menor é a tentação dos utilizadores em praticarem comportamentos desviantes, funcionando como um importante meio de dissuasão.

Já Kruger e Kearney (2006) afirmam que qualquer programa de segurança tem que ser constantemente monitorizado e medido, não só para verificar se ainda contínua útil e eficaz, devido às constantes mudanças que ocorrem e aos novos riscos que surgem no ambiente organizacional, mas também para saber se os utilizadores o aplicam e relembrar-lhes da importância que este tem para a segurança da informação na organização. Os utilizadores têm que estar cientes dos riscos associados à utilização dos SI/TI, compreender e respeitar os procedimentos de segurança que estão implementados na organização para promover a segurança da informação.

Para Furnell e Thomson (2009), não basta informar ou dizer aos utilizadores quais os comportamentos e práticas que estes têm que adoptar para se obter um nível de segurança aceitável. As organizações devem promover uma cultura de segurança junto dos utilizadores através da implementação de um conjunto de medidas. No entanto, estes podem optar por agir em conformidade ou não conformidade. De acordo com o tipo de comportamento adoptado, o nível de conformidade da segurança dos utilizadores pode ser classificado de acordo com a escala que é apresentada na tabela 1.

	Tipo de comportamento do utilizador	
Comportamentos de conformidade	Cultura	O ideal, a segurança faz parte integrante do comportamento do utilizador.
	Compromisso	A segurança é garantida através da aplicação de normas e guias de orientação, que os utilizadores aceitam e fazem um esforço para as efectivar.
	Obediência	Os utilizadores não se identificam com os princípios de segurança definidos, mas têm que os aplicar uma vez que fazem parte da política da organização.
	Sensibilização	Os utilizadores estão conscientes do seu papel na segurança da informação, mas não aplicam ainda os comportamentos e as práticas definidas.
Comportamentos de não conformidade	Ignorância	Os utilizadores ignoram as medidas de segurança e podem vir a provocar inadvertidamente danos.
	Indiferença	Os utilizadores estão conscientes do seu papel na protecção da informação, mas não querem aplicar os comportamentos e as práticas de segurança definidas.
	Resistência	Os utilizadores têm um comportamento passivo, opondo-se à adopção de práticas com que não concordam.
	Desobediência	Os utilizadores estão contra as medidas de segurança e não as adoptam, com os abusadores internos a quebrarem intencionalmente as regras e a contornarem os controlos.

Tabela 1 - Níveis de conformidade da segurança baseados nos comportamentos dos utilizadores (adaptado de Furnell e Thomson 2009)

Kruger e Drevin (2010) referem que um programa de sensibilização dos utilizadores para a segurança da informação é uma solução essencial na implementação de controlos e políticas de segurança na organização. Este tipo de programas tem como objectivo evidenciar os comportamentos a adoptar pelos utilizadores e a importância da segurança da informação e, por fim, realçar as consequências negativas de uma falha ou quebra na segurança da informação.

Ng et al. (2009) mencionam que um programa de sensibilização para as questões de segurança deve formar os utilizadores sobre os perigos dos danos provocados pelas ameaças e incidentes, para que estes percebam a necessidade de existirem regras e responsabilidades na protecção dos dados e informação da organização. Os utilizadores têm que compreender qual a função e benefícios de cada um dos tipos de controlos técnicos, físicos ou humanos e como estes ajudam a minimizar o

risco das ameaças à segurança da informação. A organização deve, com alguma regularidade, rever a estrutura e implementação das campanhas de sensibilização da segurança, para que os utilizadores percebam efectivamente as ameaças à segurança, e apliquem acções para as prevenir, evitar e eliminar de modo a promover um clima de segurança na organização.

De acordo com Kruger e Kearney (2008), um programa de sensibilização deve identificar as actividades e acções a desenvolver e o material necessário. No entanto, a primeira tarefa é identificar qual ou quais as áreas em que este vai ser aplicado, para canalizar os recursos e materiais necessários ao seu desenvolvimento.

Segundo Arcy et al. (2009), os programas de formação, treino e sensibilização de segurança da informação procuram um esforço contínuo na:

- Transmissão de conhecimentos sobre os riscos da informação no meio ambiente da organização;
- Ênfase nas sanções aplicadas aos utilizadores que provocaram violações na segurança da informação;
- Sensibilização dos utilizadores para as suas responsabilidades sobre os recursos da informação na organização.

Para Kruger e Kearney (2008), a divulgação de um programa para sensibilização das políticas de segurança da informação deve utilizar os seguintes meios de comunicação:

- Disponibilizar em todos os computadores dos utilizadores uma apresentação e um vídeo com a descrição das políticas;
- Distribuir panfletos por todos;
- Colocar posters em todas as unidades da organização;
- Conceber um sitio *Web* com informação detalhada, incluindo também uma secção de questões frequentes;
- Escrever artigos em revistas internas, caso a organização disponha deste tipo de publicação.

Já Albrechtsen (2007) refere também que o envolvimento dos trabalhadores no desenvolvimento da segurança da informação é uma medida muito mais eficaz na melhoria dos comportamentos de segurança e na sensibilização do que as campanhas de divulgação ou as regras escritas, devido a três factores:

- A participação dos utilizadores na resolução dos problemas e a possibilidade de colocarem questões;
- A possibilidade dos utilizadores reflectirem sobre as situações e que acções podem mudar para melhorar a segurança da informação;
- Reunir-se presencialmente com os responsáveis da segurança da informação, tornando-se estes mais visíveis.

Ainda de acordo com Albrechtsen (2007), os utilizadores estão motivados para adoptarem as medidas de segurança, mas não sabem como o fazer. As medidas de segurança não são aplicadas e os utilizadores não tomam as acções necessárias para o fazer devido a:

- Falta de comunicação por parte dos gestores da segurança sobre quais os comportamentos de segurança que os utilizadores devem verificar;
- A segurança da informação é implementada através de medidas tecnológicas por responsáveis da segurança da informação, que crêem que a tecnologia aplicada é suficiente para garantir o nível de segurança adequado da informação na organização;
- Falta de tempo para observar a segurança da informação no trabalho diário.

Furnell e Thomson (2009) referem que se as organizações pretendem realmente proteger a sua informação, têm que assegurar que os utilizadores estão cientes das suas responsabilidades e do seu papel neste processo e estão devidamente treinados e formados para o desempenho das funções de acordo com as políticas de segurança definidas.

Segundo Leach (2003), para efectuar a gestão eficiente das ameaças internas à segurança da informação, é necessário compreender a cultura da organização e identificar com clareza as práticas que podem influenciar o comportamento dos utilizadores. Os factores que influenciam o comportamento dos utilizadores dividem-se em dois grupos, como ilustrado na figura 5.

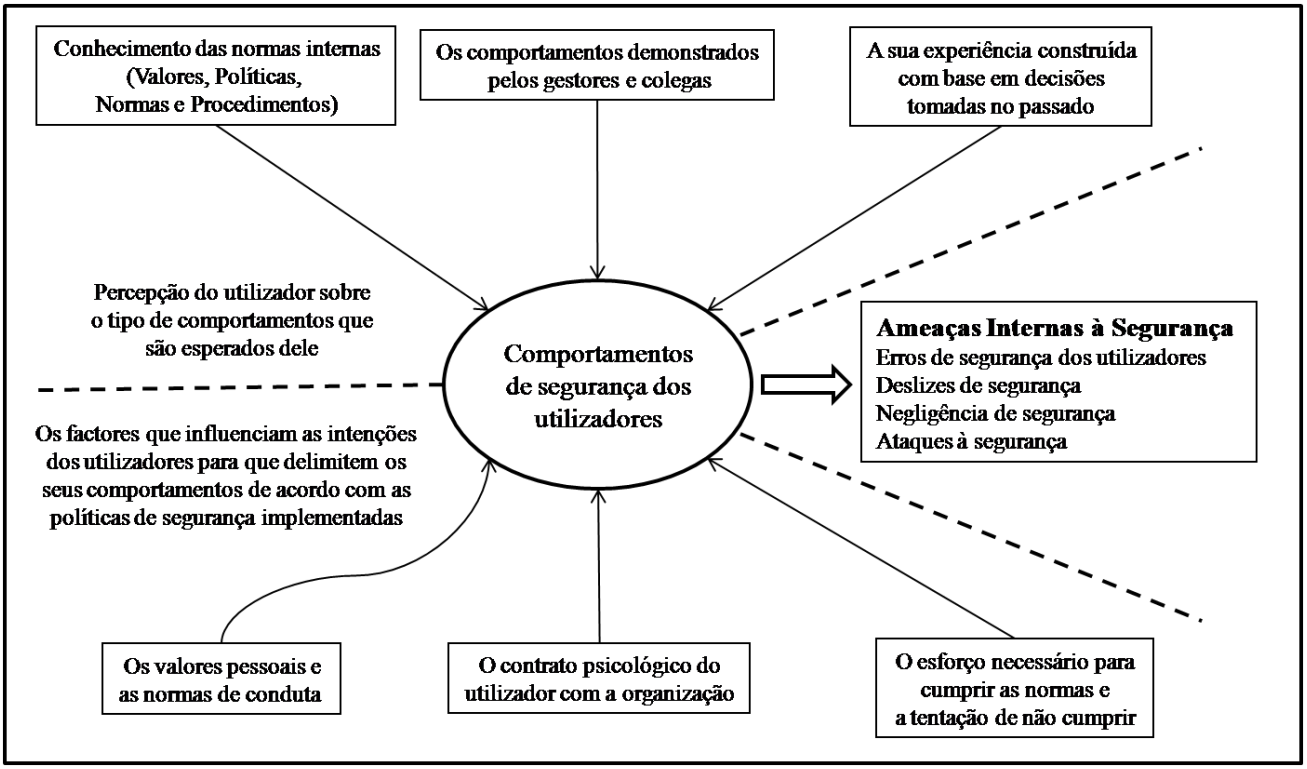

Figura 5 - Os factores com influência no comportamento de segurança dos utilizadores (adaptado de Leach 2003)

Ainda segundo Leach (2003), a percepção do utilizador sobre o tipo de comportamentos que são esperados dele engloba os seguintes factores:

- Conhecimento das normas internas – as organizações dispõe de manuais ou documentos com as normas de segurança implementadas, onde são clarificados aos utilizadores as políticas, as práticas, as normas, os procedimentos e os princípios e valores da organização. Estes manuais, usualmente designados por normas de segurança internas, contém os comportamentos de segurança a adoptar pelos utilizadores, e a sua eficácia de divulgação depende:
    - Da sua acessibilidade;
    - Da plenitude da sua cobertura;
    - Da clareza dos valores de segurança definidos;
    - Da uniformidade dos valores de segurança.
- Os comportamentos demonstrados pelos gestores e colegas – é necessário ter em atenção que existem inúmeras incoerências entre as normas definidas e o que é realmente praticado,

pelo que os utilizadores guiam-se pelo que observam e não pelo que lhes é transmitido. Os utilizadores desenvolvem as suas atitudes e comportamentos de segurança de acordo com:

  - Os valores, atitudes e comportamentos demonstrados pelos gestores da organização;
  - A coerência entre os valores definidos pela organização e os verificados nos comportamentos dos colegas de trabalho;
  - Se todas as outras práticas da organização reflectem os seus valores de segurança definidos, como por exemplo, as práticas em relação aos recursos humanos ou nos comunicados de imprensa;
  - Se a organização demonstra que as boas práticas de segurança são importantes e para tal utiliza sistemas de monitorização dos comportamentos, recompensa as boas práticas e sanciona as atitudes e comportamentos desviantes.

- A sua experiência construída com base em decisões tomadas no passado – as organizações não conseguem prever todas as situações em que é necessário tomar decisões relacionadas com a segurança. No entanto, devem concentrar os seus esforços no sentido de abranger o maior número possível de situações, tendo sempre em mente que os utilizadores irão tomar decisões próprias se não existir nenhuma recomendação para aquela situação. As decisões tomadas pelos utilizadores serão com base nas suas experiências anteriores e de acordo com o feedback que têm dessas decisões anteriores como sendo boas ou más. Os utilizadores tomam as decisões de segurança até que sejam adoptadas pelas organizações medidas ou normas de segurança interna para essas decisões.

A combinação dos três factores atrás referidos, cria no utilizador a percepção dos comportamentos e normas de segurança que são aceites e estão definidas pela organização.

Ainda de acordo com Leach (2003), os factores que influenciam as intenções dos utilizadores para que estes delimitem os seus comportamentos de acordo com as políticas de segurança implementadas são influenciados:

- Pelos valores pessoais e normas de conduta – os utilizadores atribuem grande importância aos princípios e valores, acreditam na partilha de valores e na utilização de regras sensatas. As organizações prevêem que os utilizadores que aplicam as normas e os valores definidos, vão sentir-se mais motivados na realização do seu trabalho com os outros utilizadores que seguem essas mesmas regras, do que trabalhar segundo as suas próprias regras. Existem

também situações de conflito de valores, entre os dos utilizadores e os das organizações, no entanto a solução passa por os primeiros adoptarem as normas ou abandonarem a organização;

- Pelo contrato psicológico do utilizador com a organização – os utilizadores sentem uma certa pressão psicológica para adoptar os comportamentos e as boas práticas implementadas na organização voluntariamente, tendo expressado essa vontade na altura da contratação. Apesar desta pressão, se o utilizador sentir que o seu trabalho é reconhecido e recompensado, as suas acções serão desenvolvidas de acordo com os interesses da organização, caso contrário o seu comportamento tem uma tendência desviante, podendo tornar-se numa ameaça interna para a organização;
- Pelo esforço necessário para cumprir as normas e a tentação de não cumprir – nesta situação verifica-se se o processo de cumprimento das normas e procedimentos é simples e eficaz ou existe a tentação de tirar proveitos pessoais influenciando os outros utilizadores para não os cumprirem. Mesmo que os utilizadores reconheçam o valor das políticas de segurança e os controlos adoptados pela organização, estes não os aplicam se não os entenderem ou suspeitarem da sua eficácia. A monitorização e avaliação dos comportamentos dos utilizadores e as sanções definidas para os comportamentos desviantes, têm um efeito limitado sobre as atitudes dos utilizadores, uma vez que estes por iniciativa própria não vão mudar o comportamento pelo facto de existirem mecanismos implementados.

Segundo Albrechtsen (2007), os utilizadores estão conscientes da importância do seu papel na segurança da informação na realização do seu trabalho. No entanto, existe uma falha entre a intenção e o seu real comportamento, ao não adoptarem as medidas de segurança da informação, alegando muitas vezes a falta de conhecimento das medidas existentes.

3. Políticas e procedimentos de segurança

Neste capítulo três é efectuada a descrição das políticas de segurança, a forma como estas devem ser elaboradas e como garantir a sua aplicação para uma eficaz protecção da informação nas organizações. São também identificados um conjunto de procedimentos de segurança que os utilizadores dos SI/TI devem adoptar de forma a garantir uma melhor protecção da informação. Por último é feita a referência às principais normas e legislação relacionadas com a segurança da informação.

3.1 Políticas de Segurança

A segurança da informação tornou-se num factor essencial para garantir a estabilidade de qualquer organização. Segundo Kruger e Kearney (2008), a informação representa o maior activo das organizações, pelo que está sujeita a um conjunto de vulnerabilidades e ameaças, que requerem a utilização de procedimentos e controlos tecnológicos para minimizar o seu risco.

Para Knapp et al. (2009), desenvolver um conjunto de políticas de segurança da informação é o primeiro e mais importante passo para preparar a organização contra eventuais ataques, quer estes tenham origem interna ou externa. Estas políticas de segurança são mais eficazes na redução de incidentes do que a utilização de determinados dispositivos electrónicos. As políticas de segurança da informação procuram garantir a integridade, a disponibilidade e a confidencialidade das transmissões electrónicas de dados entre SI, e são condição necessária para uma dissuasão efectiva.

Já Carneiro (2002), refere que as políticas de segurança têm por finalidade garantir a forma adequada de utilização dos recursos dos SI, as responsabilidades e direitos dos utilizadores e administradores, identificando o que deve ser protegido, e descrevem os procedimentos a desenvolver e a manter para garantir a segurança do SI.

De acordo com Mamede (2006), uma política de segurança só faz sentido na organização se for aplicada e executada por todos. Logo, a política de segurança deve assumir a forma de um contrato escrito, que cada um dos funcionários da organização deve ler, concordar e assinar. As políticas a implementar devem ser precisas, concisas e facilmente perceptíveis, não constituindo um bloqueio à produtividade individual. Além disso, devem também explicar porque são necessárias, o que contemplam, os responsáveis pelas mesmas, como vão ser aplicadas e quais as sanções pelo seu incumprimento. O procedimento de segurança deve incluir:

- Objectivo – onde se apresenta a razão da existência do procedimento;

- Descrição – onde são detalhadas todas as questões relacionadas com o procedimento em questão;
- Responsabilidades – onde são identificados todos os responsáveis pelo procedimento;
- Validade – indica a data de entrada em vigor do procedimento, e eventualmente a data da sua revisão;
- Aprovação – especifica o circuito da aprovação do procedimento e as respectivas assinaturas para o confirmar.

Segundo Knapp et al. (2009), as organizações têm que manter uma política efectiva de segurança da informação, pelo que devem realizar um guia com os princípios a adoptar e transmiti-los a todos os elementos da organização, para os sensibilizar e despertar para as questões sobre a segurança da informação.

De acordo com Kruger e Kearney (2006), é importante que os elementos da organização entendam a importância dos vários níveis de segurança que a organização tem que adoptar, compreendam as suas responsabilidades individuais no processo e percebam quais as consequências e efeitos negativos em caso de ocorrência de alguma falha ou quebra na segurança. A gestão de um programa de políticas de segurança da informação requer a combinação de controlos técnicos e processuais para gerir o risco. O valor que os controlos apresentam para a segurança da informação muitas vezes é relativo, pois pode vir a ser contornado ou abusado por quem o implementa ou utiliza, ignorando os procedimentos e políticas de segurança.

Carneiro (2002) refere que a correcta implementação de uma política de segurança depende do correcto conhecimento e cooperação dos utilizadores. Estes devem ser instruídos de modo a:

- Adoptar os comportamentos definidos perante qualquer tipo de violação;
- Saber a quem recorrer em caso de situações que provoquem algum tipo de suspeita;
- Saber quais as acções que podem realizar no sentido de minimizar os riscos de segurança;
- Interiorizar que as políticas e medidas de segurança são estabelecidas para benefício do SI e do seu nível de desempenho profissional.

Para Herath e Rao (2009), o objectivo de qualquer política de segurança na organização é influenciar e determinar as acções dos utilizadores. No entanto, o objectivo dos comportamentos relacionados com a gestão da segurança da informação é assegurar que os utilizadores agem em

conformidade com as regras e políticas estabelecidas. Os utilizadores, por seu turno, nem sempre cumprem os procedimentos de segurança da informação, e vêem as políticas de segurança como guias, linhas de orientação ou sugestões que podem adoptar em vez de normas ou regras específicas que são impostas pela organização. Face ao exposto, o grande desafio da organização é garantir a adopção das políticas de segurança pelos utilizadores.

Já Knapp et al. (2009) referem que o objectivo das políticas de segurança é fornecer a orientação e direcção à gestão das organizações e o suporte para a segurança da informação, de acordo com os requisitos da actividade da organização, com as leis, regulamentos e normalizações. Uma vez implementadas as políticas de segurança, é necessário continuar a ter o apoio da gestão, bem como a capacidade de identificar quando uma política é violada. As auditorias e as monitorizações em tempo real são as ferramentas adequadas a este cenário.

Segundo Dhillon e Torkzadeh (2006), a confidencialidade, a integridade e a disponibilidade são os principais pilares em que se baseiam as políticas de segurança. No entanto, existem outros aspectos dentro da organização que devem ser considerados como a cultura, a ética, a responsabilidade e a consciencialização. De acordo com as premissas anteriores, os autores apresentam um guia com um conjunto de objectivos fundamentais e sócio-organizacionais que pretendem indicar o rumo a adoptar para o desenvolvimento e maximização das políticas de segurança para os SI, como descrito a seguir:

- Envolver a gestão no desenvolvimento de boas práticas;
- Promover práticas adequadas de gestão de recursos humanos;
- Desenvolver e manter um ambiente ético;
- Promover o controlo de acessos;
- Promover a ética no trabalho individual;
- Promover a integridade dos dados;
- Reforçar a integridade dos processos de negócio;
- Promover a privacidade;
- Promover a integridade organizacional.

De acordo com Knapp et al. (2009), a definição, planeamento e controlo de políticas de segurança da informação passa por estabelecer o tipo de comportamentos aceitáveis, as possíveis tomadas de decisão e um conjunto de padrões a seguir, com vista à implementação de um plano de boas práticas de segurança dentro da organização.

No entanto, antes de se avançar para a criação de um plano de políticas de segurança, que deve ser bem estruturado, é necessário identificar com exactidão as vulnerabilidades dos SI, ter capacidade evolutiva, de inspecção, de detecção, de reacção e reflexo, assentando num conjunto universal de princípios, que vão permitir definir a sua estrutura, o conhecimento das suas características e melhorar a eficácia do seu desenvolvimento. Segundo Silva et al. (2003), um plano de políticas de segurança engloba o seguinte conjunto de princípios:

- Relação custo/benefício – procura um equilíbrio entre os gastos com a implementação de medidas de segurança e o retorno em termos de prevenção e protecção;
- Concentração – procura melhorar a eficiência da gestão das medidas de protecção, reduzindo a duplicação e concentrando a informação sensível com requisitos de protecção idênticos;
- Protecção em profundidade – procura melhorar a disposição dos bens a proteger, formando um anel em que os mais sensíveis estão ao centro e os menos no perímetro. A protecção é desenhada em forma de anel, que vai aumentando a complexidade das medidas e transposição das mesmas à medida que o grau de sensibilidade da informação aumenta;
- Consistência do plano – consoante o grau de sensibilidade da informação, as medidas de protecção a adoptar têm que ser semelhantes;
- Redundância – existe a necessidade de ter disponível mais do que uma forma para proteger o mesmo fim.

Após a identificação do modelo global do processo das políticas de segurança da informação e dos princípios de prevenção e protecção da segurança para a elaboração do plano, torna-se necessário elencar os princípios e mecanismos das políticas de segurança, tendo em mente que não é possível uma protecção total dos sistemas contra a utilização mal intencionada ou agressiva, pelo que as organizações têm que implementar mecanismos de protecção que impeçam a utilização do sistema por utilizadores não autorizados, como refere Carneiro (2002).

Dhillon (2004) refere que a segurança da informação envolve uma construção multifacetada, e a sua gestão exige que tenham que ser consideradas questões não apenas técnicas, mas também organizacionais, estruturais, comportamentais e aspectos sociais. As organizações não podem ter a ilusão que estão completamente seguras, devem sim focalizar a sua atenção em identificar os aspectos de segurança que melhor se ajustem e ajudem a proteger de forma eficaz a sua informação.

De acordo com Mamede (2006), os procedimentos e mecanismos mais comuns numa política de segurança são:

- Autenticação e controlo de acesso – o controlo de acesso é efectuado através da identificação e autenticação do utilizador e da utilização de dispositivos que permitam a aplicação eficaz do controlo. A forma de identificação e autenticação deve estar devidamente descrita para que todos os utilizadores conheçam a forma de aceder aos recursos, sendo atribuído a cada utilizador um determinado perfil. A autenticação pode ser implementada através de palavras-passe, *PIN*, criptografia, cartão magnético ou *RFID* e dados biométricos. São aqui definidos os critérios para a construção e a reutilização de palavras-passe, período de utilização, acções para as contas dos utilizadores criadas recentemente, especificação do número máximo de tentativas possíveis de autenticação, acções a seguir no caso de divulgação ou perda da palavra-passe;
- Criação e gestão de palavras-passe – é o factor que identifica o utilizador, pelo que deverão estar descritas as regras para a sua criação e gestão. É especificado qual o processo para a autorização da criação de um perfil de utilizador e respectiva palavra-passe. São indicadas quais as regras para a criação, preservação e manutenção das palavras-passe (utilizar a combinação de sinais, caracteres e números);
- Níveis de serviço – descreve quais os SI que têm que ser assegurados, e qual o tempo que podem permanecer indisponíveis, bem como as alternativas que estão implementadas para garantir o nível de serviço dos mesmos. Tem que identificar e descrever também as situações em que não seja possível garantir os níveis de serviços;
- Cópias de segurança e recuperação de desastre – procuram garantir a protecção dos dados em caso de incidente e recuperação de dados acidentalmente danificados. Um sistema eficaz de cópias de segurança central dá aos utilizadores toda a confiança de que estes necessitam para utilizarem as áreas de rede para armazenarem os seus dados, em detrimento do seu computador ou de dispositivos de armazenamento pessoais. Para uma maior protecção das cópias de segurança, o seu armazenamento deve ser efectuado fora das instalações da

organização. A política de segurança deve conter o método utilizado para a realização das cópias de segurança, para a recuperação de incidentes e os privilégios necessários para aceder à informação;

- Gestão do perímetro de segurança – o perímetro de segurança é uma linha virtual que faz fronteira ente a infra-estrutura interna e segura e a externa, fortemente insegura. No entanto, existe necessidade de aceder à infra-estrutura exterior, pelo que têm que existir aberturas, mas para continuar a garantir a segurança são aplicados mecanismos de controlo de tráfego e acessos, sendo o mais usual a *firewall*. A gestão do perímetro de segurança tem que impedir todos os acessos não autorizados à infra-estrutura interna;
- Formação e treino em segurança informática – os utilizadores têm que possuir um nível de sensibilização elevado para as questões da segurança da informação. Para que este factor se verifique deve ser formalizado um plano de formação com as especificações das sessões que cada um deve frequentar, devendo estas ocorrer de forma periódica;
- Aquisição de produtos e sistemas informáticos – a aquisição de novos equipamentos ou produtos deve ser realizada considerando a política de segurança implementada na organização, para que não provoquem inconsistências no que está definido;
- Segurança na transmissão de dados, ligações e acessos remotos – a organização tem que definir qual o nível de segurança que pretende ter associado à transmissão de dados, no caso de existir a comunicação entre dois pontos distantes. Após esta definição é necessário implementar os mecanismos que garantam o nível de segurança pretendido;
- Informações aos novos utilizadores – a todos os novos colaboradores são transmitidas as políticas e procedimentos implementados na organização que deverão ser rigorosamente cumpridos;
- Segurança na exteriorização de serviços – têm que estar devidamente definidos quais os serviços externos e quais os requisitos de acesso que estes necessitam, para que sejam aplicados os mecanismos adequados para garantir tanto o acesso externo aos SI, como para evitar ao máximo a execução de acções que comprometam a segurança e integridade dos dados;
- Contratação e saída de recursos humanos – tanto na entrada como na saída de utilizadores, tem de existir uma articulação entre os recursos humanos e a área responsável pela segurança, para que sejam tomadas as medidas necessárias na criação ou cancelamento de acessos e respectivos perfis. Deve-se ter também em atenção, aquando da contratação de

novos elementos, o seu registo em termos de criminalidade informática e atitudes concordantes com a ética em outras organizações;

- Acesso físico às instalações – é aqui definido o conjunto de regras e procedimentos de acesso às instalações físicas da organização, tanto por funcionários como por terceiros.
- Acesso físico à infra-estrutura e sistemas computacionais – a política de segurança deve conter medidas e controlos de acordo com a classificação da sua natureza dos computadores, terminais públicos, sistemas pessoais e sistemas de servidores;
- Configuração e gestão de equipamentos clientes – com a evolução da tecnologia, são criados diferentes dispositivos portáteis que podem ser acoplados às TI da organização. Devido a este facto, torna-se necessário criar perfis com um conjunto de controlos associado para evitar que estes dispositivos provoquem qualquer tipo de dano;
- Uso aceitável – conjunto de orientações tanto para os responsáveis pela segurança como para os utilizadores, com base nas boas práticas para se assegurar a sensibilização para as questões de segurança no trabalho do dia-a-dia;
- Protecção contra vírus – devido à rapidez com que é desenvolvido o *software* malicioso, torna-se obrigatória a utilização de *software* antivírus, instalado tanto nos servidores da organização, como em todas as estações de trabalho. O *software* deverá actualizar-se automaticamente e efectuar análise a todos os dispositivos que sejam acoplados, mensagens de correio electrónico e ficheiros que cheguem através da rede;
- Utilização da Internet – deverá existir uma clara definição do uso da Internet, o que é permitido e o que está condicionado ou negado aos utilizadores. Numa política de acesso à Internet são especificadas quais as condições em que o utilizador tem acesso à Internet, os horários, a filtragem de conteúdos, a restrição de sites ou serviços, a descarga de determinado tipo de ficheiros e programa de navegação definido;
- Correio electrónico – deverá existir uma política clara de utilização do correio electrónico, aceite por todos e respeitando as questões legais. Uma política de utilização do correio electrónico deverá conter os termos de utilização, os cuidados a ter com os conteúdos das mensagens e os perigos que daqui podem advir, bem como os danos que podem ser provocados nos SI devido a vírus, a política de monitorização das mensagens caso exista e a declaração de concordância por parte dos utilizadores;
- Ligação e acessos remotos – permitem aos funcionários da organização aceder aos SI da organização independentemente da sua localização. A política de acessos remotos especifica a forma como são efectuadas as ligações, através de linha telefónica ou rede privada virtual,

e quais os procedimentos e mecanismos que os utilizadores têm que observar para não comprometer a segurança dos SI na organização.

Carneiro (2002) refere ainda os seguintes procedimentos e mecanismos a considerar na elaboração de uma política de segurança:

- Criptografia – permite a confidencialidade dos dados e informação que são transmitidos entre duas entidades. Os dados são codificados de acordo com um modelo específico e só quem tem conhecimento do modelo consegue ter acesso aos dados;
- Mecanismos de assinatura digital – servem para comprovar que uma entidade é realmente quem diz ser;
- Mecanismos de integridade de dados – garantem que os dados recebidos pelo receptor estão íntegros.

Para Kruger e Kearney (2008), a implementação efectiva de controlos de segurança depende da criação e divulgação de um conjunto de boas práticas e comportamentos que sejam percebidos e adoptados por todos os elementos da organização.

Já Post e Kangan (2007) referem que é também pertinente identificar se o sistema de segurança implementado não interfere com as actividades dos utilizadores, criando problemas de acesso aos dados, lentidão e atrasos nas comunicações de rede, passos adicionais na realização de tarefas, o que poderia ter consequências negativas em termos de produtividade para a organização.

As organizações devem também consultar os trabalhadores no processo de identificação e estabelecimento de políticas de segurança e no teste das mesmas, possibilitando deste modo a verificação de eventuais interferências nas suas actividades ou falhas na segurança.

No entanto, segundo Mishra e Dhillon (2010), a grande maioria dos controlos implementados nas organizações não tem em consideração a perspectiva dos colaboradores, que são os responsáveis pela sua implementação. Esta situação pode provocar divergências de entendimento entre a gestão da organização, que elabora os controlos com um determinado significado e fim, e os utilizadores que eventualmente podem percepcionar de forma diferente o sentido de um determinado controlo.

Segundo Herath e Rao (2009), quando existe um conflito de interesses entre os utilizadores e os gestores da segurança, na maioria das vezes os primeiros quebram as políticas de segurança de forma intencional ou iludem a aplicação das políticas por conveniência. Os utilizadores argumentam que as restrições impostas pelas políticas de segurança têm uma influência negativa na

flexibilização das suas rotinas diárias e quebram a sua produtividade. Muito embora as organizações possam implementar tecnologias de monitorização para verificar o comportamento dos utilizadores, existem alguns comportamentos que não se conseguem controlar, como a escrita em papel e a partilha de palavras-passe com outros utilizadores.

Para Albrechtsen (2007), o conflito individual de interesses entre a segurança da informação e a funcionalidade é criado pelos seguintes factores:

- Prioridade na realização das actividades de trabalho;
- A motivação de cada indivíduo para a segurança da informação;
- A qualidade da estratégia seguida pelos gestores da segurança.

De acordo com Dhillon (2001), os problemas relacionados com a segurança ocorrem devido à ausência de medidas de segurança da informação na organização. Até pode existir uma estrutura de medidas na organização, no entanto é preciso transmiti-la correctamente aos colaboradores através dos canais de comunicação apropriados. A implementação de controlos internos em qualquer organização é a chave para a segurança da informação na organização.

Já para Mamede (2006), é impossível obter-se um nível eficiente e eficaz de segurança sem uma visão global da organização. No decorrer do processo de definição e implementação de políticas de segurança é comum cometerem-se os seguintes erros:

- Uma expressão inadequada das intenções dos gestores da organização – muitas organizações não possuem uma política de segurança reconhecida por todos, outras possuem uma política de segurança, mas as orientações são inadequadas relativamente às decisões que têm que ser tomadas. As políticas normalmente falham porque não se identifica correctamente o nível de risco aceitável, não são atribuídas correctamente as responsabilidades e deveres sobre os vários recursos, o que leva à existência de uma segurança ineficiente;
- A existência de múltiplos mecanismos de autenticação e de palavras-passe – se para entrar num sistema os utilizadores têm que utilizar vários identificadores e palavras-passe para se autenticarem, esta situação, em conjunto com as regras na criação de palavras-passe fortes e com a periodicidade de alteração, pode levar os utilizadores a descurarem a segurança, devido ao facto de terem de memorizar várias palavras-passe e com receio de as esquecerem escrevem-nas em papéis, os quais são guardados junto ao seu posto de trabalho;

- A existência de múltiplos pontos de controlo – esta situação pode originar a falta de protecção, fiabilidade e coerência dos dados, pelo facto de existirem vários mecanismos e processos que controlam o acesso aos dados, em vez de existir apenas um sistema integrado de controlo de acessos, o que por vezes resulta num controlo inconsistente e incompleto;
- A utilização de sistemas com configurações e instalações por defeito – este facto permite uma maior rapidez e facilidade na instalação e configuração, mas por outro lado leva a uma perda de controlo e instabilidade dos sistemas. Qualquer sistema antes de entrar em funcionamento tem que ser testado e ajustado para garantir a segurança;
- Uma administração complexa – o número de controlos existentes, as relações entre eles e a quantidade de conhecimentos técnicos para a sua utilização, pode levar a que o foco esteja centrado na funcionalidade dos sistemas em vez da segurança e controlo;
- Uma tardia capacidade de reconhecimento de problemas – sem uma monitorização sistemática dos sistemas, problemas e erros que possam ocorrer, são com toda a certeza detectados tardiamente e corrigidos posteriormente. Este tipo de situação pode originar a existência de ataques sem que sejam detectados, que posteriormente irão causar custos mais avultados do que os necessários para a implementação de uma monitorização eficaz, que detectaria os ataques e permitiria uma reacção e a adopção das medidas de segurança adequadas;
- A importância dos SI e o incremento da sua utilização nas organizações – com a crescente utilização dos SI nas organizações, verifica-se também um crescimento na utilização de TI e utilizadores, o que cria problemas às questões relacionadas com a segurança que não conseguem acompanhar o ritmo de crescimento.

3.2 Procedimentos de segurança a adoptar pelos utilizadores

Segundo Ng et al. (2009), a segurança dos SI depende essencialmente do comportamento do utilizador. Os colaboradores nas organizações têm um papel crucial na prevenção e detecção das violações de segurança. Para que exista uma segurança realmente eficaz, os utilizadores têm que agir de uma forma consciente, cumprir as políticas de segurança da organização e adoptar comportamentos que não comprometam a segurança dos SI, como por exemplo, definindo palavras-passe robustas, garantindo a sua confidencialidade e não transmissão a terceiros. As organizações devem promover programas para sensibilizar os utilizadores, mostrando-lhes que as suas atitudes e

comportamentos influenciam de uma forma activa a possibilidade de existirem violações à segurança da informação.

Para Workman et al. (2008), as organizações além de definirem procedimentos de segurança dos SI devem motivar os utilizadores a aplicá-los, mostrando-lhes através de simulações que as suas acções podem provocar vulnerabilidades e, consequentemente, ataques aos SI da organização. Com este tipo de acções procura-se que os utilizadores compreendam as reais ameaças e que não contornem as medidas de segurança, nem as desactivem, relegando para a organização a responsabilidade da sua implementação e controlo.

De acordo com Rhee et al. (2009), os utilizadores devem, além dos mecanismos de segurança definidos, adoptar as seguintes medidas de segurança no seu posto de trabalho:

- Aplicar as actualizações de segurança recomendadas;
- Utilizar e actualizar com frequência os programas antivírus e *anti-spyware*;
- Realizar cópias de segurança com regularidade;
- Utilizar palavras-passe robustas e diferentes em cada aplicação;
- Procurar enviar / transferir a sua informação de forma encriptada;
- Não partilhar a informação do seu computador com outros;
- Não partilhar ou divulgar as suas palavras-passe com os outros.

Kruger e Kearney (2008) referem também os seguintes procedimentos:

- Ser responsável e cuidadoso na utilização da Internet e do correio electrónico;
- Ser cuidadoso na utilização de equipamentos de armazenamento externos;
- Informar no caso de incidentes com vírus, roubos ou perdas de informação;
- Estar ciente que todos os actos praticados têm consequências.

Workman et al. (2008) evidenciam também a utilização de uma *Firewall*.

Por último, Albrechtsen (2007) acrescenta ainda os seguintes procedimentos:

- Bloquear o computador quando se ausenta;
- Não utilizar *software* ilegal ou de partilha de ficheiros.

3.3 Enquadramento Normativo e Legal

O uso das TI e dos SI pelas organizações na realização das suas tarefas diárias necessita de ser regulado, de forma a garantir que as operações realizadas pelas organizações estão de acordo com os padrões, normas e legislação. Qualquer organização, na realização das suas actividades, utiliza dados que são recolhidos e posteriormente transformados em informação, os quais são armazenados e partilhados com outros parceiros de negócio. Neste âmbito, segundo Gaivéo (2008), é necessário providenciar a segurança dos dados e da informação, quer sejam pessoais ou organizacionais, que permitem concretizar os objectivos da organização e que têm de observar a legislação em vigor e, eventualmente, adoptar as normas apropriadas para garantir a segurança desses recursos.

3.3.1 Normas Internacionais

Existem a nível internacional um conjunto de normas que as organizações podem adoptar com vista a melhorar a segurança dos SI/TI. Segundo Santos (2008), as organizações ao adoptarem as normas conseguem poupar recursos e custos, porque não necessitam de reinventar controlos e procedimentos, uma vez que já estão definidos pelas normas internacionais. A conformidade com estas normas fornece uma base comum para todas as organizações desenvolverem, executarem, aplicaram e melhorarem efectivamente as práticas de segurança.

Da panóplia de normas existentes, são destacadas e apresentadas uma síntese estrutural de três relacionadas com a segurança da informação, desenvolvidas pela *International Organization for Standardization* (ISO)[2] e pela *British Standard* (BS)[3]:

- ISO/IEC 17799:2005 (*Code of Practice for Information Security Management*);
- ISO/IEC 27001:2005 (*Information Security Management Systems – Requirements*);
- BS 7799-3:2006 (*Guidelines for Information Security Risk Management*).

[2] A ISO é uma entidade não-governamental representada em 163 países, e tem como objectivo efectuar a padronização/normalização consensual de soluções que atendam às necessidades dos negócios e das necessidades mais amplas da sociedade.

[3] A BS desenvolve e publica padrões de qualidade de bens e serviços para atender às necessidades das empresas e da sociedade, e é reconhecida pelo governo britânico como a Entidade Nacional de Padrões (*National Standards Body*) para o Reino Unido.

De acordo com a ISO (2009), a ISO/IEC 17799:2005, actualmente designada por ISO/IEC 27002:2005, estabelece as directrizes e os princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação nas organizações. Tem como objectivo fornecer orientações gerais sobre as metas vulgarmente aceites na gestão da segurança da informação.

Segundo o ISECT (2010), esta norma é um código de boas práticas e guia que as organizações podem adoptar, abrangendo todos os tipos de organizações, desde as comerciais às sem fins lucrativos.

Esta norma contém um conjunto de procedimentos de boas práticas assentes em 11 directrizes com controlos para a segurança da informação (Godwin 2007 e Mamede 2006):

1. Política de segurança - refere a necessidade de existir um documento com a política de segurança da informação, aprovado pela gestão, publicado e comunicado a todos os colaboradores e entidades externas que prestem serviços à organização. Este documento deve ser revisto periodicamente, para assegurar que os controlos de segurança são eficazes para o perfil de risco associado ao SI/TI;
2. Organização da segurança da informação - tem como objectivo gerir a segurança da informação dentro e fora da organização, mantendo os níveis de segurança necessários nas instalações de processamento da informação;
3. Gestão dos activos - tem como objectivo manter a segurança apropriada dos bens de SI/TI da organização;
4. Segurança dos recursos humanos - tem como objectivo reduzir os riscos de erro humano, roubo, fraude ou utilização indevida do sistema, assegurar que os utilizadores estão sensibilizados quanto às ameaças, à segurança da informação e têm os equipamentos necessários para suportar a política de segurança da organização. Procura também minimizar os danos de incidentes ou falhas de funcionamento e aprender com os erros ocorridos;
5. Segurança ambiental e física - tem como objectivo evitar os acessos não autorizados, danos e interferências à execução normal das actividades, prevenir perdas, danos ou roubos de informação ou dispositivos de processamento de informação;
6. Gestão das operações e das comunicações - tem como objectivo assegurar a operação correcta e segura das instalações de processamento de informação, minimizar o risco de falhas, proteger a integridade das aplicações e da informação, manter a integridade e disponibilidade do processamento da informação e da comunicação, protecção da infra-

estrutura de rede e salvaguardar a informação que nela transita, prevenir a perda, modificação ou má utilização da informação trocada entre organizações;

7. Controlo dos acessos - especifica o controlo de acesso à informação, prevenindo os acessos não autorizados aos SI, assegurar a protecção dos serviços de rede, prevenir o acesso não autorizado a computadores, detecção de actividades não autorizadas e assegurar a segurança da informação em ambientes de computação móvel;
8. Manutenção, desenvolvimento e aquisição de sistemas de informação - tem como objectivo garantir que a segurança é construída nos próprios sistemas operacionais, prevenindo a perda, modificação ou má utilização dos dados nas aplicações, garantir a confidencialidade, autenticidade e integridade da informação, assegurar que os projectos informáticos e as actividades de suporte são conduzidas de forma segura de modo a garantir a segurança das aplicações e dos dados;
9. Gestão dos incidentes de segurança da informação - qualquer tipo de incidente ou falha deve ser imediatamente reportado aos responsáveis pela segurança. Devem existir relatórios dos eventos e falhas da segurança da informação para reportar qualquer incidente que ocorra e efectuada a gestão de incidentes com a segurança da informação e respectivas melhorias;
10. Gestão da continuidade do negócio - tem como objectivo prevenir as interrupções às actividades e aos processos críticos da organização, provocadas por falhas ou desastres;
11. Conformidade - tem como objectivo assegurar que não existem contrariedades de carácter legal, de qualquer lei criminal ou cível, estatutária, regulatória ou contratual de qualquer das especificações de segurança, assegurar concordância dos SI com as políticas e normas organizacionais e maximizar a eficiência dos processos de auditoria aos sistemas e minimizar a interferência aos mesmos.

De acordo com a ISO (2009), a ISO 27001:2005 abrange todos os tipos de organizações, desde empresas privadas, a governamentais e organizações sem fins lucrativos. Especifica os requisitos para a criação, implantação, operação, monitorização, revisão, manutenção e melhorias de um sistema de gestão de segurança da informação no contexto dos riscos associados ao negócio das organizações. Apresenta um conjunto de requisitos para a implementação de controlos de segurança que pode ser aplicado à totalidade ou só a uma parte da organização, e, segundo ISECT (2010), inclui controlos que são continuamente revistos e ajustados de acordo com a mutação das ameaças à

segurança, vulnerabilidades e falhas na segurança da informação. É adequada para diversos tipos de situações, incluindo:

- Formulação dos requisitos e objectivos de segurança para a organização;
- Garantir a relação custo/eficácia da segurança nas organizações;
- Garantir o cumprimento das leis e regulamentos nas organizações;
- Modelo para a implementação e gestão dos controlos de segurança nas organizações;
- Definição de um novo processo de gestão da segurança;
- Identificação e clarificação do actual processo de gestão de segurança da informação;
- Verificação do estado das actividades da segurança da informação;
- As auditorias internas e externas para verificar o grau de cumprimento das políticas, directivas e normas adoptadas pela organização;
- O uso, por parte das organizações, para informar os parceiros e outras organizações dos procedimentos, das políticas, das directrizes e normas adoptadas nas questões operacionais e comerciais;
- A implementação de uma política efectiva de segurança da informação;
- Informar os clientes da sua política de segurança da informação.

Ainda de acordo com ISECT (2010), as organizações desenham a sua própria política de segurança da informação com base na lista de controlos disponibilizados pela norma, tendo em conta a avaliação efectuada aos riscos a que a informação está sujeita, com base nas seguintes directrizes:

1. Sistema de Gestão da Segurança da Informação (SGSI) – tem como base o modelo "plano, realizar, verificar e agir". O plano define os requisitos, a avaliação do risco e quais os controlos a aplicar. A realização implementa e efectiva o SGSI, através da aplicação de controlos e de procedimentos que permitam detectar incidentes. A verificação monitoriza e efectua a revisão do SGSI, através da medição da eficácia dos controlos e da revisão dos riscos. Agir mantém e procura melhorar o SGSI, aplicando as medidas correctivas necessárias e comunicando as acções a adoptar;
2. Responsabilidade da gestão – a gestão tem que demonstrar o seu envolvimento com o SGSI e providenciar a afectação dos recursos necessários à sua implementação e operacionalização;

3. Auditoria interna do SGSI – a organização tem que providenciar a auditoria interna do SGSI para assegurar que este contém os controlos adequados e eficazes;
4. Revisão do SGSI – a gestão da organização tem que efectuar a revisão da adequação e efectividade do SGSI pelo menos uma vez por ano e providenciar, caso sejam necessárias, as mudanças para o ajustarem às novas realidades;
5. Melhoria do SGSI – a organização tem que procurar a melhoria contínua do SGSI, efectuando as mudanças que se verifiquem necessárias para assegurar a sua efectividade de modo a evitar as não conformidades dos controlos.

Segundo a BS (2009), a BS 7799-3:2006 apresenta um conjunto de directrizes que visam permitir uma gestão do risco mais eficiente nas organizações.

De acordo com ISECT (2010), esta norma foi adoptada pela ISO/IEC e é actualmente designada por ISO/IEC 27005:2008, fornecendo linhas de orientação para a gestão do risco da segurança da informação. Foi projectada com o intuito de implementar a segurança da informação com base na abordagem da gestão do risco. É aplicada a todo o tipo de organizações que pretendam efectuar a gestão dos riscos que podem comprometer a segurança da informação. A norma indica a necessidade de identificar os riscos associados aos activos da informação, as potenciais ameaças e as suas fontes, as potenciais vulnerabilidades e o impacto que advém da concretização dos riscos.

A estrutura da norma encontra-se dividida em quatro grupos de directrizes na gestão do risco, de acordo com a BS (2009) e Gaivéo (2008):

1. Risco da segurança da informação no contexto organizacional considerando: o âmbito e políticas do SGSI (que engloba o caso do negócio; âmbito do SGSI; políticas do SGSI) e a abordagem do risco / filosofia;
2. Avaliação do risco, considerando: processo de avaliação do risco; a identificação dos activos; a identificação dos requisitos legais e de negócio (que engloba a origem dos requisitos; os requisitos legais, regulamentares e contratuais; os princípios organizacionais, objectivos e requisitos do negócio); a avaliação dos activos; a identificação e avaliação das ameaças e vulnerabilidades (que engloba controlos implementados; identificação das ameaças e vulnerabilidades); a avaliação das ameaças e vulnerabilidades; o cálculo e avaliação do risco; o responsável pela gestão do risco;

3. Tratamento e gestão do risco de acordo com as decisões da gestão, considerando: as disposições genéricas; o processo e tomada de decisão; a redução do risco; a aceitação do risco de uma forma consciente e objectiva; a transferência do risco; evitar o risco; o risco residual; o plano de tratamento do risco;
4. Processo contínuo da gestão do risco, considerando: a gestão contínua do risco de segurança; a manutenção e monitorização; a revisão da gestão; a revisão e reavaliação do risco; a auditoria; o controlo da documentação; as acções preventivas e correctivas; o reporte e comunicação que engloba o plano de comunicação; envolvimento e feedback; o gestor do risco de segurança.

3.3.2 Legislação

Em Portugal, segundo Silva et al. (2003), existe um esforço recente na criação de um quadro legal que vise o correcto enquadramento das normas de segurança, e que se traduz na transposição das directivas comunitárias.

Gaivéo (2008) refere como crucial identificar as leis aplicáveis em Portugal, para que seja possível a correcta e adequada aplicação das normas de segurança às necessidades de segurança da informação, sem que sejam violadas as Leis vigentes. Das Leis existentes em Portugal relacionadas com a problemática da segurança da informação, destacam-se as seguintes:

A Lei nº 109/91, de 17 de Agosto, da Criminalidade Informática, enquadra em termos de quadro penal os crimes praticados na informática, identifica e tipifica os mesmos e define as penalidades em termos de moldura penal (Lei nº 109/91). São identificados por esta Lei seis crimes ligados à informática:

- Falsidade informática (artigo 4º) - a introdução, alteração ou eliminação ilegítima de dados ou programas informáticos que possam servir de prova em relações jurídicas;
- Dano relativo a dados ou programas informáticos (artigo 5º) - a introdução, alteração ou eliminação ilegítima de dados ou programas informáticos com o objectivo de causar prejuízos a terceiros ou proveitos próprios;
- Sabotagem informática (artigo 6º) - a introdução, alteração, eliminação ou interferência ilegítima de dados ou programas informáticos com o objectivo de perturbar ou interromper o seu funcionamento ou transmissão;
- Acesso ilegítimo (artigo 7º) - quando existe o acesso ilegítimo a um sistema ou rede informática;

- Intercepção ilegítima (artigo 8º) - quando há a intercepção não autorizada das comunicações num sistema ou rede informática;
- Reprodução ilegítima de programa protegido (artigo 9º) - quando é efectuada a reprodução, divulgação ou comunicação pública não autorizada de um programa informático protegido por lei.

A Lei estabelece ainda as penas aplicáveis às pessoas colectivas e equiparadas, bem como todo o conjunto de penas acessórias a aplicar a quem cometa os crimes referidos.

O Decreto-Lei nº 252/94, de 20 de Outubro, que transpõe para a ordem jurídica portuguesa a Directiva nº 91/250/CEE do Conselho Europeu de 14 de Maio, relativa à protecção jurídica dos programas de computador (Decreto-Lei nº 252/94). Este documento, nos termos do seu artigo 1º, confere aos programas de computador a protecção idêntica à concedida às obras literárias, nos casos em que estes tenham carácter criativo. Já o artigo 2º procede à definição e forma como a protecção é efectuada e a sua extensão. Nos artigos 14º e 15º são fixadas a tutela penal e a tutela por outras disposições legais que são aplicadas à reprodução não autorizada dos programas de computador.

A Lei nº 67/98, de 26 de Outubro, Lei da Protecção dos Dados Pessoais, adopta para a ordem jurídica nacional a Directiva Comunitária nº 95/46/CE do Parlamento Europeu e do Conselho Europeu de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de forma transparente dos dados pessoais e à livre circulação destes (Lei nº 67/98). Esta Lei aplica-se, nos termos do nº1 do artigo 4º, ao tratamento dos dados pessoais quer por meios total ou parcialmente automatizados, quer através de meios não automatizados contidos em ficheiros manuais. Os capítulos mais relevantes definidos na presente Lei são:

- Tratamento dos dados pessoais (artigos 5º ao 17º) – define os princípios de legitimidade e tratamentos dos dados pessoais, todos os direitos dos titulares dos dados e a segurança e confidencialidade do tratamento dos dados;
- Transferência dos dados pessoais (artigos 18º ao 20º) – estipula o processo de transferência de dados pessoais dentro e para fora da União Europeia;

- Comissão Nacional de Protecção de Dados (CNPD) (artigos 21º ao 31º) – estabelece a natureza, atribuições, competências, composição e competências da CNPD no âmbito de toda a regulamentação de protecção dos dados pessoais;
- Códigos de conduta (artigo 32º) – a CNPD procede à sua supervisão e aprovação de acordo com as disposições da presente Lei;
- Tutela administrativa e jurisdicional (artigos 33º ao 49º) – são identificados os meios administrativos jurisdicionais a que os cidadãos podem recorrer em caso de violação dos seus dados, bem como definidos todo o conjunto de contra-ordenações e crimes para quem não cumprir as disposições legais da presente Lei.

A Lei nº 5/2004 de 10 de Fevereiro, Comunicações Electrónicas, estabelece o *"regime jurídico aplicável às redes e serviços de comunicações electrónicas e aos recursos e serviços conexos e define as competências da autoridade reguladora nacional neste domínio"* e transpõe para a ordem jurídica nacional as Directivas n.os 2002/19/CE, 2002/20/CE, 2002/21/CE e 2002/22/CE do Parlamento Europeu e do Conselho Europeu de 7 de Março de 2002, e a Directiva 2002/77/CE da Comissão Europeia de 16 de Setembro de 2002 (Lei nº 5/2004). Os capítulos mais relevantes definidos na presente Lei são:

- Autoridade Reguladora Nacional (ARN) (artigos 4º ao 13º) – procede à definição e estabelece as suas competências e objectivos de regulação no âmbito das comunicações electrónicas;
- Supervisão e fiscalização (artigos 107º ao 119º) – são identificadas as formas de resolução de conflitos, os incumprimentos, as medidas a aplicar, as formas de fiscalização, as coimas e contra-ordenações e as sanções a aplicar a quem não cumprir com o disposto na presente Lei.

A Lei nº 41/2004, de 18 de Agosto, Lei da Protecção da Privacidade no Sector das Comunicações Electrónicas, transpõe para a ordem jurídica nacional a Directiva Comunitária nº 2002/58/CE do Parlamento Europeu e do Conselho Europeu de 12 Julho de 2002 relativa ao tratamento dos dados pessoais e à privacidade no sector das comunicações electrónicas (Lei nº 41/2004). A presente Lei,

segundo Veiga (2009), especifica e complementa as disposições da Lei nº 67/98. Os capítulos mais relevantes desta Lei são:

- Objectivo e âmbito (artigos 1º e 2º) – onde é fixado o objectivo e âmbito da presente Lei, a sua aplicação e efectuada a definição dos termos utilizados;
- Segurança e confidencialidade (artigos 3º ao 13º) – procedem à definição das medidas para garantir a privacidade nas comunicações electrónicas, a inviolabilidade das comunicações electrónicas, as formas de armazenamento e acesso à informação, o tratamento dos dados e a sua localização;
- Regime sancionatório (artigos 14º ao 16º) – são estabelecidas as coimas e contra-ordenações e ainda como vão ser processadas e aplicadas para quem não cumpra com as disposições definidas na presente Lei

.

4. Metodologia

No capítulo quatro é apresentada a abordagem metodológica utilizada na realização deste trabalho, identificada a população e a amostra, o instrumento e o processo de recolha de dados e por último como será efectuada a análise dos dados.

4.1 Fundamentação teórica

A metodologia, segundo Freixo (2009), inclui todos os elementos que ajudam a conferir à investigação um caminho ou direcção, sendo necessário escolher um método ou procedimento apropriado conforme se trate de explorar ou de descrever um fenómeno, de examinar associações e diferenças ou de verificar hipóteses. A metodologia preocupa-se também com a definição da população e com a escolha dos instrumentos mais apropriados para efectuar a colheita dos dados, e com a sua fiabilidade.

Ainda de acordo com Freixo (2009), o método é o caminho pelo qual se chega a um determinado resultado, ainda que esse caminho não tenha sido fixado de antemão de modo reflectido e deliberado. O método implica um conjunto de actividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objectivo definido, traçar o caminho a ser seguido, detectando erros e auxiliando as decisões.

Assim, de acordo com o descrito, o método é um plano geral traçado para dar resposta à questão de investigação, e deve ser adequado para concretizar o objectivo geral da investigação, que neste caso é saber em que medida os comportamentos e as atitudes dos utilizadores constituem um risco ou uma protecção para a segurança dos SI nas organizações.

O método dedutivo, segundo Freixo (2009), parte de premissas gerais em busca de uma verdade particular, não trata da verdade dos factos, mas sim da sua validade. Este método deve partir de uma teoria que é comprovada, ou não, através da observação (dedução).

Já o método quantitativo, ainda de acordo com Freixo (2009), constitui um processo sistemático de colheita de dados observáveis e quantificáveis. É baseado na observação de factos objectivos, de acontecimentos e de fenómenos que existem independentemente do investigador. Tem por finalidade contribuir para o desenvolvimento e validação dos conhecimentos, oferece também a possibilidade de generalizar os resultados, de predizer e de controlar os acontecimentos.

Deste modo, para atingir o objectivo deste trabalho será utilizada a abordagem dedutiva, sendo efectuada uma pesquisa bibliográfica exploratória com base em fontes secundárias (artigos

científicos, livros, teses, etc.), que permitirá realizar a revisão da literatura onde vão ser explanados os tópicos relacionados com a segurança da informação, isto com o intuito de identificar os procedimentos que os utilizadores devem adoptar para garantir a segurança dos SI dentro das organizações.

A abordagem de investigação quantitativa será utilizada para analisar os resultados obtidos no questionário com recurso às ferramentas estatísticas.

4.2 População e Amostra

Considerando o objectivo principal deste trabalho, identificar em que medida os comportamentos e as atitudes dos utilizadores constituem um risco ou uma protecção para a segurança dos SI nas organizações, a população alvo deste estudo são todos aqueles que para realizar as suas tarefas numa organização utilizam SI/TI. Como o universo dos utilizadores dos SI/TI nas organizações não se encontra registado, pelo que é impossível determinar a sua população, será utilizada uma amostra não probabilística. A técnica de amostragem utilizada será uma amostra por conveniência, na qual, de acordo com Hill e Hill (2005), os elementos escolhidos são aqueles que estão disponíveis. Tem a vantagem de ser um método rápido, barato e fácil. Como desvantagem, o rigor, os resultados e as conclusões só se aplicam à amostra, não podem ser extrapolados com confiança para o universo. Isto porque não há garantia que a amostra seja razoavelmente representativa do universo.

4.3 Recolha de dados

4.3.1 Instrumento de recolha de dados

A recolha dos dados, como refere Freixo (2009), envolve a colheita da informação junto dos participantes com a ajuda dos instrumentos de medida seleccionados. É identificado o instrumento de medida que pode ser a entrevista, o questionário, a grelha de observação e a escala de medida. O investigador descreve as características dos instrumentos e trata dos aspectos de fiabilidade e de validade. Prevê, tanto quanto possível, os problemas que o processo de colheita dos dados poderá levantar.

De acordo com o exposto no parágrafo anterior o instrumento seleccionado para efectuar a recolha de dados é o questionário, e tem como população alvo os utilizadores que usam os SI/TI para realizarem as suas tarefas na organização. As questões do questionário serão elaboradas tendo por base os procedimentos de segurança identificados na revisão da literatura.

O questionário, segundo Freixo (2009), é constituído por um conjunto de enunciados ou questões que permitem avaliar as atitudes e opiniões dos sujeitos ou colher qualquer outra informação junto

desses mesmos sujeitos. O questionário é habitualmente preenchido pelos próprios sujeitos e sem assistência. É um instrumento de medida que traduz os objectivos de um estudo com variáveis mensuráveis. O conteúdo de um questionário não constitui um acumular de questões em jeito livre e arbitrário, desordenado e sem nexo, pelo contrário, este conteúdo deve responder aos pressupostos colocados pelo problema, e sobretudo, pelas hipóteses e variáveis de investigação. No questionário, todas as questões são formuladas antecipadamente e podem ser do tipo aberto ou fechado.

Neste trabalho as perguntas do questionário são do tipo fechado, onde os respondentes escolhem uma opção de resposta entre as disponíveis, pois trata-se de um questionário anónimo e preenchido pelo utilizador sem assistência.

Ainda de acordo com Freixo (2009), nas perguntas do tipo fechado são apresentadas ao respondente uma lista pré-estabelecida de respostas possíveis de entre as quais lhe é solicitado para indicar a que melhor corresponde à resposta que deseja dar. A utilização deste tipo de respostas tem como vantagens a rapidez e facilidade de resposta, a maior uniformidade, rapidez e simplificação na análise das respostas, facilita a categorização das respostas para posterior análise e permite contextualizar melhor a questão. Como principais desvantagens, a dificuldade em elaborar as respostas possíveis a uma determinada questão, não estimula a originalidade e a variedade de resposta, não preza uma elevada concentração do inquirido sobre o assunto em questão e o inquirido pode optar por uma resposta que se aproxima mais da sua opinião não sendo esta uma representação fiel da realidade.

A construção e aplicação do questionário tem como objectivo principal identificar em que medida os comportamentos e as atitudes dos utilizadores constituem um risco ou uma protecção para a segurança dos SI nas organizações.

Na elaboração do questionário, o primeiro elemento colocado foi a introdução no início da primeira página, que, segundo Hill e Hill (2005), deve incluir os seguintes aspectos:

- Um pedido de cooperação no preenchimento do questionário, referindo o tempo de preenchimento;
- A razão da aplicação do questionário, indicando qual o objectivo principal do questionário;
- Uma apresentação curta da natureza geral do questionário, referindo que o questionário não é um teste e que não há respostas certas ou erradas;
- O nome da instituição (faculdade)

- Uma declaração formal da confidencialidade das respostas – a informação fornecida será tratada confidencialmente, e que os resultados da pesquisa não vão identificar ninguém;
- Uma declaração formal da natureza anónima do questionário.

Como referido, o questionário é composto por um conjunto de perguntas do tipo fechado pelo que, de acordo com Freixo (2009), torna-se necessário escolher um conjunto de respostas alternativas para cada uma destas perguntas, devendo associar-se números a essas respostas para que estas possam ser analisadas posteriormente por meio de técnicas estatísticas.

Os valores numéricos associados a cada um dos conjuntos de respostas possíveis às questões representam uma escala de medida. Neste questionário foram utilizadas as escalas nominal e ordinal, as quais foram identificadas e seleccionadas com base na literatura (Hill e Hill, 2005).

Segundo Freixo (2009), a escala nominal é utilizada para a atribuição de números a elementos para representar categorias mutuamente exclusivas e exaustivas sem que os números tenham valor quantitativo. Esta categorização permite diferenciar os indivíduos em função de critérios qualitativos sem que haja ordenamento de uma categoria ou outra. A escala ordinal é utilizada para atribuir um valor numérico a pessoas ou objectos que se classificam em categorias segundo uma ordem de grandeza, ou seja, nesta escala são atribuídos números aos elementos segundo o seu valor relativo para representar uma ordem de grandeza. Esta ordem de grandeza não significa que os intervalos entre as categorias sejam iguais, mas que as categorias são ordenadas, além de serem diferentes.

Em termos de construção de escalas, é utilizada a escala de Likert, que é uma escala de cinco níveis, em que cada um desses níveis é considerado de igual amplitude, significando que a análise dos dados provenientes deste tipo de escala se baseia, normalmente, em resultados somados a partir de um número de itens. A sua utilização tem lugar na procura de indicadores para registar o grau de concordância ou de discordância com determinada afirmação sobre uma atitude, uma crença, ou um juízo de valor, segundo Freixo (2009).

O questionário elaborado é composto por três grupos de questões. O primeiro grupo é constituído por três questões. A primeira questão do grupo I tem como objectivo servir de filtro para identificar quais os respondentes que cumprem os requisitos para preencher a totalidade do questionário, que neste caso são os utilizadores dos SI/TI nas organizações. Nesta questão é utilizada uma escala de medida nominal.

A segunda questão do grupo I é composta por 27 alíneas, que foram colocadas de forma não ordenada, e contém um conjunto de afirmações construídas com base nos procedimentos de segurança identificados na revisão da literatura, em que o respondente tem que escolher qual a opção que melhor caracteriza a sua opinião. As respostas possíveis são: sim, não e não sei. A escala de medida utilizada nesta questão é a nominal. Algumas alíneas da questão foram elaboradas na negativa com o intuito de evitar que o respondente entre em monotonia e efectue uma análise adequada da questão antes de responder.

A terceira questão do grupo I contém um conjunto de 18 afirmações colocadas de forma não ordenada, também construídas com base nos procedimentos de segurança identificados na revisão da literatura, em que o respondente tem que escolher qual o seu grau de concordância ou discordância segundo a escala não comparativa de Likert de 1 a 5 (em que 1 corresponde a "Discordo totalmente", 2 a "Discordo em parte", 3 a "Nem concordo nem discordo", 4 a "Concordo em parte" e 5 a "Concordo totalmente"). Nesta questão a escala de medida utilizada é ordinal. Aqui nesta questão foram também elaboradas algumas afirmações na negativa.

O segundo grupo é composto por uma questão destinada a registar comentários ou sugestões, não sendo obrigatório o seu preenchimento.

No último grupo de questões são solicitados os dados de caracterização dos respondentes, nomeadamente o intervalo de idade, o sexo, o grau de ensino mais elevado concluído, a situação profissional, o número de trabalhadores na organização, o distrito de trabalho e o sector de actividade da organização. Os dados aqui solicitados são os estritamente necessários à consecução do estudo, sendo garantindo o anonimato dos respondentes. Aqui a escala de medida utilizada é a nominal.

4.3.2 Pré-teste

Após a construção do questionário, o mesmo foi submetido a um pré-teste, com o intuito de identificar a existência de qualquer dificuldade de interpretação ou de preenchimento das questões, bem como o tempo que os utilizadores necessitam para responder ao mesmo. O pré-teste foi distribuído em papel junto de 13 utilizadores de SI/TI nas organizações, escolhidos de forma aleatória, com as seguintes actividades profissionais:

- Agente de Autoridade;
- Secretária de Direcção;

- Técnico Superior;
- Recepcionista;
- Assistente Operacional;
- Chefe de Secção de hipermercado;
- Monitora numa instituição de ensino particular;
- Responsável de armazém;
- Professora de Ensino Básico;
- Professora de Escola Profissional;
- Secretária de Junta de Freguesia;
- Bibliotecária;
- Chefe de Secção numa empresa de frio;

Depois de terminado o pré-teste e efectuada a respectiva recolha dos questionários, estes foram processados e analisados onde foi apurado que o tempo necessário para o preenchimento do questionário pelos utilizadores situou-se entre os 9 e os 15 minutos. Cada um dos utilizadores apresentou, no final do preenchimento do questionário, a sua opinião acerca das questões bem como das dificuldades encontradas. Os pontos apontados pelos utilizadores às questões do questionário foram essencialmente na compreensão de algumas questões, no enquadramento da questão naquele grupo e dificuldade em responder a algumas questões que se encontravam na negativa.

Deste processo resultou o estabelecimento do tempo indicativo de resposta ao questionário a colocar na introdução do mesmo, cerca de 15 minutos e a alteração de questões no grupo 2, por dificuldades de interpretação, e reformuladas algumas no grupo 3 cuja redacção não se enquadrava correctamente neste grupo.

Após serem efectuadas as correcções apontadas ao questionário, o mesmo foi submetido a um novo pré-teste, desta vez *on-line*, para identificar possíveis falhas na navegação ou qualquer dificuldade de interpretação ou de preenchimento que ainda pudessem persistir. O questionário foi divulgado de forma aleatória para um conjunto de 9 utilizadores com as seguintes actividades profissionais:

- Enfermeira;
- Tesoureiro;

- Professora na área da Contabilidade;
- Bancário;
- Empregada de escritório;
- Trabalhador em controlo de gestão;
- Consultor de gestão;
- Chefe de Secretaria;
- Técnica Superior;

Depois de terminado o pré-teste e segundo a opinião dos utilizadores, não foram detectadas falhas tanto na navegação como na interpretação.

Após este passo o questionário foi colocado *on-line* e o processo de recolha dos dados junto dos utilizadores de SI/TI nas organizações processou-se entre os dias 31 de Janeiro de 2011 e 31 de Março de 2011.

No anexo 1 apresenta-se uma cópia do conteúdo do questionário que foi disponibilizado através da Internet.

4.3.3 Processo de recolha dos dados

Segundo Hill e Hill (2005), o processo de recolha de dados descreve como vai ser aplicado o questionário, devendo incluir os detalhes necessários para que o leitor possa avaliar as circunstâncias do preenchimento e o nível de controlo atingido na aplicação do mesmo.

O processo de recolha dos dados será efectuado *on-line*, pelo que é criado especificamente para este fim um sítio *Web*, que tem associada uma base de dados do Microsoft Access para efectuar o armazenamento das respostas ao questionário. A divulgação e o apelo à participação no questionário são efectuados com recurso ao correio electrónico, tendo sido criada a conta de correio electrónico questionario.seginf@gmail.com para proceder ao envio da mensagem com a hiperligação para o questionário, bem como para prestar qualquer informação ou esclarecimento aos utilizadores sobre o questionário. É também elaborada uma carta de apresentação (apresentada no anexo 2) a incluir na mensagem de correio electrónico que tem como destinatário os utilizadores dos SI/TI nas organizações, com o objectivo de obter o maior número possível de respostas.

4.4 Análise dos dados

De acordo com Freixo (2009), os dados são analisados e apresentados de forma a facultar uma ligação lógica com o objecto do estudo. Nesta etapa há lugar à classificação, codificação e selecção dos dados, sendo necessário igualmente reagrupá-los de forma compreensível a fim de facilitar a análise e interpretação a ter lugar na fase de apresentação dos resultados.

- A classificação dos dados significa dividir os dados em partes, dando-lhes ordem, colocando cada um no seu lugar. O processo de classificação é baseado num determinado critério ou fundamento adoptado pelo investigador que orienta a divisão de um todo em partes, classes ou categorias. Não se podem usar critérios diferentes e as categorias estabelecidas devem abranger todos os elementos coligidos tendo como preocupação não deixar nenhum de fora. A classificação é portanto uma forma de distribuir e seleccionar os dados obtidos na fase de recolha, reunindo-os em classes ou grupos de acordo com os objectivos e interesses da pesquisa.
- A codificação abrange todas as tarefas de classificação dos dados e atribuição de símbolos (códigos). A codificação transforma os dados em elementos quantificáveis.
- A tabulação apresenta os dados obtidos da categorização em tabelas. A disposição dos dados graficamente permite facilitar a interpretação e análise e facilita ainda o processo de inter-relação entre eles e da relação dos mesmos com as hipóteses de estudo.

Segundo Hill e Hill (2005), nesta fase processa-se também a listagem de todas as variáveis incluídas na investigação empírica e indica-se brevemente como é que cada uma delas foi medida.

Face ao exposto, e após a conclusão da recolha de dados, foi efectuada a análise dos mesmos com recurso ao *software* Microsoft Excel e ao SPSS (*Statistical Package for the Social Sciences*). De modo a facilitar a análise dos dados, aquando da construção do questionário *on-line* foi efectuada uma codificação das opções possíveis de respostas às questões que posteriormente iriam ser armazenadas na base de dados (ver anexo 3).

Os dados armazenados na base de dados foram exportados para o *software* Microsoft Excel, onde foi efectuada uma filtragem a estes com o intuído de proceder à limpeza dos registos danificados ou que não estavam em condições de serem considerados na análise, de modo a prepará-los para a análise quantitativa. Após este processo os dados foram importados para o SPSS, onde previamente foi definido para cada variável o nome, tipo, tamanho, valores assumidos e o tipo de escala associado, de modo a permitir a sua análise estatística.

Ainda segundo Hill e Hill (2005), na análise dos dados é necessário descrever as técnicas que foram aplicadas para testar cada uma das hipóteses da investigação, bem como os tipos de estatísticas descritivas que foram utilizadas (por exemplo, média e desvio padrão) e as técnicas indutivas aplicadas. A estatística descritiva, que descreve de uma forma sumária alguma característica de uma ou mais variáveis fornecidas por uma amostra de dados. As medidas mais utilizadas são as de tendência central, nomeadamente, o valor médio, a mediana e a moda. O desvio padrão, a variância, e o intervalo inter-quartil também são estatísticas descritivas porque dão uma descrição sumária da variação dos valores de uma variável. As estatísticas descritivas podem ser apresentadas por meio de quadros ou gráficos. Por seu turno, as estatísticas indutivas permitem avaliar o papel dos factores ligados com o acaso quando se pretende retirar conclusões a partir de uma ou mais amostras de dados.

Pestana e Gageiro (2008), referem que a informação descritiva relevante para as variáveis nominais refere-se às frequências simples e à categoria mais frequente (moda). A informação descritiva relevante para as variáveis ordinais refere-se às frequências simples, às frequências acumuladas, à moda e às estatísticas de ordem.

Já Freixo (2009) refere que a escala nominal permite a utilização de estatísticas descritivas tais como as distribuições de frequências, as percentagens e as correlações de contingência.

Tendo por base os objectivos deste trabalho e o tipo de escalas usadas, as técnicas estatísticas utilizadas na análise dos dados são:

- Análise de Frequências;
- Média.

Para uma melhor percepção da distribuição da amostra e das respostas ao questionário, as diversas técnicas estatísticas utilizadas irão ser apresentadas através de gráficos e quadros.

As alíneas e afirmações das questões 2. e 3. foram colocadas no questionário de forma não ordenada, no entanto para efectuar a análise dos dados irão ser agregadas as que estão inter-relacionadas com base nos procedimentos de segurança da informação identificados na revisão da literatura, de acordo com a tabela seguinte:

Procedimento de segurança	Questão 2	Questão 3
Actualizações de segurança	2.1	3.1
Programas antivírus e *anti-spyware*	2.2; 2.16	3.2; 3.18
Cópias de segurança	2.3; 2.17	3.3; 3.12
Palavras-passe robustas e diferentes	2.4 ; 2.11; 2.18; 2.19; 2.26	3.4; 3.13
Encriptação da informação	2.5; 2.23	3.5
Partilha da informação do computador	2.6; 2.22	-
Partilha de palavras-passe	2.7; 2.24	3.6
Internet e correio electrónico	2.8; 2.20; 2.25	3.7; 3.17
Equipamentos de armazenamento externos	2.9	3.8
Incidentes com a informação	2.10; 2.21	3.14
Consciência dos actos praticados	2.12; 2.27	3.9; 3.15
Utilização de *Firewall*	2.13	3.10
Bloqueio do computador	2.14	3.11
Utilização de *software* ilegal	2.15	3.16

Tabela 2 - Agrupamento das alíneas das questões 2. e 3. de acordo com os procedimentos de segurança

5. Resultados e discussão

Segundo Hill e Hill (2005), os resultados têm que continuar a história da investigação e os resultados numéricos, resultantes da análise estatística, têm que ser explicados em palavras.

Aqui serão apresentados os principais resultados das análises estatísticas efectuadas às respostas ao questionário.

5.1 Resultado da recolha dos inquéritos

A tabela 3 efectua o resumo das respostas ao questionário evidenciando, o número total de respostas ao questionário, o número de respostas válidas e o número de respostas não válidas.

Número total de respostas ao questionário	Número de respostas válidas	Número de respostas não válidas
817	780	37

Tabela 3 - Resultado da recolha dos inquéritos

Como se pode observar, dos 817 respondentes ao questionário foram excluídos 37 elementos. Dos 37 elementos, 18 foram excluídos pelo facto de terem respondido "Não" à questão "1. Usa computador na sua actividade profissional?" e 19 elementos porque, embora tenham respondido na íntegra ao questionário, indicaram na questão "4. Situação profissional" serem estudantes ou estarem desempregados.

Assim, foram admitidos no estudo 780 elementos, passando a designar-se por "respostas válidas", uma vez que desenvolvem a sua actividade com recurso ao computador, a população alvo, deste estudo.

5.2 Caracterização dos respondentes

Neste ponto é caracterizado o perfil dos elementos (780) que compõem o estudo, e que desenvolvem a sua actividade profissional nas organizações com recurso ao computador.

Para uma melhor visualização das variáveis de caracterização, são utilizadas, preferencialmente as tabelas com a análise das frequências. No entanto, sempre que a visualização se torne mais fácil são utilizados gráficos.

No anexo 4 foram colocadas todas as tabelas de frequências geradas para as variáveis de caracterização da amostra.

5.2.1 Escalão das idades e sexo

A tabela 4 ilustra a distribuição dos respondentes por escalão etário.

	Frequências	**Percentagem**
Menos de 16 anos	0	0,0
Dos 16 aos 29 anos	109	14,0
Dos 30 aos 49 anos	**497**	**63,7**
Dos 50 aos 64 anos	170	21,8
Mais de 64 anos	4	0,5
Total	780	100,0

Tabela 4 – Questão III-1: Distribuição das respostas válidas por idade

Das 780 respostas válidas, 63,7% situam-se no escalão etário entre os 30 e os 49 anos, 21,8% situam-se entre os 50 e os 64 anos, 14% situam-se entre os 16 e os 29 anos e 0,5% com mais de 64 anos.

De acordo com o boletim da estatística do emprego, 1º trimestre de 2011 (INE[4], 2011) 51,6 % da população activa situa-se no escalão etário entre os 25 aos 44 anos, 36,1% dos 45 aos 64 anos, 6,6% dos 15 aos 24 anos e 5,7 % mais de 65 anos. Pela observação destes dados, e comparando com os dados obtidos no questionário, podemos concluir que em termos de escalão etário, os respondentes encontram-se distribuídos de acordo com os parâmetros normais da população activa.

Relativamente ao género dos respondentes válidos, 55,1 % são do sexo feminino e 44,9% do masculino. Pelo resultado observado podemos constatar que o questionário teve um maior número de respostas por parte do sexo feminino. Esta situação fica a dever-se ao facto de a maioria dos respondentes desenvolverem a sua actividade no sector dos serviços, como se pode verificar no ponto 5.2.6 Sector de actividade da organização. De acordo com o boletim da estatística do emprego, 1º trimestre de 2011 (INE, 2011), no sector de actividade dos serviços 55,69% dos trabalhadores são do sexo feminino e 44,31% do sexo masculino. Face a estes dados, conclui-se que o resultado obtido para o género dos respondentes encontra-se de acordo com os valores normais da população activa.

[4] INE – Instituto Nacional de Estatística

5.2.2 Grau de ensino mais elevado que terminou

A tabela 5 apresenta a distribuição dos respondentes pelo grau de ensino mais elevado que terminaram.

	Frequências	Percentagem
Não frequentou a Escola ou não concluiu o 1.º …	0	0,0
Ensino Básico 1.º Ciclo (4.º ano de escolaridade)	1	0,1
Ensino Básico 3.º Ciclo (9.º ano de escolaridade)	8	1,0
Ensino Secundário (12.ª ano de escolaridade)	68	8,7
Curso Pós-Secundário – Curso de Especialização	22	2,8
Curso Superior (Bacharel, Licenciatura)	**371**	**47,6**
Curso Pós-Graduado (Mestrado, Doutoramento)	310	39,7
Total	780	100,0

Tabela 5 - Questão III-3: Distribuição das respostas válidas por grau de ensino

Em termos do grau de ensino mais elevado concluído pelos respondentes, 47,6% têm Curso Superior (Bacharel, Licenciatura), 39,7% têm Curso Pós-Graduado (Mestrado, Doutoramento), 8,7% têm o Ensino Secundário (12º ano de escolaridade), 2,8% têm Curso Pós-Secundário – Curso de Especialização, 1% têm o Ensino Básico 3º Ciclo (9º de escolaridade) e 0,1% têm o Ensino Básico 1º Ciclo (4º ano de escolaridade).

Da análise dos dados constata-se ainda que 87,3% (47,6% + 39,7%) dos respondentes têm formação superior. Este valor pode-se explicar pelo facto de a grande maioria dos inquiridos desenvolver a sua actividade profissional em sectores onde são exigidas qualificações de nível superior, pelo que têm também uma maior sensibilidade e formação relativamente às questões relacionadas com a segurança da informação. O maior nível de qualificação e formação dos respondentes permitiu obter no seu conjunto respostas mais coerentes e adequadas.

5.2.3 Situação profissional

O gráfico seguinte ilustra distribuição dos respondentes segundo a sua situação profissional.

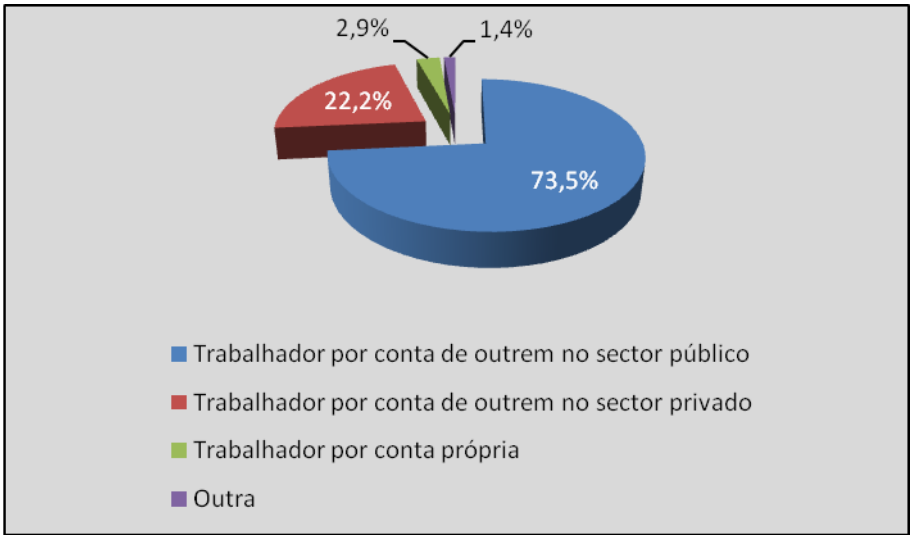

Figura 6 - Questão III-4: Distribuição das respostas válidas por situação profissional

Dos 780 respondentes, 73,5% trabalham por conta de outrem no sector público, 22,2% trabalha por conta de outrem no sector privado, 2,9% trabalha por conta própria e 1,4% encontram-se em outra situação. A tabela com a distribuição dos respondentes com respostas válidas pode ser consultada no anexo 4.

De acordo com o ilustrado no gráfico, a maioria dos respondentes desenvolvem a sua actividade no sector público. Este resultado fica a dever-se, essencialmente, ao facto de ser o sector com o qual tínhamos maior proximidade e, consequentemente, um vasto leque de contactos através do qual foi divulgado o questionário, o que provocou a tendenciosidade do resultado.

As outras situações profissionais referidas (1,4%) representam essencialmente questões pontuais, nomeadamente situações em que os respondentes trabalham no sector público e no sector privado.

5.2.4 Número de trabalhadores da organização

A tabela 6 apresenta a distribuição dos respondentes em termos de número de empregados da entidade empregadora.

	Frequências	Percentagem
Menos de 10 funcionários	47	6,0
De 10 a 49 funcionários	89	11,4
De 50 a 249 funcionários	**335**	**42,9**
250 funcionários ou mais	271	34,7
Não sei	38	4,9
Total	780	100,0

Tabela 6 - Questão III-5: Distribuição das respostas válidas por número de trabalhadores

Quanto ao número de trabalhadores da organização, dos 780 respondentes, 42,9% trabalham em organizações que têm de 50 a 249 funcionários, 34,7% trabalham em organizações com 250 funcionários ou mais, 11,4% trabalham em organizações que têm de 10 a 49 funcionários, 6% trabalham em organizações que têm menos de 10 funcionários e 4,9% não sabe o número de funcionários da organização onde trabalham. Face a estes resultados, a maioria dos respondentes ao questionário trabalham em organizações com mais de 50 funcionários

Segundo os dados disponibilizados pelo INE (2009), sobre as empresas portuguesas, no tecido empresarial português 95,59% têm menos de 10 funcionários, 3,78% têm de 10 a 49 funcionários, 0,54% têm de 50 a 249 funcionários e 0,08% têm 250 funcionários ou mais. Pelos resultados obtidos podemos constatar que embora o número de empresas com 50 ou mais funcionários represente apenas 0,63% (0,54% + 0,08) do tecido empresarial português, o maior número de repostas ao questionário situa-se neste grupo (organizações com 50 ou mais funcionários) o que pensamos, se deve ao facto de estarmos perante grandes organizações do sector público.

5.2.5 Distrito da organização

O gráfico seguinte ilustra a distribuição dos respondentes pelo distrito onde trabalham.

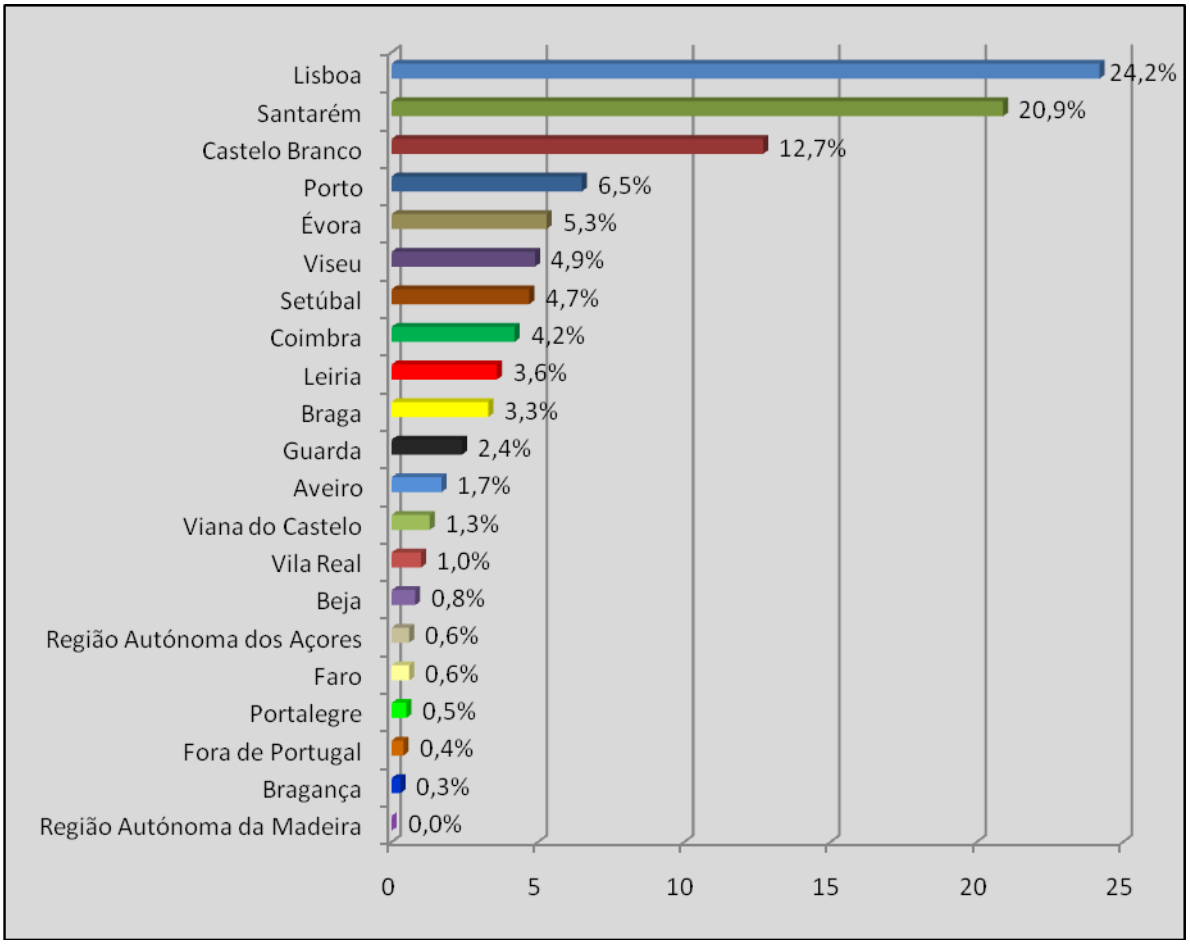

Figura 7 - Questão III-6: Distribuição das respostas válidas por distrito

O distrito com maior representatividade na amostra é o de Lisboa com 24,2%, seguindo-se o de Santarém com 20,9%, o de Castelo Branco com 12,7%, o do Porto com 6,5% e os restantes distritos apresentam frequências mais baixas. Da observação dos valores, Lisboa é o distrito que apresenta mais respostas pelo facto de ser a região com maior número de empresas, como se pode comprovar pelos dados disponibilizados pelo INE (2009), sobre as empresas portuguesas, onde 30,62% das empresas a nível nacional encontram-se situadas na região de Lisboa. Em segundo e terceiro lugar, Santarém e Castelo Branco respectivamente, por serem os distritos onde tínhamos o maior número de colegas e amigos que colaboraram e se predispuseram a ajudar na divulgação do questionário, disponibilizando também os seus contactos de correio electrónico.

Relativamente a este ponto, é de referir também que três respondentes indicaram que trabalhavam fora de Portugal, um em Espanha, outro no Reino Unido e o último no Brasil. A tabela com a distribuição pode ser visualizada no anexo 4.

5.2.6 Sector de actividade da organização

Os dados referentes à distribuição dos respondentes pelo sector de actividade são ilustrados na tabela seguinte.

	Frequências	**Percentagem**
Actividades de consultoria, científicas, técnicas ...	40	5,1
Administração Pública e defesa	50	6,4
Educação	**481**	**61,7**
Outras actividades de serviços	32	4,1
Outra	53	6,8
Restantes actividades	153	15,9
Total	780	100,0

Tabela 7 - Questão III-7: Distribuição das respostas válidas por sector de actividade

O sector de actividade mais representado foi o da Educação, com 61,7%, seguindo-se "Outra" com 6,8%, a Administração Pública e defesa com 6,4%, as actividades de consultoria, científicas, técnicas e similares com 5,1%, outras actividades de serviços com 4,1% e os restantes sectores com frequências mais baixas representando, em conjunto 15,9%.

É notória a diferença entre o sector de actividade com maior percentagem, o da Educação com 61,7%, e o segundo valor mais elevado de percentagem a opção "Outra" com 6,8%. Esta situação deve-se principalmente ao facto de ser esta a área, como referido anteriormente, onde se concentravam essencialmente os nossos contactos e por estarmos perante uma amostra não probabilística por conveniência, realizada através de um questionário *on-line* divulgado através do correio electrónico pelas listas de contactos de colegas e amigos tipo "corrente". A divulgação do questionário foi efectuada deste modo com o intuito de obter o maior número de respostas possível para a concretização do estudo. Por este facto, a divulgação foi feita sobretudo junto da comunidade académica, o que provocou uma maior representatividade destes respondentes. De facto, embora este método funcione bem em termos de divulgação, o mesmo não se pode dizer em termos de representatividade da população.

A tabela de frequências relativa à opção "Outra" dos respondentes pode ser consultada no anexo 4. Embora a lista dos sectores de actividade fosse bastante representativa, podem no entanto ter suscitado algumas dúvidas aos respondentes. Algumas das respostas na opção "Outra" correspondem a classificações dos sectores de actividade referidos no CAE-Ver.3.

5.3 Análise dos resultados

As questões 2 e 3 do grupo I, como referido no ponto 4.4 (ver págs. 62 e 63), foram agrupadas de acordo com os procedimentos de segurança identificados na revisão da literatura. As análises estatísticas efectuadas a este conjunto de questões permitem percepcionar a forma como as questões do questionário se distribuem de acordo com os procedimentos de segurança.

Nas questões do grupo 2 foram geradas todas as tabelas de frequência e em seguida construídos gráficos com a distribuição das frequências. Nas questões do grupo 3, onde foi utilizado uma escala de Likert de 5 pontos (como valor médio da escala de 3), além das tabelas de frequências foi calculado o valor médio para cada questão, com o intuito de verificar se a média das respostas está acima da média da escala. As questões 3.1, 3.7, 3.14 e 3.16 foram colocadas na negativa, pelo que é necessário ter este factor em consideração na análise das mesmas, uma vez que a média das respostas para estar de acordo com os procedimentos correctos terá que ser inferior à média da escala.

Neste ponto são utilizados os gráficos com a distribuição dos valores e com os valores médios das respostas em vez das tabelas de frequência, pelo facto de permitirem uma visualização mais simplificada e imediata dos valores obtidos nas respostas. Associado a cada procedimento de segurança e respectivos gráficos é efectuada uma pequena descrição dos resultados obtidos. Todas as tabelas de frequência foram geradas e podem ser consultadas no anexo 5.

Os resultados a seguir apresentados resultam das 27 respostas da questão 2 e das 18 respostas da questão 3, e tinham como objectivo identificar se os comportamentos adoptados pelos respondentes estão de acordo com os procedimentos de segurança identificados na revisão da literatura.

5.3.1 Actualizações de segurança

A figura 8 ilustra a distribuição das respostas à questão 2.1 e a figura 9 o valor médio das respostas à questão 3.1, onde os inquiridos eram questionados sobre as actualizações de segurança recomendadas.

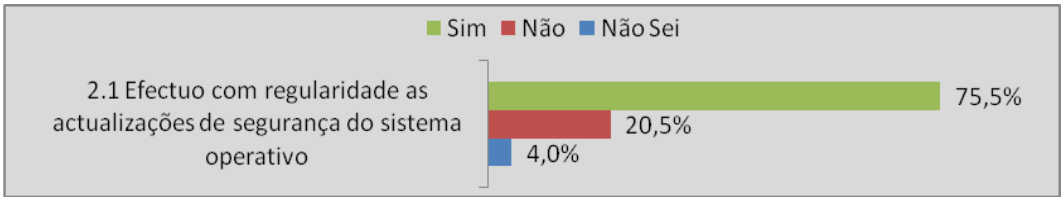

Figura 8 – Questão 2.1: Distribuição das respostas ao procedimento actualizações de segurança

Como se pode observar pelos dados da figura 8, mais de 75% dos respondentes efectuam com regularidade as actualizações de segurança do sistema operativo, o que revela um comportamento adequado.

Da análise da figura 9 podemos visualizar que os respondentes consideram importante efectuar as actualizações de segurança do sistema operativo e restantes aplicações, o que é, também, uma atitude correcta.

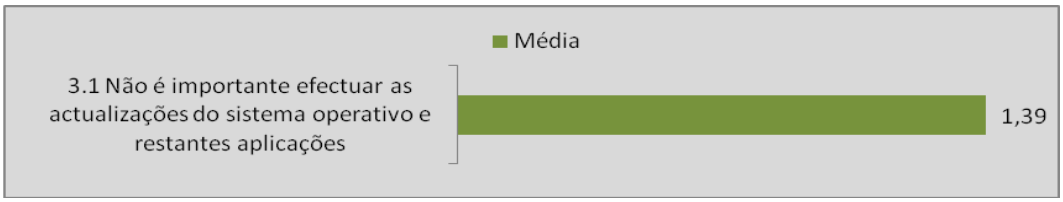

Figura 9 - Questão 3.1: Valor médio das respostas ao procedimento actualizações de segurança

Face a estes resultados, fica comprovado que os utilizadores apresentam um comportamento e uma atitude de acordo com o recomendado, como referem Rhee et al. (2009), que mencionam que os utilizadores devem, além dos mecanismos de segurança definidos, aplicar as actualizações de segurança recomendadas.

5.3.2 Programas antivírus e *anti-spyware*

As figuras a seguir apresentam a distribuição das respostas às questões 2.2 e 2.16, e o valor médio das respostas às questões 3.2 e 3.18, onde os inquiridos eram questionados sobre a utilização de programas antivírus e *anti-spyware*.

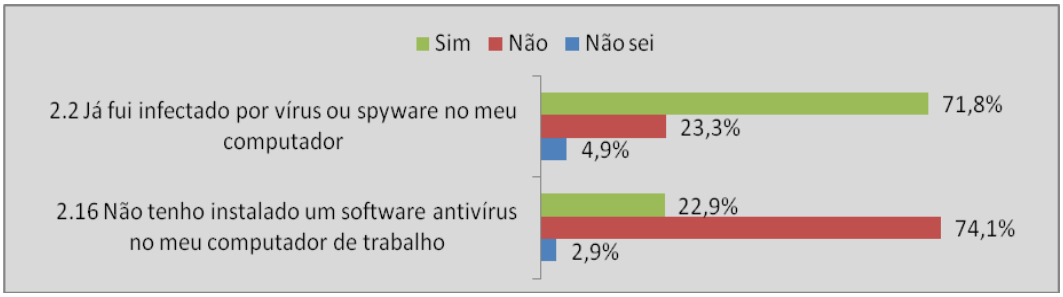

Figura 10 - Questões 2.2 e 2.16: Distribuição das respostas ao procedimento antivírus e *anti-spyware*

As respostas à questão 2.16 revelam que a maior parte, 74,1%, dos respondentes têm instalado um programa antivírus no computador de trabalho. Por outro lado, uma percentagem elevada dos respondentes, 71,8%, também já foi infectado por vírus ou *spyware*, facto que pode ser entendido como alguma falta de cuidado por parte dos utilizadores. De facto, os programas antivírus e *anti-spyware* não garantem a protecção total, pelo que, mesmo com aquele tipo de programas é necessário algum cuidado e não adoptar comportamentos de risco. De acordo com Mamede (2006) e com Rhee et al. (2009), embora as organizações possuam programas antivírus e *anti-spyware* instalados e actualizados, estes podem vir a relevar-se ineficazes devido às acções dos utilizadores, como por exemplo: colocarem um dispositivo de armazenamento externo infectado, abrirem uma mensagem de correio electrónico ou efectuar um *download* de um site que contém um vírus ou outro *software* malicioso, podendo estes vir a infiltrar-se nos SI da organização e a provocar danos ou permitir o acesso não autorizado.

A análise da figura 11 revela que os respondentes têm uma atitude correcta em relação aos programas antivírus e *anti-spyware* como meio de protecção, bem como relativamente à necessidade de actualizar estes programas regularmente.

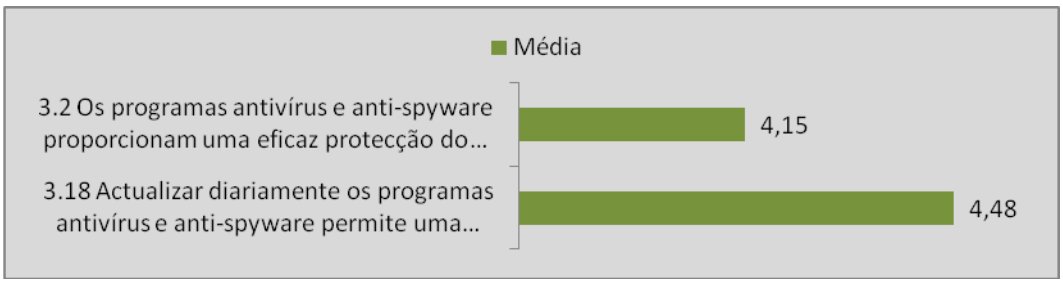

Figura 11 - Questões 3.2 e 3.18: valor médio das respostas ao procedimento antivírus e *anti-spyware*

Neste procedimento os respondentes, e como se pode observar pelas figuras anteriores, têm um comportamento e uma atitude consideradas adequadas, pois não só têm instalado *software* antivírus no seu computador, como atribuem a este tipo de programas capacidade de protecção do computador. No entanto, a grande maioria revela que já foi infectada por vírus, pelo que os utilizadores devem ter maior atenção neste ponto e não adoptar alguns dos comportamentos de risco referidos anteriormente.

5.3.3 Cópias de segurança

Apresentamos, nas figuras seguintes, a distribuição das respostas às questões 2.3 e 2.17, e o valor médio das respostas às questões 3.3 e 3.12, onde os inquiridos eram questionados sobre a realização de cópias de segurança.

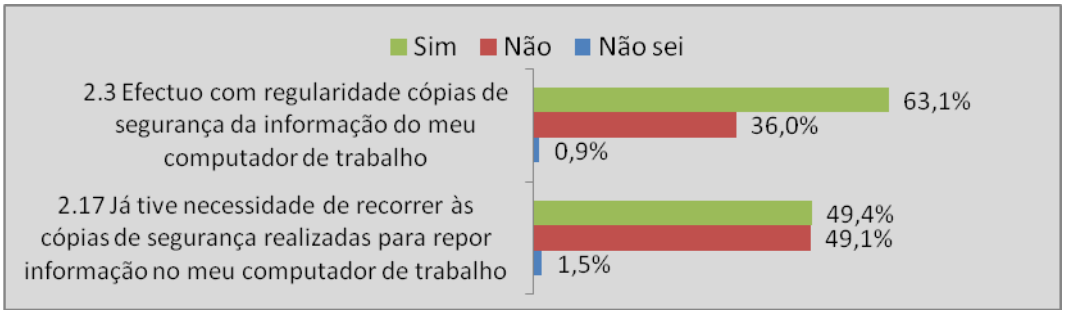

Figura 12 - Questões 2.3 e 2.17: Distribuição das respostas ao procedimento cópias de segurança

A maioria dos respondentes, 63,1%, efectua cópias de segurança da sua informação, como se pode observar na figura 12. O facto de 49,4% dos respondentes indicarem que já tiveram necessidade de recorrer às cópias de segurança, vem reforçar e comprovar a importância da sua existência e da sua realização com alguma regularidade.

Na figura 13 podemos constatar que os respondentes reconhecem que não é uma atitude correcta efectuar cópias de segurança apenas para o disco do computador e admitem ser suficiente efectuar as cópias de segurança semanalmente.

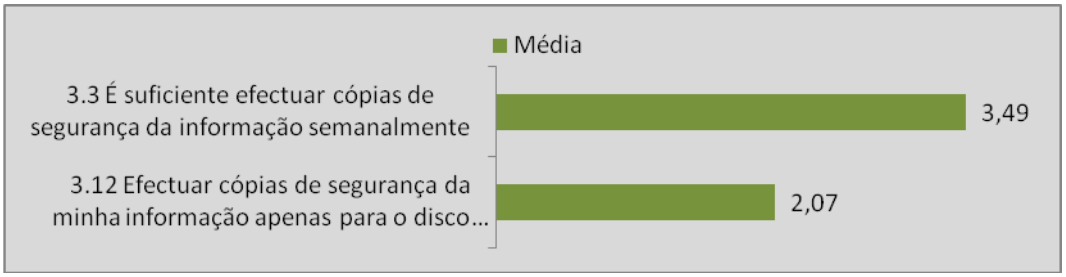

Figura 13 - Questões 3.3 e 3.12: Valor médio das respostas ao procedimento cópias de segurança

Perante estes resultados, e embora a maioria dos utilizadores (63,1%) apresente um comportamento adequado, ao indicar que efectua com regularidade as cópias de segurança, há ainda uma percentagem de utilizadores, 36,0%, que não estão devidamente sensibilizados para a importância da realização das cópias de segurança. Em nossa opinião, a percentagem dos que realizam com regularidade cópias de segurança deveria estar próxima de 100%. De referir ainda que a atitude dos utilizadores relativamente à questão da periocidade semanal na realização das cópias de segurança deveria também ter um valor superior, com uma média das respostas de pelo menos 4, o que pode ser indicador de algum relaxe por parte dos utilizadores na regularidade com que efectuam as cópias de segurança. De acordo com os valores obtidos, podemos considerar que os utilizadores apresentam comportamentos e atitudes adequados na realização das cópias de segurança, no entanto os valores observados deveriam ser, como referido anteriormente, superiores. Ou seja, os utilizadores deveriam estar mais consciencializados para a importância de realizarem com regularidade as cópias de segurança, como referem Rhee et al. (2009).

5.3.4 Palavras-passe robustas e diferentes

A figura 14 ilustra a distribuição das respostas às questões 2.4, 2.11, 2.18, 2.19 e 2.26, enquanto a figura 15 representa o valor médio das respostas às questões 3.4 e 3.13, onde os inquiridos eram questionados sobre a construção e utilização de palavras-passe.

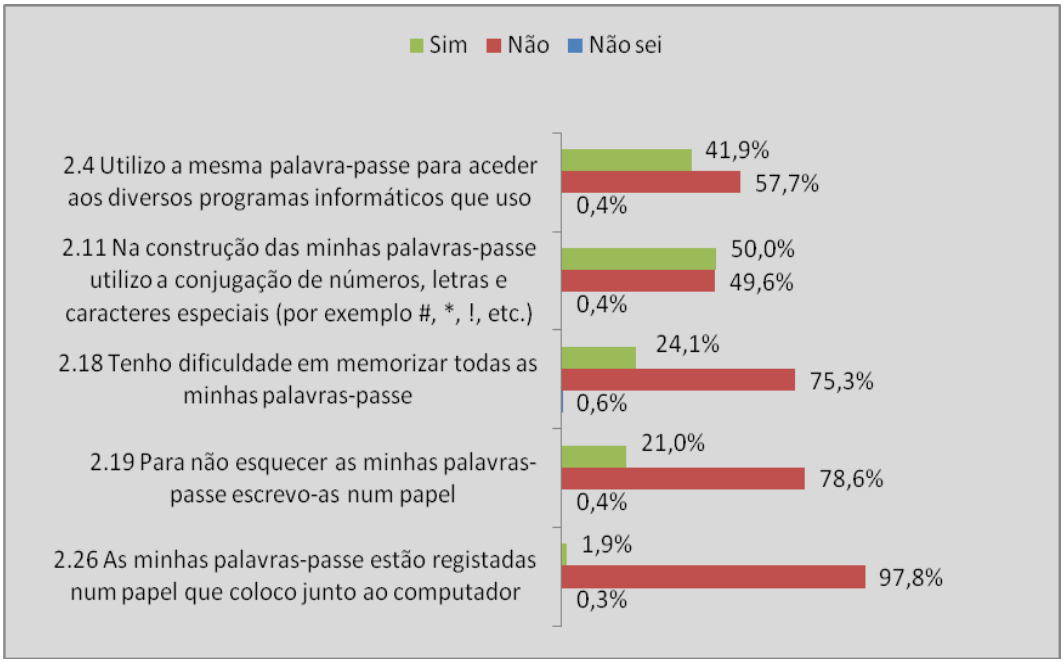

Figura 14 - Questões 2.4, 2.11, 2.18, 2.19 e 2.26: Distribuição das respostas ao procedimento de construção das palavras-passe

Segundo o ilustrado na figura 14, a grande maioria dos respondentes indica não ter qualquer dificuldade em memorizar as palavras-passe (75,3%) e não ser necessário registar as mesmas em papel (78,6%), estando estes comportamentos de acordo com o recomendado. No entanto, como se pode visualizar na mesma figura, uma percentagem razoável dos respondentes (41,9%) utiliza a mesma palavra-passe para aceder aos diversos programas, e só metade usa números, letras e caracteres especiais na construção da palavra-passe. A quase totalidade dos respondentes refere que não tem as palavras-passe registadas num papel colocado junto ao computador.

De acordo com o observado na figura 15, os respondentes indicam ser uma atitude correcta alterar as palavras-passe uma vez por ano, no entanto quando são solicitados para proceder à alteração das palavra-passe optam pelas fáceis de memorizar, o que não é uma atitude de acordo com o correcto, devendo os utilizadores procurar utilizar palavras-passe robustas como referem Rhee et al (2009).

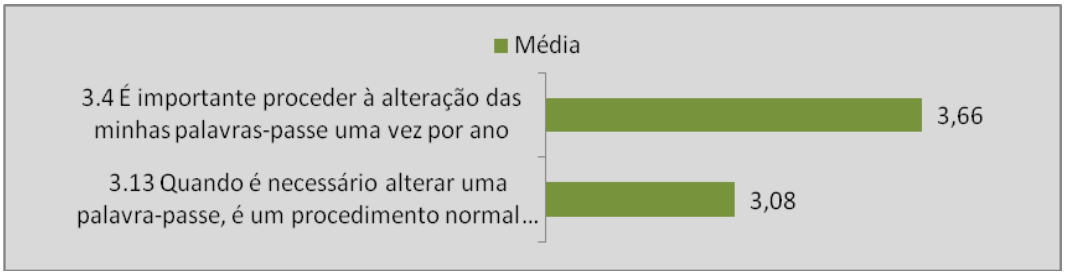

Figura 15 - Questões 3.4 e 3.13: Valor médio das respostas ao procedimento de construção das palavras-passe

Os respondentes revelam ter um comportamento adequado ao não escreverem as suas palavras-passe em papéis, ao memorizarem as mesmas e não as colocarem registadas em papel junto ao computador. Por outro lado, só metade dos utilizadores usa números, letras e caracteres especiais na construção da palavra-passe, o que é um valor baixo; como refere Mamede (2006), os utilizadores na construção das palavras-passe, devem combinar sinais, caracteres e números. Cerca de 40% dos utilizadores usa a mesma palavra-passe para aceder aos diversos programas, o que não é um comportamento considerado correcto, como mencionam Rhee et al (2009), ao referirem que os utilizadores devem usar diferentes palavras-passe para aceder às várias aplicações. Contudo, esta situação é, por vezes, inevitável, pelo facto de algumas organizações integrarem todos os seus sistemas, o que implica que a palavra-passe utilizada nos diferentes sistemas pelo utilizador seja obrigatoriamente a mesma.

Face aos valores obtidos, os utilizadores apresentam comportamentos e atitudes positivas na utilização das palavras-passe, contudo devem melhorar a construção destas com a utilização de números, letras e caracteres especiais em detrimento das fáceis de memorizar.

5.3.5 Encriptação da informação

As figuras a seguir apresentam a distribuição das respostas às questões 2.5 e 2.23, e o valor médio das respostas à questão 3.5, onde os inquiridos eram questionados sobre o envio de informação de forma codificada.

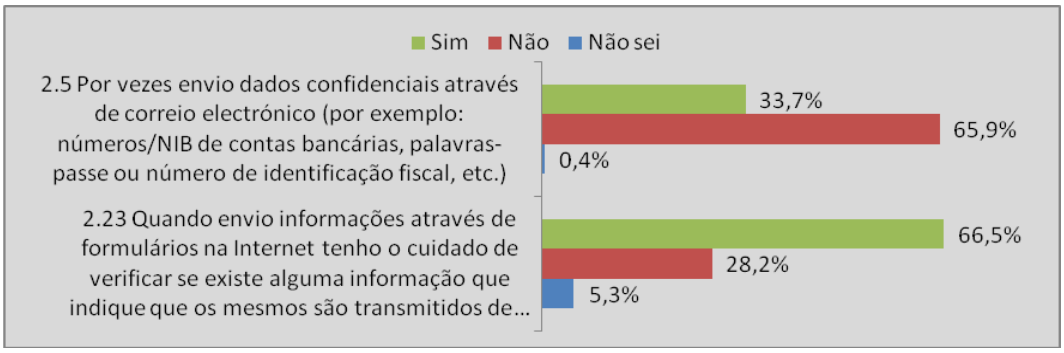

Figura 16 - Questões 2.5 e 2.23: Distribuição das respostas ao procedimento de envio da informação encriptada

Como se pode observar na figura 16, a maioria dos respondentes têm um comportamento que está de acordo com o recomendado, uma vez que não enviam dados confidenciais (65,9%) e têm o cuidado de verificar se os mesmos são enviados de forma codificada (66,5%). No entanto, e uma vez que se trata de informação confidencial, pensamos que os valores deveriam ser mais elevados. Portanto, este comportamento fica aquém do recomendado por Rhee et al. (2009), e coincide com a atitude revelada pelos respondentes. Como pode ser comprovado pela análise da figura 17, a média das respostas é 1,89, ou seja, o valor anda longe do desejável (1,0).

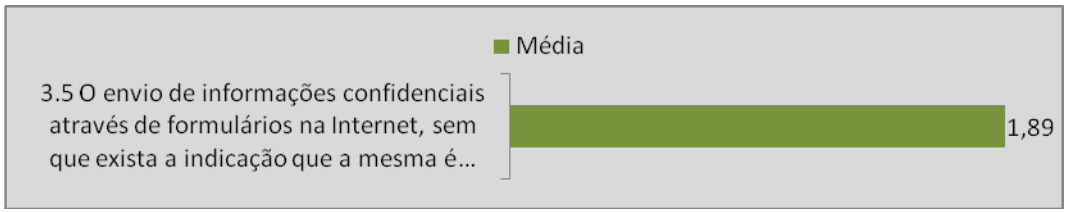

Figura 17 - Questão 3.5: Valor médio das respostas ao procedimento de envio da informação encriptada

De acordo com os dados observados, neste procedimento os utilizadores devem melhorar o seu comportamento e atitude, procurando ser mais prudentes, e verificar se a informação é enviada de forma codificada.

5.3.6 Partilha da informação do computador

Apresentamos, na figura seguinte, a distribuição das respostas às questões 2.6 e 2.22 onde os inquiridos eram questionados sobre a partilha de informação do seu computador com outros utilizadores.

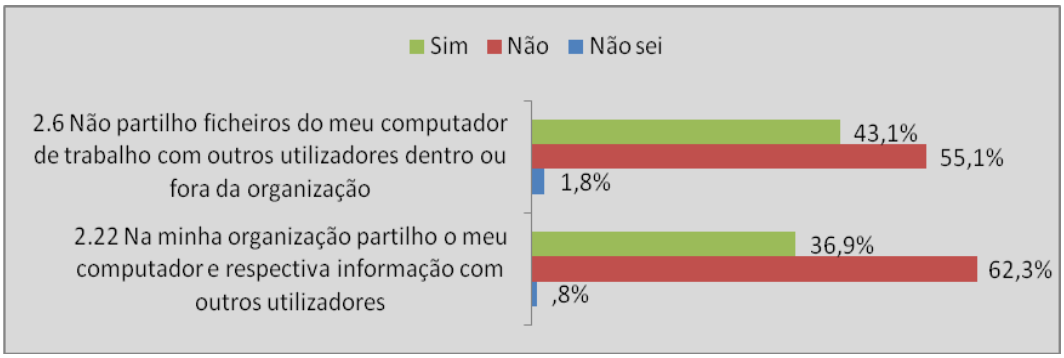

Figura 18 - Questão 2.6 e 2.22: Distribuição das respostas ao procedimento de partilha de informação

Neste procedimento, e segundo o ilustrado na figura 18, mais de metade dos respondentes (55,1%) partilham informação com outros utilizadores. No entanto, este facto é uma inevitabilidade na maioria dos locais de trabalho, pois para realizarem as suas tarefas diárias com sucesso, os utilizadores necessitam de partilhar informação. Os utilizadores referem também (36,9%) que partilham o seu computador e respectiva informação com outros utilizadores, o que pode vir a comprometer a segurança da informação. Neste caso os utilizadores devem ter definidas áreas de trabalho diferentes e ter instalado os mecanismos de protecção adequados, como por exemplo um programa antivírus, e recorrer a estes sempre que necessário para despistar a existência de qualquer ameaça. Face a este cenário, os utilizadores têm que estar cientes do perigo que representam estes comportamentos, devendo ser cautelosos e adoptar as medidas necessárias de modo a garantir a integridade e segurança dos SI, como referem Rhee et al. (2009).

5.3.7 Partilha de palavras-passe

A figura 19 ilustra a distribuição das respostas às questões 2.7 e 2.24, enquanto a figura 20 representa o valor médio das respostas à questão 3.6, onde os inquiridos eram questionados sobre a partilha e divulgação das suas palavras-passe.

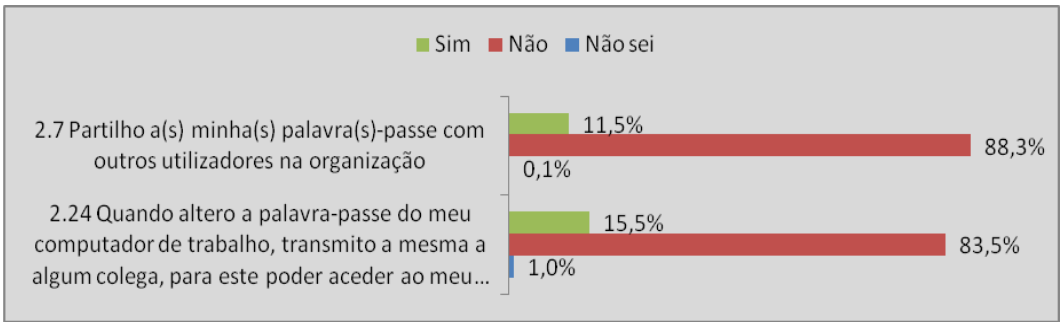

Figura 19 - Questões 2.7 e 2.24: Distribuição das respostas ao procedimento de partilha ou divulgação das palavras-passe

As respostas às questões 2.7 e 2.24 revelam que uma percentagem elevada de utilizadores, 88,3% e 83,5% respectivamente, não partilha e não transmite as suas palavras-passe com outros utilizadores, pelo que neste procedimento os respondentes apresentam um comportamento adequado como referem Rhee et al. (2009).

Da análise da figura 20 podemos visualizar que os respondentes têm uma atitude correcta ao revelarem que não é seguro a partilha das palavras-passe com os colegas de trabalho. Embora os utilizadores revelem ter uma atitude adequada, o valor obtido nesta questão deveria ser a média de 1,0, pelo que fica aqui uma chamada de atenção aos utilizadores, que devem evitar a partilha de palavras-passe com outros utilizadores, como indicam Herath e Rao (2009).

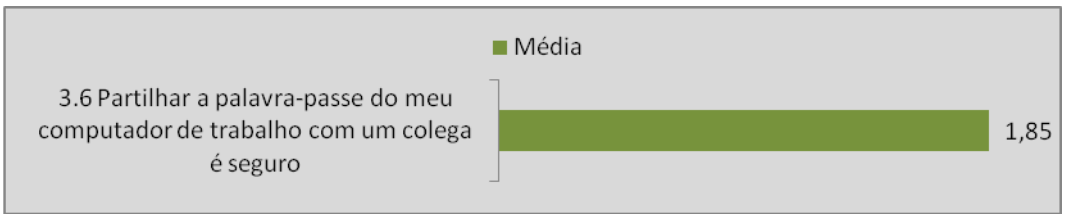

Figura 20 – Questão 3.6: Valor médio das respostas ao procedimento envio de partilha ou divulgação das palavras-passe

Pela observação dos resultados obtidos podemos considerar que neste procedimento os utilizadores apresentam um comportamento e uma atitude de acordo com o recomendado.

5.3.8 Internet e correio electrónico

As figuras a seguir apresentam a distribuição das respostas às questões 2.8, 2.20 e 2.25, e o valor médio das respostas às questões 3.7 e 3.17, onde os inquiridos eram questionados sobre os cuidados na utilização da Internet e do correio electrónico.

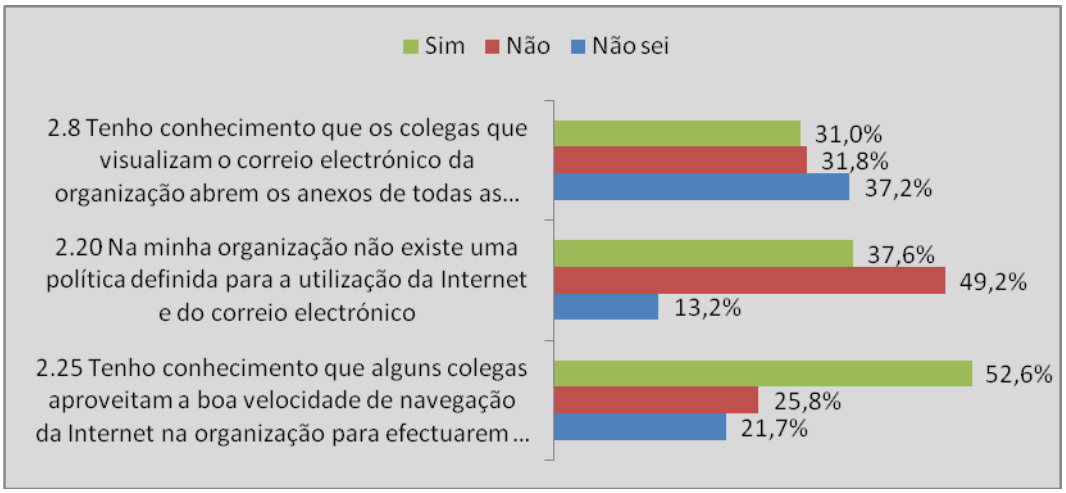

Figura 21 - Questões 2.8, 2.20 e 2.25: Distribuição das respostas ao procedimento de utilização da Internet e correio electrónico

Cerca de 52,6% dos respondentes indica ter conhecimento que alguns colegas utilizam a Internet da organização para assuntos não relacionados com o trabalho, o que é um comportamento que não está de acordo com o recomendado. Por outro lado, mais de metade dos respondentes (49,2% + 13,2%) indica que não existe ou não sabe da existência de uma política definida para a utilização da Internet e correio electrónico, sendo estes os canais que geram maior número de ameaças para os SI, o que revela uma grande falta de sensibilização e cuidado por parte dos responsáveis das organizações onde os respondentes trabalham. Kruger e Kearney (2008) referem que os utilizadores têm que ser responsáveis e cuidadosos na utilização da Internet e do correio electrónico e, para isso, pensamos que também é importante a definição e divulgação, no seio das organizações, de uma política para a utilização da Internet e correio electrónico. Relativamente à questão 2.8, sobre a abertura de todos os anexos das mensagens de correio electrónico, os resultados revelam-se inconclusivos, situando-se as respostas possíveis todas na ordem dos 30%, não nos permitindo deste modo apurar o sentido do comportamento dos utilizadores. Em qualquer dos casos, este é um comportamento que pode ser perigoso para a segurança dos SI/TI.

A análise da figura 22 permite-nos concluir que os respondentes têm uma atitude de acordo com o recomendado, ao reconhecerem a importância de analisar o assunto das mensagens de correio electrónico e enviarem para o lixo as mensagens de remetentes desconhecidos. Ainda relativamente ao envio das mensagens para o lixo de remetentes desconhecidos, pensamos que deve existir um bom senso por parte do utilizador, que após analisar o corpo da mensagem, deve decidir se o conteúdo lhe poderá ser útil e ter interesse, ou se simplesmente é para ignorar e enviar a mensagem de correio electrónico para o lixo.

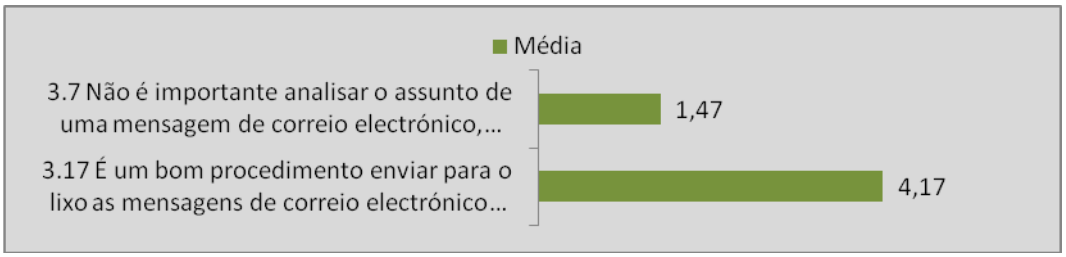

Figura 22 - Questões 3.7 e 3.17: Valor médio das respostas ao procedimento de utilização da Internet e correio electrónico

Face aos resultados obtidos, os respondentes têm uma atitude que está de acordo com o recomendado, mas no que respeita ao comportamento o mesmo não é o mais adequado como mencionam Kruger e Kearney (2008).

5.3.9 Equipamentos de armazenamento externos

Apresentamos, nas figuras seguintes, a distribuição das respostas à questão 2.9 e o valor médio das respostas à questão 3.8, onde os inquiridos eram questionados sobre o uso de equipamento de armazenamento externo.

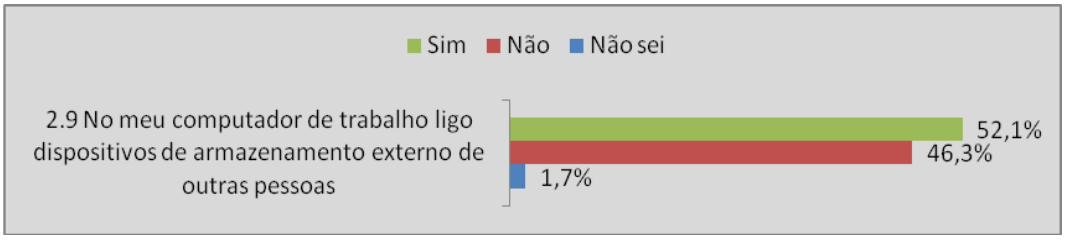

Figura 23- Questão 2.9: Distribuição das respostas ao procedimento de utilização de equipamentos de armazenamento externo

Como se pode observar na figura 23, a maioria os respondentes liga ao seu computador dispositivos de armazenamento externo de outras pessoas, o que não é um comportamento de acordo com o

recomendado, pois, como referem Kruger e Kearney (2008), os utilizadores devem estar sensibilizados e ser cuidadosos na utilização de equipamentos de armazenamento externo. O utilizador sempre que ligar no seu computador um dispositivo de armazenamento externo, em primeiro lugar tem que verificar a existência de vírus no mesmo. Este facto vem reforçar a necessidade de os utilizadores terem instalado e actualizado um programa antivírus no seu computador.

Os respondentes, como se pode comprovar pela figura 24, revelam que guardar informação em dispositivos de armazenamento externo próprios depois de os ligar a outros computadores não é uma atitude prudente, no entanto a média das respostas é 2,75, o que representa um valor longe do desejável (1,0) e recomendado por Kruger e Kearney (2008).

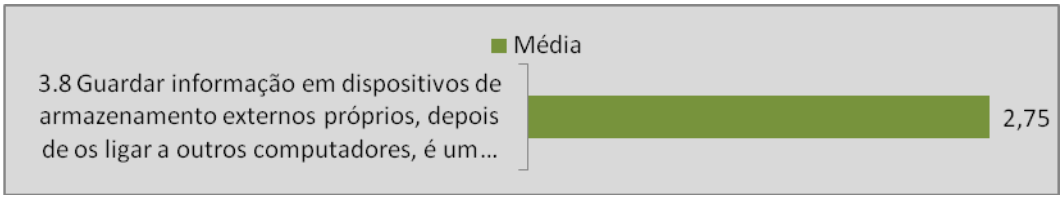

Figura 24 - Questão 3.8: Valor médio das respostas ao procedimento de utilização de equipamentos de armazenamento externo

Neste procedimento os utilizadores revelam ter um comportamento e uma atitude que não estão de acordo com o recomendado, no entanto a utilização dos dispositivos de armazenamento externo para a troca de informação mostra-se necessária no desenvolvimento das suas actividades, pelo que os utilizadores devem estar cientes dos perigos que advém desta situação, devendo utilizar de forma racional e cuidadosa os dispositivos de armazenamento externo.

5.3.10 Incidentes com a informação

A figura 25 ilustra a distribuição das respostas às questões 2.10 e 2.21, enquanto a figura 26 representa o valor médio das respostas à questão 3.14, onde os inquiridos eram questionados sobre o reporte de incidentes.

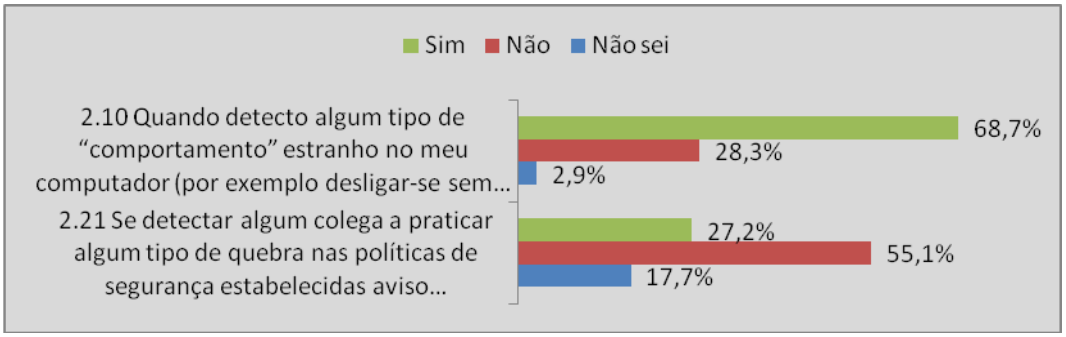

Figura 25 - Questões 2.10 e 2.21: Distribuição das respostas ao procedimento de incidentes com vírus, roubos ou perdas de informação

Cerca de 68,7% dos respondentes revela que se detectar algum tipo de anomalia no seu computador comunicam o sucedido ao seu superior ou responsável pela informática, como pode ser observado na figura 25, o que de acordo com Kruger e Kearney (2008) é um comportamento adequado. A maioria dos utilizadores, 55,1%, indica que se detectar algum colega a quebrar as políticas de segurança estabelecidas não toma a iniciativa de comunicar o sucedido aos superiores, o que é um comportamento não recomendado, no entanto esta situação pode até ser compreensível, uma vez que é complicado e difícil denunciar um colega de trabalho. De qualquer forma, os utilizadores têm que ter consciência da perigosidade que esta situação representa para os SI da organização e adoptar o comportamento correcto, comunicando a situação aos superiores.

De acordo com o observado na figura 26, o valor médio das respostas é de 1,81, o que pode ser entendido como uma atitude correcta dos utilizadores ao reconhecerem que é necessário informar os superiores se detectarem algum comportamento estranho no seu computador, no entanto este valor deveria ser mais próximo de 1,0, pelo que fica aqui a chamada de atenção aos utilizadores para a necessidade de informar sempre os seus superiores caso detectem alguma anomalia no seu computador.

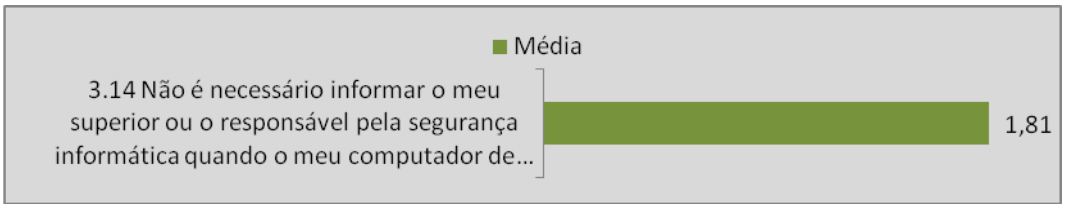

Figura 26 – Questão 3.14: Valor médio das respostas ao procedimento de incidentes com vírus, roubos ou perdas de informação

Segundo os resultados obtidos, neste procedimento os respondentes apresentam um comportamento correcto, no entanto devem ter sempre em mente que têm que comunicar qualquer anomalia, mesmo

no caso de esta ser provocada por algum colega. Os respondentes têm também neste procedimento uma atitude adequada.

5.3.11 Consciência dos actos praticados

As figuras a seguir apresentam a distribuição das respostas às questões 2.12 e 2.27, e o valor médio das respostas às questões 3.9 e 3.15, onde os inquiridos eram questionados sobre as consequências dos seus actos.

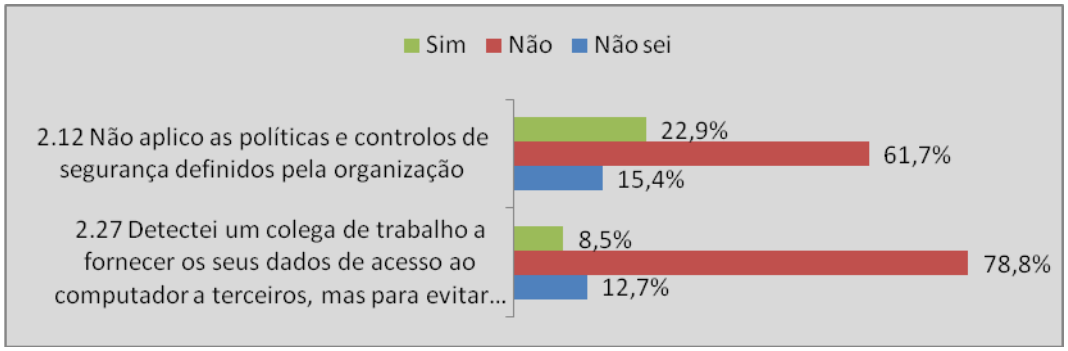

Figura 27 - Questões 2.10 e 2.21: Distribuição das respostas ao procedimento estar ciente que os actos praticados têm consequências

Segundo o ilustrado na figura 27, 61,7%, dos respondentes revela que aplica as políticas e controlos de segurança definidos pela organização, o que é um comportamento adequado segundo Kruger e Kearney (2008). Embora o resultado obtido nesta questão seja positivo, fica um pouco aquém do valor desejável, 100%, ou seja, os utilizadores devem ter em mente que têm que aplicar sempre as políticas e controlos de segurança definidos pela organização. Por outro lado, 78,8%, dos respondentes indica que se detectar algum colega a fornecer os seus dados de acesso ao computador a terceiros não ignora a situação, o que é um comportamento correcto, e que demonstra que os utilizadores estão cientes das consequências nefastas que esta situação pode causar aos SI da organização.

A maioria dos respondentes tem uma atitude que está de acordo com o recomendado, ao reconhecerem a importância de a organização lhes apresentar através de um documento escrito as políticas de segurança e das formações sobre as políticas de segurança, como se pode comprovar pela figura 28.

Figura 28 - Questões 3.9 e 3.15: Valor médio das respostas ao procedimento estar ciente que os actos praticados têm consequências

Face aos resultados obtidos neste procedimento, os respondentes apresentam um comportamento e atitudes de acordo com o recomendado.

5.3.12 Utilização de *Firewall*

Apresentamos, nas figuras seguintes, a distribuição das respostas à questão 2.13 e o valor médio das respostas à questão 3.10, onde os inquiridos eram questionados sobre a utilização de *Firewall*.

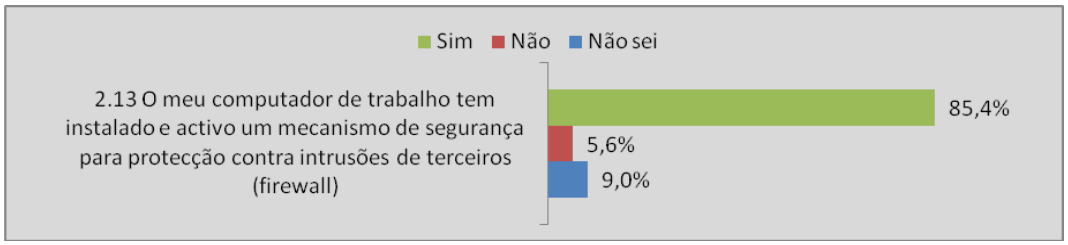

Figura 29 - Questão 2.13: Distribuição das respostas ao procedimento de utilização de *firewall*

Os respondentes, 85,4%, indicam que têm instalado e activo um mecanismo de segurança contra terceiros, como se pode observar na figura 29, o que é um comportamento de acordo com o recomendado.

Reconhecem também, como se pode visualizar na figura 30, a importância da utilização de *software* antivírus e contra a intrusão de terceiros (*firewall*) pela organização, o que revela uma atitude correcta.

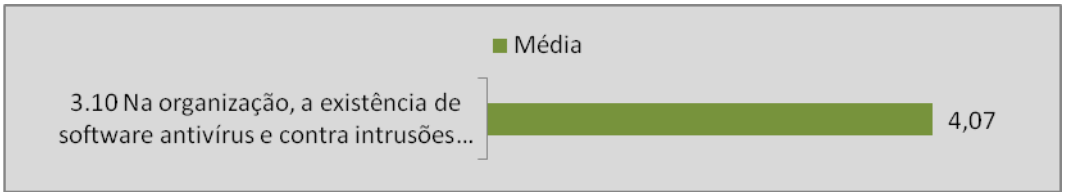

Figura 30 - Questão 3.10: Valor médio das respostas ao procedimento de utilização de *firewall*

De acordo com os resultados obtidos, fica comprovado que os utilizadores têm instalado e activo no seu computador um mecanismo contra a intrusão de terceiros e reconhecem a sua importância como sinónimo de segurança para a organização, o que é um comportamento e atitude que está de acordo com o proferido por Workman et al. (2008).

5.3.13 Bloqueio do computador

A figura 31 ilustra a distribuição das respostas à questão 2.14 e a figura 32 o valor médio das respostas à questão 3.11, onde os inquiridos eram questionados sobre o bloqueio do computador quando se ausentam.

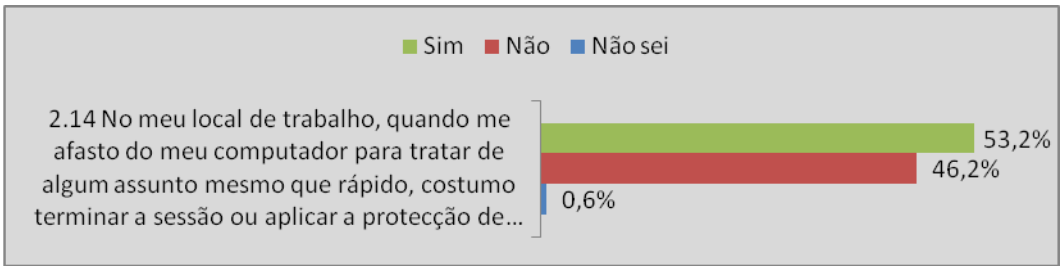

Figura 31 - Questão 2.14: Distribuição das respostas ao procedimento bloqueio do computador quando se ausenta

Como se pode observar na figura 31, só 53,2%, dos respondentes é que termina a sessão ou aplica protecção de ecrã quando se afasta do seu computador. Este valor embora positivo, está longe do desejável, que deveria rondar os 100%, pelo que neste procedimento os utilizadores apresentam um comportamento ainda longe do recomendado por Albrechtsen (2007).

A análise da figura 32, revela que os respondentes não estão a ter uma atitude de acordo com o recomendado pois 2,75 de média das respostas, indicam que não existe qualquer risco em deixar o computador ligado quando se afastam do mesmo.

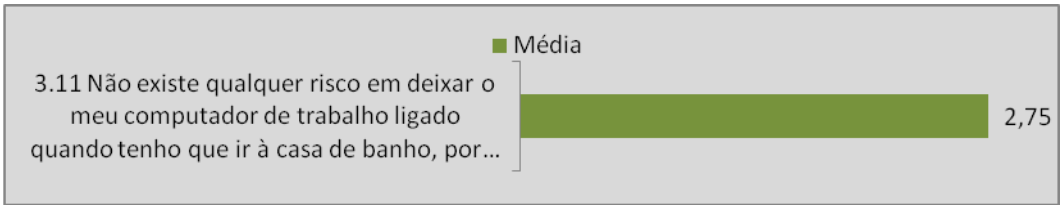

Figura 32 - Questões 3.11: Valor médio das respostas ao procedimento bloqueio do computador quando se ausenta

Face a estes resultados, fica comprovado que neste procedimento os utilizadores devem rever e adequar o seu comportamento e atitude, bloqueando o computador quando se ausentam, como menciona Albrechtsen (2007).

5.3.14 Utilização de *software* ilegal

As figuras a seguir apresentam a distribuição das respostas à questão 2.15 e o valor médio das respostas à questão 3.16, onde os inquiridos eram questionados sobre a utilização de *software* ilegal ou de partilha de ficheiros.

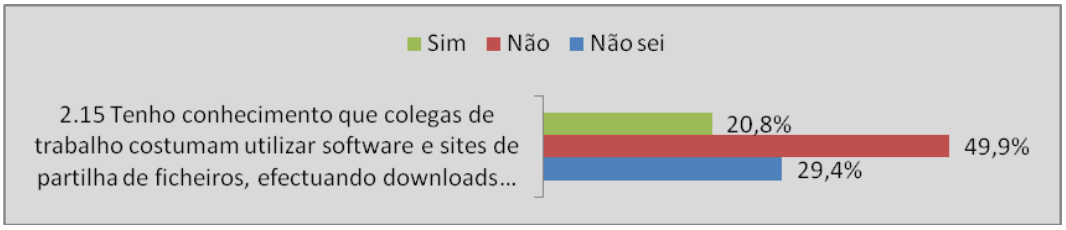

Figura 33 - Questão 2.15: Distribuição das respostas ao procedimento não utilização de *software* ilegal

Só cerca de metade dos respondentes, 49,9%, indicam que os colegas de trabalho não utilizam *software* e sites de partilha de ficheiros, como se pode visualizar na figura 33, o que é um resultado manifestamente baixo, devido ao risco que este tipo de *software* representa para a segurança dos SI na organização. Perante este resultado, podemos afirmar que os utilizadores adoptam um comportamento que não está de acordo com o recomendado.

De acordo com o observado na figura 34, os respondentes têm uma atitude correcta ao reconhecerem que a utilização da Internet na organização para efectuar *download* de filmes e jogos representa uma ameaça para a segurança do SI.

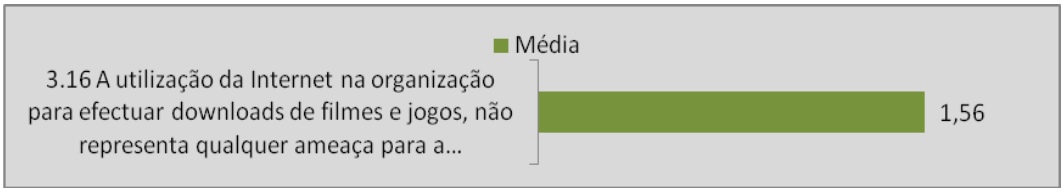

Figura 34 - Questões 3.16: Valor médio das respostas ao procedimento não utilização de *software* ilegal

Pela observação dos resultados obtidos, os utilizadores têm que ter consciência do perigo da utilização deste tipo de *software*, e adequar os seu comportamentos de acordo com o recomendado para não colocar em risco a segurança dos SI nas organizações, como refere Albrechtsen (2007).

5.4 Comentários ou Sugestões

Foram efectuados pelos inquiridos 118 comentários ou sugestões na questão 4. Esta questão tinha como principal objectivo obter contributos adicionais por parte dos inquiridos sobre os comportamentos e atitudes dos utilizadores dos SI/TI das organizações.

Destacamos apenas alguns comentários considerados pertinentes e que reforçam a importância do desenvolvimento deste trabalho:

"É importante a formação dentro da organização aos elementos que potencialmente venham a explorar um software ou sistemas da mesma." (Anónimo)

"Considero este tipo de estudos de extrema importância…. No entanto, existe um controle muito fraco em termos de verificação do correcto uso dos computadores e seus sistemas de informação, nomeadamente a internet, nos locais de trabalho e em horas de expediente…" (Anónimo)

"Na minha opinião a maioria dos utilizadores constitui-se como factor de risco no que diz respeito à utilização das tecnologias de informação, nomeadamente, o uso do computador e de programas não autorizados..." (Anónimo)

"A partilha de passwords na empresa onde trabalho é necessária porque existem contas de e-mail por exemplo por secção e não individuais, no entanto discordo completamente deste modo de funcionamento." (Anónimo)

"Não existe política de utilização de equipamentos informáticos na organização onde trabalho e todos os computadores são partilhados." (Anónimo)

"Falta nas organizações muita formação sobre a segurança informática, é por vezes ignorada como se trata-se de um sector sem importância, nos dias de hoje é exactamente o contrário." (Anónimo)

"Deveríamos receber regras de utilização segura dos computadores por parte da organização para que haja uniformização de procedimentos." (Anónimo)

Como referido, não foi efectuada qualquer análise aos dados obtidos através desta questão. No entanto, como se pode observar alguns dos cometários proferidos pelos respondentes vêm confirmar alguns dos resultados obtidos no estudo, nomeadamente:

- quando referem a importância de ser definida uma política de segurança pela organização bem como a formação sobre esta;

- sobre ausência de uma política de utilização e partilha dos computadores no seio da organização;
- a definição de regras de utilização da Internet dentro da organização durante o horário de trabalho.

6. Considerações finais

Segundo Freixo (2009), este ponto representa o final da pesquisa efectuada, e ao mesmo tempo, o começo de novas dúvidas, indicações e abertura de novas pesquisas.

Este trabalho procurou investigar se os comportamentos e as atitudes dos utilizadores representam um risco ou uma protecção para a segurança dos SI nas organizações. Neste ponto são apresentadas as conclusões e os contributos deste estudo, tendo por base a revisão da literatura, os resultados obtidos pela recolha dos dados no questionário, sempre em consonância com os objectivos do estudo.

São também aqui identificadas algumas limitações a este estudo, que por sua vez podem potenciar futuras investigações sobre os utilizadores e a segurança da informação nos SI das organizações.

6.1 Conclusões do estudo

Este estudo tinha como objectivo principal averiguar se os comportamentos e as atitudes dos utilizadores constituem um risco ou uma protecção para a segurança dos SI nas organizações.

Segundo Workman et al. (2008), a principal ameaça à segurança é a falta de consciencialização dos utilizadores para esta questão, uma vez que existem medidas de segurança disponíveis que podem ser aplicadas, mas estes ignoram-nas deixando que sejam provocados ataques e violações à segurança dos SI nas organizações.

A recolha dos dados deste estudo permitiu concluir que, de uma forma geral, os utilizadores apresentam-se como uma protecção para a segurança da informação nos SI das organizações, pelo facto de assumirem comportamentos e atitudes correctas na maioria dos procedimentos identificados na revisão da literatura. Apresentamos a seguir os aspectos positivos e negativos obtidos pela análise dos dados relativamente à actuação dos utilizadores, de acordo, ou não, com o recomendado e que nos permitiu chegar à conclusão final.

Aspectos positivos nos comportamentos e atitudes dos utilizadores de SI nas organizações:

- Aplicam as actualizações de segurança recomendadas;
- Utilizam e actualizam com frequência os programas antivírus *e antispyware*;
- Realizam cópias de segurança com regularidade;
- Utilizam palavras-passe diferentes em cada aplicação;
- Procuram enviar / transferir a sua informação de forma encriptada;

- Não partilham o seu computador com outros;
- Não partilham ou divulgam as suas palavras-passe com os outros;
- Informam no caso de incidentes com vírus, roubos ou perdas de informação;
- Estão cientes que todos os actos praticados têm consequências;
- Utilizam uma *Firewal*;

Aspectos negativos nos comportamentos e atitudes dos utilizadores:

- A maioria já foi infectada por vírus;
- Optam por palavras-passe fáceis de memorizar em detrimento das de construção robusta;
- Utilizam a Internet na organização não só para fins profissionais;
- Ligam dispositivos de armazenamento externo de outras pessoas;
- Não bloqueiam o seu computador quando se ausentam.

Para que o objectivo principal deste estudo fosse atingido existiu um subconjunto de objectivos específicos, representando pequenos passos na concretização do objectivo geral.

O primeiro objectivo específico deste trabalho consistia em **identificar e descrever, com base na literatura, os procedimentos de segurança que os utilizadores das TIC devem adoptar para garantir a segurança dos SI**. Para o alcançar foi efectuado um enquadramento teórico, onde foram descritos os principais conceitos relacionados com a segurança da informação e com os utilizadores, de modo a encontrar uma fundamentação para a problemática em questão, como pode ser observado no capítulo 2. Este primeiro enquadramento permitiu-nos ir de encontro às principais políticas e procedimentos de segurança, que após a consulta da literatura foram identificados no capítulo 3 os seguintes procedimentos que os utilizadores devem adoptar:

- Aplicar as actualizações de segurança recomendadas;
- Utilizar e actualizar com frequência os programas antivírus e *anti-spyware*;
- Realizar cópias de segurança com regularidade;
- Utilizar palavras-passe robustas e diferentes em cada aplicação;
- Procurar enviar / transferir a sua informação de forma encriptada;
- Não partilhar a informação do seu computador com outros;

- Não partilhar ou divulgar as suas palavras-passe com os outros;
- Ser responsável e cuidadoso na utilização da Internet e do correio electrónico;
- Ser cuidadoso na utilização de equipamentos de armazenamento externos;
- Informar no caso de incidentes com vírus, roubos ou perdas de informação;
- Estar ciente que todos os actos praticados têm consequências;
- Utilizar uma *Firewall*;
- Bloquear o computador quando se ausenta;
- Não utilizar *software* ilegal ou de partilha de ficheiros.

A identificação deste conjunto de procedimentos foi essencial para a consecução do segundo objectivo específico que era **construir e aplicar um questionário sobre a segurança dos SI junto de utilizadores das organizações que utilizam as TIC**. Com base nos procedimentos de segurança identificados foi construído um questionário contendo 3 grupos de questões. O primeiro grupo era constituído por 3 questões, a primeira questão tinha como função servir de filtro para identificar quais os respondentes que cumprem os requisitos para preencher a totalidade do questionário. A segunda questão continha um conjunto de 27 alíneas construídas com base nos procedimentos de segurança identificados na revisão da literatura, em que o respondente tinha que escolher qual a opção que melhor caracterizava a sua opinião. A terceira questão tinha um conjunto de 18 afirmações também construídas com base nos procedimentos de segurança identificados na revisão da literatura, em que o respondente tinha que escolher qual o seu grau de concordância ou discordância segundo a escala não comparativa de Likert de 1 a 5. O segundo grupo era composto por uma questão, destinada a registar comentários ou sugestões, não sendo obrigatório o seu preenchimento. No último grupo de questões eram solicitados os dados de caracterização dos respondentes. Foi construído um sítio *Web* com o objectivo de recolher as respostas ao questionário *on-line* e assim conseguir o maior número de participantes possíveis.

Os dados recolhidos através do questionário permitiram atingir o terceiro objectivo que **era analisar os resultados obtidos através do questionário, para verificar se o comportamento e as atitudes dos utilizadores constituem um risco ou uma protecção para a segurança dos SI nas organizações**. Da análise dos dados chegou-se à conclusão que os utilizadores, de um modo geral, constituem uma protecção para os SI das organizações, uma vez que adoptam a maioria dos procedimentos de segurança identificados.

A análise dos dados recolhidos possibilitou também a consecução do último objectivo específico que era **apresentar um conjunto de recomendações que os utilizadores de TIC nas organizações podem adoptar para melhorar a segurança dos SI**. Com base no observado na análise dos dados existem alguns procedimentos em que os utilizadores ainda não procedem de acordo com as boas práticas identificadas na literatura, e que, no pior dos cenários, pode vir a constituir uma ameaça para a segurança dos SI nas organizações. As recomendações aqui apresentadas são pistas genéricas, que os utilizadores podem aproveitar para alinharem alguns dos seus comportamentos e atitudes no sentido de aumentarem a segurança do SI. As atitudes ou os comportamentos que os utilizadores devem ajustar são os seguintes:

- Ter cuidado com os vírus e *spyware*: como referido pelos próprios utilizadores, 71,8% já foi infectado por vírus, sendo estes uma das grandes ameaças à segurança da informação, pelo que devem ter todo o cuidado quando navegam na Internet, efectuam *download* de ficheiros, abrem mensagens de correio electrónico ou ligam dispositivos de armazenamento externo, pois são estas as principais formas de propagação dos vírus. E devem também certificar-se que têm instalado e actualizado no seu computador um *software* antivírus, *anti-spyware* e uma *firewall*.

- Utilização de palavras-passe robustas: 49,6% dos utilizadores referem que não utiliza a conjugação de letras, números e caracteres especiais na construção das suas palavras-passe, optando por uma fácil de memorizar, pelo que devem efectuar um esforço e aplicar as regras referidas na construção das suas palavras-passe, para que estas sejam robustas, proceder à sua mudança anualmente e não as partilhar com terceiros.

- Ter atenção na partilha de ficheiros com outros utilizadores: segundo o estudo, 55,1% dos respondentes partilha ficheiros com outros utilizadores. Embora a partilha de ficheiros seja necessária para a consecução das actividades do dia-a-dia, os utilizadores devem ter todo o cuidado na partilha destes e rejeitar todos os ficheiros de origem desconhecida ou não fidedigna. Verificar sempre através da análise do antivírus os ficheiros recebidos de outros utilizadores. Uma boa prática passa também pela utilização do correio electrónico para trocar ficheiros com outros utilizadores, isto pelo facto de a informação que é enviada através desta via, ser sujeita a verificação por parte dos antivírus instalados nos servidores de correio electrónico.

- Ser cuidadoso na utilização da Internet e do correio electrónico: a maioria dos utilizadores, 52,6%, indica que tem conhecimento que outros utilizadores usam a Internet na organização

sem ser para fins profissionais. A Internet apresenta-se como um meio de comunicação e de acesso à informação dos mais variados tipos e géneros, pelo que é necessário estar atento aos sites que se visitam, procurar sempre navegar ou procurar informação em sites com alguma fidedignidade / credibilidade, sob pena de poder ser infectado por algum vírus ou outro tipo de *software* malicioso e, como consequência, provocar danos nos SI das organizações. Ter atenção às mensagens que recebem, analisar em primeiro lugar o assunto e o emissor, e caso este seja de origem estranha a opção deverá ser a eliminação da mensagem.

- Cuidado na utilização de equipamentos de armazenamento externo: 52,1% dos respondentes liga dispositivos externos de outras pessoas no seu computador de trabalho, o que representa um perigo, não sendo possível determinar antecipadamente se o dispositivo já esteve ligado em algum computador infectado com vírus e se se encontra infectado; mesmo que possuam antivírus instalados e actualizados é sempre um risco, pelo facto de existirem diversas e cada vez mais sofisticadas formas de o *software* malicioso se introduzir nos SI/TI e provocar danos. Uma boa prática, como referido anteriormente, passa pela utilização do correio electrónico; se não existir outra alternativa procurar certificar-se que o dispositivo não contém vírus ou qualquer outro tipo de *software* malicioso efectuando uma análise do mesmo com o antivírus.
- Cópias de segurança: sempre que possível efectuar cópias de segurança da informação do computador, ou para uma partilha na rede da organização, ou para um CD/DVD, ou um disco externo. Neste dois últimos casos, devem ser guardados num local diferente da localização do computador.
- Bloquear ou terminar a sessão no seu computador sempre que se ausenta: sempre que abandona o seu posto de trabalho, mesmo que por pouco tempo, deve proceder-se ao bloqueio do mesmo, pois um utilizador com segundas intenções, mesmo um colega de trabalho, pode aproveitar para roubar algum tipo de informação ou provocar algum tipo de dano nos SI da organização.
- Aplicar as políticas de segurança definidas pela organização: só pouco mais de metade dos utilizadores aplica as políticas de segurança definidas pela organização, o que é um valor manifestamente baixo. As políticas de segurança têm como objectivo a protecção dos SI das organizações contra as diversas ameaças e ataques, pelo que os utilizadores têm que ter

consciência desta situação e adequar o seu comportamento, e aplicar as mesmas para não colocar em risco a segurança dos SI.

Ter sempre em mente que a organização está dependente dos seus SI para realizar as suas actividades diárias, pelo que mais uma vez se reforça o que foi referido ao longo deste trabalho, os utilizadores são um dos elementos que podem provocar danos na segurança dos SI, pelo que devem estar conscientes que os seus comportamentos e atitudes têm consequências e devem ser ajustados de acordo com os procedimentos identificados e as políticas definidas pela organização.

6.2 Limitações do estudo

Todos os trabalhos desta natureza têm limitações e este estudo não foge à regra. A principal prende-se com o facto de se ter utilizado uma amostra não probabilística por conveniência, pelo que os resultados e as conclusões só se aplicam à amostra, não podem ser extrapolados para o universo. Isto porque não há garantia que a amostra seja razoavelmente representativa do universo, uma vez que não se conhece o tamanho do universo em questão, por não se encontrar registado.

Outra limitação encontrada durante o desenvolvimento do trabalho foi a escassez de estudos sobre os comportamentos e atitudes dos utilizadores na segurança dos SI nas organizações, para se poder efectuar algum tipo de comparação com o estudo em causa.

Também o questionário *on-line* se apresenta como uma limitação, pelo facto de não estar disponível para todas as pessoas, umas devido à política de utilização da Internet na organização, outros pelo facto de a mensagem não ser distribuída pelos utilizadores na organização e ser descartada no endereço geral de correio electrónico das mesmas.

O envio da mensagem de divulgação do questionário através de correio electrónico também se mostrou uma limitação devido ao facto de apenas poderem ser enviadas 500 mensagem de correio electrónico por dia, sob pena de ser considerada spam e sofrer sanções, nomeadamente a conta de correio electrónica ficar bloqueada durante alguns dias.

Por último, o facto de 70,3% dos respondentes serem trabalhadores por conta de outrem no sector público e 61,7% pertencerem em termos de sector de actividade à Educação. Esta situação ficou a dever-se ao facto de ser o sector onde tínhamos um maior relacionamento e número de contactos, e como o método de divulgação foi do tipo “corrente”, acabou por resultar numa maior participação por parte da comunidade académica.

6.3 Recomendações para trabalhos futuros

O desenvolvimento deste trabalho procurou verificar se os utilizadores têm consciência que as suas atitudes e comportamentos influenciam a segurança dos SI nas organizações. Existem certamente outro tipo de abordagens a este tema, pelo que se abrem portas a novos tipos de investigação.

Uma das opções, e aceitando a sugestão de um dos inquiridos, seria acrescentar uma variável denominada grupo profissional para visualizar a distribuição dos respondentes pelas diversas categorias profissionais de modo a identificar qual ou quais os grupos que representam um factor maior de risco ou protecção para a segurança dos SI nas organizações.

Outra opção de trabalho passa por efectuar o cruzamento de algumas variáveis de caracterização do questionário, e efectuar a sua comparação em termos de atitudes e comportamentos para observar se existem diferenças entre:

- Organizações do sector público com as do sector privado;
- Distritos com maior densidade populacional versus distritos com menor densidade;
- Organizações de pequena dimensão versus organizações de média ou grande dimensão.

Uma outra possibilidade de estudo passa por inserir uma nova variável de caracterização das organizações denominada "existência de uma política de segurança definida e implementada", para ser possível comparar e verificar se os comportamentos e atitudes dos utilizadores são iguais ou não nas organizações com políticas de segurança definidas e nas que não têm políticas de segurança.

A última opção, passa por utilizar um tipo de amostra diferente (probabilística de preferência), de modo a que os resultados obtidos possam ser mais representativos da população em estudo.

Bibliografia

ALBRECHTSEN, Eirik - *A qualitative study of users' view on information security*. Computers & Security. ISSN 0167-4048. Vol. 26, nº 4 (2007) p. 276 – 289;

ALBRECHTSEN, Eirik; HOVDEN, Jan - *The information security digital divide between information security managers and users*. Computers & Security. ISSN 0167-4048. Vol. 28, nº 6 (2009) p. 476 – 490;

ARBAUGH, William A.; FITHEN, William L.; MCHUGH, John - *Windows of vulnerability: a case study analysis*. IEEE Computer Society. ISSN: 0018-9162. Vol.33, nº 12 (2000) p. 52- 59;

ARCY, John D'; HOVAV, Anat; GALLETTA, Dennis – *User Awareness of security countermeasures and its impact on information system misuse: a deterrence approach*. Information Systems Research. ISSN: 1047 – 7047. Vol. 28, nº 1 (2009) p. 79 – 98;

BS - *British Standards*. [Consult. 03 de Nov. 2009]. Disponível na WWW:<URL:http://www. standardsuk.com/>;

CARNEIRO, Alberto – *Introdução à segurança dos sistemas de informação*. Lisboa: FCA, 2002. ISBN 972-722-315-X;

CHOO, Chun Wei - *Gestão de informação para a organização inteligente: a arte de explorar o meio ambiente*. Lisboa: Caminho, 2003. ISBN 972-21-1506-5;

Decreto-Lei 252/94 de 20 de Outubro de 1994. Diário da República nº 243 – I Série –A. Presidência Conselho Ministros. Lisboa;

DHILLON, Gurpreet; BACKHOUS, James - *Information System Security Management in the New Millennium*. Communications of the ACM. Vol. 43, Nº 7 (2000) p. 125 - 128;

DHILLON, Gurpreet - *Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns*. Computers & Security. ISSN 0167-4048. Vol. 20, nº 2 (2001) p. 165 – 172;

DHILLON, Gurpreet - *Realizing benefits of an information security program*. Business Process Management Journal. Vol. 10, nº 3 (2004) p. 260-261;

DHILLON, Gurpreet - *Gaining benefits from IS/IT implementation: Interpretations from case studies*. International Journal of Information Management. ISSN 0268-4012. Vol. 25, nº 6 (2005) p. 502-515;

DHILLON, Gurpreet - *Organizational competence for harnessing IT: A case study*. Information & Management. ISSN 0378-7206. Vol. 45, nº 5 (2008) p. 297-303;

DLAMINI, M.T.; ELOFF, J.H.P.; ELOFF, M.M. - *Information security: The moving target*. Computers & Security. ISSN 0167-4048. Vol. 28, nº 3-4 (2009) p. 189 – 198;

FREIXO, Manuel João Vaz – *Metodologia Científica*. Lisboa: Instituto Piaget, 2009. ISBN: 978-989-659-020-8;

FURNELL, Steven; THOMSON, Kerry-Lynn - *From culture to disobedience: Recognising the varying user acceptance of IT security*. Computer Fraud & Security. ISSN 1361-3723. Vol. 2009, nº 2 (2009) p. 5 – 10;

GAIVÉO, José Manuel - *As Pessoas nos Sistemas de Gestão da Segurança da Informação*. 2008. Acessível em http://repositorioaberto.univ-ab.pt/handle/10400.2/1272;

GODWIN, Thomas; REINHARDT, A. Botha - Secure Mobile Device Use in Healthcare Guidance from HIPAA and ISO17799. Information Systems Management. ISSN: 1058 – 0530. Vol. 24, nº 4 (2007) p. 333 – 342.

HERATH, Tejaswini; RAO, H.R. - *Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness*. Decision Support Systems. ISSN 0167-9236. Vol. 47, nº 2 (2009) p. 154 – 165;

HILL, Manuela Magalhães; Hill, Andrew – *Investigação por Questionário*. Lisboa: Sílabo, 2005. ISBN 972-618-273-5;

INE – *Instituto Nacional de Estatística – Estatísticas do Emprego – 1º trimestre de 2011*. [Consult. 17 Jul. 2011]. Disponível na WWW:<URL: http://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=109726964&PUBLICACOESmodo=2>;

INE – *Instituto Nacional de Estatística – Empresas e Portugal - 2009*. [Consult. 20 Jul. 2011]. Disponível na WWW:<URL: http://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=116399684&PUBLICACOESmodo=2>;

ISO – *International Organization for Standardization*. [Consult. 02 Nov. 2009]. Disponível na WWW:<URL:http://www.iso.org>;

ISECT - *ISO/IEC 27001:2005 Information technology - Security techniques - Specification for an Information Security Management System*. [Consult. 29 Junho

2010]. Disponível na WWW:<URL: http://www.iso27001security.com/html/27001.html >;

ISECT - *ISO/IEC 27002:2005 Information technology - Security techniques - Code of Practice for Information Security Management*. [Consult. 29 Junho 2010]. Disponível na WWW:<URL http://www.iso27001security.com/html/27002.html>;

ISECT - *ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management*. [Consult. 29 Junho 2010]. Disponível na WWW:<URL http://www.iso27001security.com/html/27005.html>;

KNAPP, Kenneth J.; MORRIS, R. Franklin Jr.; MARSHALL, Thomas E.; BYRD, Terry Anthony - *Information security policy: An organizational-level process model*. Computers & Security. ISSN 0167-4048. Vol. 28, nº 7 (2009) p. 493-508;

KRUGER, H.A.; KEARNEY, W.D. - *A prototype for assessing information security awareness*. Computers & Security. ISSN 0167-4048. Vol. 25, nº 4 (2006) p. 289-296;

KRUGER, H.A.; KEARNEY, W.D. - *Consensus ranking - An ICT security awareness case study*. Computers & Security. ISSN 0167-4048. Vol 27, nº 7 (2008) p. 254 – 259;

KRUGER, H.A.; DREVIN, L.; STEYN, T. - *A Framework for evaluating ICT security awareness*. [Consult. 07 Maio 2010]. Disponível na WWW: <URL: http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/17_Paper.pdf>;

LAUDON, Kenneth C.; LAUDON, Jane P. - *Management information systems: managing the digital firm*. 10 th ed. Upper Saddle River : Prentice Hall, 2007. ISBN 0-13-230461-9;

LEACH, John - *Improving user security behaviour*. Computers & Security. ISSN 0167-4048. Vol. 22, nº 8 (2003) p. 685 – 692;

Lei nº 109/91 de 17 de Agosto de 1991. Diário da República nº188 - I Série-A. Assembleia da Republica. Lisboa;

Lei nº 67/98 de 26 de Outubro de 1998. Diário da República nº247 - I Série-A. Assembleia da Republica. Lisboa;

Lei nº 41/2004 de 18 de Agosto de 2004. Diário da República nº194 - I Série-A. Assembleia da Republica. Lisboa;

MAMEDE, Henrique São – *Segurança informática nas organizações*. Lisboa: FCA, 2006. ISBN 13: 978-972-722-411-8;

MISHRA, Sushma; DHILLON, Gurpreet – *Defining internal control objectives for information systems security: a value focused assessment*. [Consult. 03 Junho 2010]. Disponível na WWW: <URL: http://is2.lse.ac.uk/asp/aspecis/20080113.pdf>;

MUKHERJI, Ananda - *The evolution of information systems: Their impact on organizations and structures*. Management Decision. ISSN 0025-1747. Vol. 40, nº 5 (2002) p. 497 – 597;

NG., Boon-Yuen; KANKANHALLI, Atreyi; XU, Yunjie (Calvin) - *Studying users' computer security behavior: A health belief perspective, Decision*. Decision Support Systems. ISSN 0167-9236. Vol. 46, nº 5 (2009) p. 815 – 825;

PESTANA, Maria Helena; GAGEIRO, João Nunes – *Análise de dados para Ciências Sociais – A Complementaridade do SPSS*. Lisboa: Edições Sílabo, 2008. ISBN 978-972-618-498-0;

POST, Gerald V.; KANGAN, Albert - Evaluating information security tradeoffs: Restricting access can interfere with user tasks. Computers & Security. ISSN 0167-4048. Vol. 26, nº 3 (2007) p. 229 – 237;

RHEE, H-S; KIM C; RYU YU - *Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior*. Computers & Security. ISSN 0167-4048. Vol. 28 (2009) p. 816 - 826;

RODRIGUES, Luís Silva - *Arquitecturas dos sistemas de informação*. Lisboa: FCA, 2002. ISBN 972-722-316-8;

SANTOS, Luís – *Factores de sucesso na gestão de segurança da informação nas empresas Portuguesas*. [Consult. 29 Jun. 2010]. Disponível na WWW:URL:<http:// myluissantos.googlepages.com/Factores_de_Sucesso_na_Gesto_de_Segu.pdf>

SERRANO, António; CALDEIRA, Mário; GUERREIRO, António - *Gestão de sistemas e tecnologias de informação*. Lisboa: FCA, 2004. ISBN 972-722-409-1;

SERRANO, António; FIALHO, Cândido - *Gestão do conhecimento: O novo paradigma das organizações*. Lisboa : FCA, 2005. ISBN 978-972-722-484-5;

SERRANO, António; JARDIM, Nuno - *Disaster recovery: um paradigma na gestão do conhecimento*. Lisboa: FCA, 2007. ISBN 978-972-722-539-2;

SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho - *Segurança dos sistemas de informação - Gestão estratégica da segurança empresarial*. Lisboa: Centro Atlântico, 2003. ISBN 972-8426-66-6;

STANTON, Jeffrey M.; STAM, Kathryn R.; MASTRANGELO, Paul; JOLTON Jeffrey - *Analysis of end user security behaviors*. Computers & Security. ISSN 0167-4048. Vol. 28, nº 2 (2005) p. 124 – 133;

VARAJÃO, João Eduardo Quintela – *A Arquitectura da gestão de sistemas de informação*. Lisboa: FCA, 1998. ISBN 972-722-140-8;

VEIGA, Armando – *Legislação de direito da informática*. 2ª ed. Coimbra: Coimbra editora, 2009. ISBN 978-972-32-1664-6;

WORKMAN, Michael; BOMMER, William H.; STRAUB, Detmar - *Security lapses and the omission of information security measures: A threat control model and empirical test*. Computers in Human Behavior. ISSN 0747-5632. Vol. 24, nº 6 (2008) p. 2799 – 2816;

ZORRINHO, Carlos; SERRANO, António; LACERDA, Palmira - *Gerir em complexidade: um novo paradigma da gestão.* 2ª ed. Lisboa : Sílabo, 2007. ISBN 978-972-618-445-4;

Anexos

Anexo 1 - Questionário

Inquérito por Questionário

"O contributo dos comportamentos e atitudes dos utilizadores para a segurança dos Sistemas de Informação das Organizações."

Investigação realizada no âmbito da dissertação do Mestrado em Gestão

Departamento de Gestão. Universidade de Évora.

Este questionário faz parte de um estudo do Departamento de Gestão da Universidade de Évora e tem como objectivo recolher informações sobre os comportamentos dos utilizadores relativamente aos Sistemas de Informação das Organizações.

Gostaríamos de salientar que não existem respostas certas ou erradas a este questionário, apenas se pretende a sua opinião sobre as questões colocadas.

As respostas ao questionário são anónimas, não sendo solicitadas informações que o possam de alguma forma identificar.

O tempo de realização deste questionário é de cerca de 15 minutos. A sua colaboração é fundamental para o desenvolvimento deste trabalho.

Agradecemos desde já a sua colaboração.

INSTRUÇÕES DE PREENCHIMENTO

Por ser fundamental uma boa interpretação das suas respostas, pedimos a sua especial atenção para as instruções de preenchimento, abaixo descritas:

- Preencha o questionário seleccionando a resposta, de entre as opções disponíveis, que melhor caracteriza a sua opinião.
- Deve escolher apenas uma de entre as várias opções de resposta que lhe são dadas.
- Responda a todas as questões, pois só assim será possível considerar como válida a sua resposta para tratamento dos dados.

I. A SEGURANÇA NOS SISTEMAS DE INFORMAÇÃO

	Sim	Não
1. Usa computador na sua actividade profissional?	☐	☐

Se respondeu Não ou Não sei na questão "1. Usa computador para desenvolver a sua actividade profissional?", avance para o grupo de questões III (dados de caracterização).

2. Leia as afirmações seguintes sobre os comportamentos no uso dos Sistemas de Informação e seleccione, para cada uma delas, a alternativa que melhor corresponde ao seu caso:

	Sim	Não	Não sei
2.1. Efectuo com regularidade as actualizações de segurança do sistema operativo;	☐	☐	☐
2.2. Já fui infectado por vírus ou *spyware* no meu computador;	☐	☐	☐
2.3. Efectuo com regularidade cópias de segurança da informação do meu computador de trabalho;	☐	☐	☐
2.4. Utilizo a mesma palavra-passe para aceder aos diversos programas informáticos que uso;	☐	☐	☐
2.5. Por vezes envio dados confidenciais através de correio electrónico (por exemplo: números/NIB de contas bancárias, palavras-passe ou número de identificação fiscal, etc.);	☐	☐	☐
2.6. Não partilho ficheiros do meu computador de trabalho com outros utilizadores dentro ou fora da organização;	☐	☐	☐
2.7. Partilho a(s) minha(s) palavra(s)-passe com outros utilizadores na organização;	☐	☐	☐
2.8. Tenho conhecimento que os colegas que visualizam o correio electrónico da organização abrem os anexos de todas as mensagens que são recebidas;	☐	☐	☐
2.9. No meu computador de trabalho ligo dispositivos de armazenamento externo de outras pessoas;	☐	☐	☐
2.10. Quando detecto algum tipo de "comportamento" estranho no meu computador (por exemplo desligar-se sem motivo aparente) aviso logo o meu superior ou o responsável do sector da informática;	☐	☐	☐
2.11. Na construção das minhas palavras-passe utilizo a conjugação de números, letras e caracteres especiais (por exemplo #, *, !, etc.);	☐	☐	☐
2.12. Não aplico as políticas e controlos de segurança definidos pela organização;	☐	☐	☐
2.13. O meu computador de trabalho tem instalado e activo um mecanismo de segurança para protecção contra intrusões de terceiros (*firewall*);	☐	☐	☐

	Sim	Não	Não sei
2.14. No meu local de trabalho, quando me afasto do meu computador para tratar de algum assunto mesmo que rápido, costumo terminar a sessão ou aplicar a protecção de ecrã;	☐	☐	☐
2.15. Tenho conhecimento que colegas de trabalho costumam utilizar *software* e sites de partilha de ficheiros, efectuando downloads no local de trabalho (por exemplo: *Kazaa*, pirata tuga, *rapidshare*, etc.);	☐	☐	☐
2.16. Não tenho instalado um *software* antivírus no meu computador de trabalho;	☐	☐	☐
2.17. Já tive necessidade de recorrer às cópias de segurança realizadas para repor informação no meu computador de trabalho;	☐	☐	☐
2.18. Tenho dificuldade em memorizar todas as minhas palavras-passe;	☐	☐	☐
2.19. Para não me esquecer das minhas palavras-passe escrevo-as num papel;	☐	☐	☐
2.20. Na minha organização não existe uma política definida para a utilização da Internet e do correio electrónico;	☐	☐	☐
2.21. Se detectar algum colega a praticar algum tipo de quebra nas políticas de segurança estabelecidas aviso imediatamente o meu superior ou o responsável pela segurança informática;	☐	☐	☐
2.22. Na minha organização partilho o meu computador e respectiva informação com outros utilizadores;	☐	☐	☐
2.23. Quando envio informações através de formulários na Internet tenho o cuidado de verificar se existe alguma informação que indique que os mesmos são transmitidos de forma protegida;	☐	☐	☐
2.24. Quando altero a palavra-passe do meu computador de trabalho, transmito a mesma a algum colega, para este poder aceder ao meu computador;	☐	☐	☐
2.25. Tenho conhecimento que alguns colegas aproveitam a boa velocidade de navegação da Internet na organização para efectuarem pesquisas de assuntos particulares;	☐	☐	☐
2.26. As minhas palavras-passe estão registadas num papel que coloco junto ao computador;	☐	☐	☐
2.27. Detectei um colega de trabalho a fornecer os seus dados de acesso ao computador a terceiros, mas para evitar problemas ignorei o caso;	☐	☐	☐

3. Indique para cada uma das afirmações o seu grau de concordância relativamente à adopção de comportamentos no uso dos Sistemas de Informação nas Organizações:

		Discordo totalmente	Discordo em parte	Nem concordo nem discordo	Concordo em parte	Concordo totalmente
3.1.	Não é importante efectuar as actualizações do sistema operativo e restantes aplicações;	☐	☐	☐	☐	☐
3.2.	Os programas antivírus e *anti-spyware* proporcionam uma eficaz protecção do computador;	☐	☐	☐	☐	☐
3.3.	É suficiente efectuar cópias de segurança da informação semanalmente;	☐	☐	☐	☐	☐
3.4.	É importante proceder à alteração das minhas palavras-passe uma vez por ano;	☐	☐	☐	☐	☐
3.5.	O envio de informações confidenciais através de formulários na Internet, sem que exista a indicação que a mesma é enviada de forma protegida, é seguro;	☐	☐	☐	☐	☐
3.6.	Partilhar a palavra-passe do meu computador de trabalho com um colega é seguro;	☐	☐	☐	☐	☐
3.7.	Não é importante analisar o assunto de uma mensagem de correio electrónico, antes de a abrir;	☐	☐	☐	☐	☐
3.8.	Guardar informação em dispositivos de armazenamento externos próprios, depois de os ligar a outros computadores, é um procedimento prudente;	☐	☐	☐	☐	☐
3.9.	Considero que é importante a organização apresentar, através de um documento escrito, as políticas de segurança que tenho que respeitar;	☐	☐	☐	☐	☐
3.10.	Na organização, a existência de *software* antivírus e contra intrusões por terceiros (*firewall*) instalados no computador é sinónimo de segurança;	☐	☐	☐	☐	☐
3.11.	Não existe qualquer risco em deixar o meu computador de trabalho ligado quando tenho que ir à casa de banho, por exemplo;	☐	☐	☐	☐	☐
3.12.	Efectuar cópias de segurança da minha informação apenas para o disco do meu computador é um bom procedimento;	☐	☐	☐	☐	☐
3.13.	Quando é necessário alterar uma palavra-passe, é um procedimento normal colocar uma fácil de memorizar;	☐	☐	☐	☐	☐

	Discordo totalmente	Discordo em parte	Nem concordo nem discordo	Concordo em parte	Concordo totalmente
3.14. Não é necessário informar o meu superior ou o responsável pela segurança informática quando o meu computador de trabalho reinicia sozinho, sem motivo aparente;	☐	☐	☐	☐	☐
3.15. As formações sobre as políticas de segurança da organização são importantes;	☐	☐	☐	☐	☐
3.16. A utilização da Internet na organização para efectuar *downloads* de filmes e jogos, não representa qualquer ameaça para a segurança dos Sistemas de Informação dessa organização;	☐	☐	☐	☐	☐
3.17. É um bom procedimento enviar para o lixo as mensagens de correio electrónico de remetentes que não conheço;	☐	☐	☐	☐	☐
3.18. Actualizar diariamente os programas antivírus e *anti-spyware* permite uma melhor protecção do meu computador de trabalho;	☐	☐	☐	☐	☐

II. COMENTÁRIOS OU SUGESTÕES (RESPOSTA NÃO OBRIGATÓRIA)

4. Utilize este espaço para incluir sugestões, justificações ou outras observações que julgue convenientes. Se pretender fazer uma observação relativamente a determinada questão, por favor, não se esqueça de a identificar.

III. DADOS DE CARACTERIZAÇÃO

NOTA: relembramos que os dados recolhidos são os estritamente necessários ao desenvolvimento deste estudo. As questões seguintes servem apenas para caracterizar o perfil dos utilizadores dos Sistemas de Informação nas Organizações. Salientamos ainda que não será solicitado qualquer dado pessoal que o possa identificar e é garantido o anonimato total das respostas.

1. Idade

1.1. Menos de 16 anos ☐
1.2. Dos 16 aos 29 anos ☐
1.3. Dos 30 aos 49 anos ☐
1.4. Dos 50 aos 64 anos ☐
1.5. Mais de 64 anos ☐

2. Sexo

2.1. Masculino ☐
2.2. Feminino ☐

3. Grau de ensino mais elevado que terminou

3.1. Não frequentou a Escola ou não concluiu o 1.º Ciclo do Ensino Básico ☐
3.2. Ensino Básico 1.º Ciclo (4.º ano de escolaridade) ☐
3.3. Ensino Básico 2.º Ciclo (6.º ano de escolaridade) ☐
3.4. Ensino Básico 3.º Ciclo (9.º ano de escolaridade) ☐
3.5. Ensino Secundário (12.ª ano de escolaridade) ☐
3.6. Curso Pós-Secundário – Curso de Especialização Tecnológica ☐
3.7. Curso Superior (Bacharel, Licenciatura) ☐
3.8. Curso Pós-Graduado (Mestrado, Doutoramento) ☐

4. Situação profissional

4.1. Trabalhador por conta de outrem no sector público ☐
4.2. Trabalhador por conta de outrem no sector privado ☐
4.3. Trabalhador por conta própria ☐
4.4. Outra? Indique qual : _____ ☐

5. Número de trabalhadores da Organização

5.1. Menos de 10 funcionários	☐
5.2. De 10 a 49 funcionários	☐
5.3. De 50 a 249 funcionários	☐
5.4. 250 funcionários ou mais	☐
5.5. Não sei	☐

6. Distrito do local de trabalho:

6.1. Aveiro	☐
6.2. Beja	☐
6.3. Braga	☐
6.4. Bragança	☐
6.5. Castelo Branco	☐
6.6. Coimbra	☐
6.7. Évora	☐
6.8. Faro	☐
6.9. Guarda	☐
6.10. Leiria	☐
6.11. Lisboa	☐
6.12. Portalegre	☐
6.13. Porto	☐
6.14. Santarém	☐
6.15. Setúbal	☐
6.16. Viana do Castelo	☐
6.17. Vila Real	☐
6.18. Viseu	☐
6.19. Região Autónoma dos Açores	☐
6.20. Região Autónoma da Madeira	☐
6.21. Fora de Portugal. Indique o país: _____	☐

7. Sector de actividade da Organização:

7.1. Agricultura, produção animal, caça, floresta e pesca	☐
7.2. Indústrias extractivas	☐
7.3. Indústrias transformadoras	☐
7.4. Electricidade, gás, vapor, água quente e fria e ar frio	☐

7.5. Captação, tratamento e distribuição de água	☐
7.6. Construção	☐
7.7. Comércio por grosso e a retalho	☐
7.8. Alojamento, restauração e similares	☐
7.9. Actividades de informação e de comunicação	☐
7.10. Actividades financeiras e de seguros	☐
7.11. Actividades imobiliárias	☐
7.12. Actividades de consultoria, científicas, técnicas e similares	☐
7.13. Actividades administrativas e dos serviços de apoio	☐
7.14. Administração Pública e defesa	☐
7.15. Educação	☐
7.16. Actividades de saúde humana e apoio social	☐
7.17. Actividades artísticas, de espectáculos, desportivas e recreativas	☐
7.18. Outras actividades de serviços	☐
7.19. Actividades das famílias empregadoras de pessoal doméstico e actividades e produção das famílias para uso próprio	☐
7.20. Actividades dos organismos internacionais e outras instituições extraterritoriais	☐
7.21. Outra Indique qual:_____	☐

Anexo 2 - Carta de Apresentação

Exmo.(a) Sr. ou Sr.ª:

Sou estudante da Universidade de Évora, do Mestrado em Gestão, na área de especialização de Organização e Sistemas de Informação.

Para a realização da tese de Mestrado estou a efectuar um estudo sobre os comportamentos dos utilizadores relativamente aos Sistemas de Informação das Organizações.

A recolha dos dados está a ser feita através de um questionário *on-line*, para o qual peço a sua colaboração. A sua participação é muito importante para a realização deste trabalho.

Para preencher o questionário, por favor clique em: http://docentes.esgs.pt/inqseg/index.htm

Os dados recolhidos neste questionário serão apenas visualizados pelos autores do estudo e serão utilizados apenas para a elaboração do mesmo, sendo assegurada a sua confidencialidade.

Agradeço também que, se possível, divulgue este questionário através da sua lista de contactos, para que possa obter um número de respostas ao questionário suficientes para a elaboração do estudo.

Caso tenha algum interesse nos resultados do estudo, ou se necessitar de mais informação, por favor contacte-me através do endereço de correio electrónico: questionario.seginf@gmail.com.

Atenciosamente,

Alexandre Pimenta

Anexo 3 - Codificação dos dados

	Respostas possíveis	Valor Atribuído
Questão 1	Sim	1
	Não	2

	Respostas possíveis	Valor Atribuído
Questão 2	Sim	1
	Não	2
	Não sei	3

	Respostas possíveis	Valor Atribuído
Questão 3	Discordo totalmente	1
	Discordo em parte	2
	Nem concordo nem discordo	3
	Concordo em parte	4
	Concordo totalmente	5

Dados de caracterização

	Respostas possíveis	Valor atribuído
Idade	Menos de 16 anos	1
	Dos 16 aos 29 anos	2
	Dos 30 aos 49 anos	3
	Dos 50 aos 64 anos	4
	Mais de 64 anos	5

	Respostas possíveis	Valor atribuído
Sexo	Masculino	1
	Feminino	2

	Respostas possíveis	Valor atribuído
Grau de ensino mais elevado que terminou	Não frequentou a Escola ou não concluiu o 1.º Ciclo do Ensino Básico	1
	Ensino Básico 1.º Ciclo (4.º ano de escolaridade)	2
	Ensino Básico 2.º Ciclo (6.º ano de escolaridade)	3
	Ensino Básico 3.º Ciclo (9.º ano de escolaridade)	4
	Ensino Secundário (12.ª ano de escolaridade)	5
	Curso Pós-Secundário – Curso de Especialização Tecnológica	6
	Curso Superior (Bacharel, Licenciatura)	7
	Curso Pós-Graduado (Mestrado, Doutoramento)	8

	Respostas possíveis	Valor atribuído
Situação profissional	Trabalhador por conta de outrem no sector público	1
	Trabalhador por conta de outrem no sector privado	2
	Trabalhador por conta própria	3
	Outra	4

	Respostas possíveis	Valor atribuído
Número de trabalhadores da Organização	Menos de 10 funcionários	1
	De 10 a 49 funcionários	2
	De 50 a 249 funcionários	3
	250 funcionários ou mais	4
	Não sei	5

	Respostas possíveis	Valor atribuído
Distrito do local de trabalho	Aveiro	1
	Beja	2
	Braga	3
	Bragança	4
	Castelo Branco	5
	Coimbra	6
	Évora	7
	Faro	8
	Guarda	9
	Leiria	10
	Lisboa	11
	Portalegre	12
	Porto	13
	Santarém	14
	Setúbal	15
	Viana do Castelo	16
	Vila Real	17
	Viseu	18
	Região Autónoma dos Açores	18
	Região Autónoma da Madeira	20
	Fora de Portugal	21

	Respostas possíveis	Valor atribuído
Sector de actividade da Organização	Agricultura, produção animal, caça, floresta e pesca	1
	Indústrias extractivas	2
	Indústrias transformadoras	3
	Electricidade, gás, vapor, água quente e fria e ar frio	4
	Captação, tratamento e distribuição de água	5
	Construção	6
	Comércio por grosso e a retalho	7
	Alojamento, restauração e similares	8
	Actividades de informação e de comunicação	9
	Actividades financeiras e de seguros	10
	Actividades imobiliárias	11
	Actividades de consultoria, científicas, técnicas e similares	12
	Actividades administrativas e dos serviços de apoio	13
	Administração Pública e defesa	14
	Educação	15
	Actividades de saúde humana e apoio social	16
	Actividades artísticas, de espectáculos, desportivas e recreativas	17
	Outras actividades de serviços	18
	Actividades das famílias empregadoras de pessoal doméstico e actividades e produção das famílias para uso próprio	19
	Actividades dos organismos internacionais e outras instituições extraterritoriais	20
	Outra	21

Anexo 4 – Caracterização dos respondentes

III - 2. Sexo

	Frequências	Percentagem
Masculino	350	44,9
Feminino	**430**	**55,1**
Total	780	100,0

Tabela 8 - Questão III-2: Distribuição das respostas válidas por sexo

	Frequências	Percentagem
Masculino	16	43,2
Feminino	**21**	**56,8**
Total	37	100,0

Tabela 9 - Questão III-2: Distribuição das respostas não válidas por sexo

III - 4. Situação profissional

	Frequências	Percentagem
Trabalhador por conta de outrem no sector público	**573**	**73,5**
Trabalhador por conta de outrem no sector privado	173	22,2
Trabalhador por conta própria	23	2,9
Outra	11	1,4
Total	780	100,0

Tabela 10 - Questão III-4: Distribuição das respostas válidas por situação profissional

	Frequências	Percentagem
Trabalhador por conta de outrem no sector	7	18,9
Trabalhador por conta de outrem no sector	3	8,1
Trabalhador por conta própria	1	2,7
Outra	**26**	**70,3**
Total	37	100,0

Tabela 11 - Questão III-4: Distribuição das respostas não válidas por situação profissional

III – 4.4 Outra situação.

	Frequências	Percentagem
Em branco	3	27,3
Bolseiro	1	9,1
Bolseiro de Investigação	1	9,1
Estudante-trabalhador	1	9,1
Prestação de serviços no sector público	1	9,1
Prof. contratado e trabalhador em nome individual	1	9,1
Sócio gerente	1	9,1
Trabalhador por conta de outrem no privado e	1	9,1
Trabalhador por conta de outrem no sector público	1	9,1
Total	11	100,0

Tabela 12 - Questão III-4.4: Lista de outras situações e respectiva distribuição das respostas válidas

	Frequências	Percentagem
Desempregada	1	3,8
Desempregado	1	3,8
Estudante	**21**	**80,8**
Estudante a concluir licenciatura	2	7,7
Estudante e desempregado	1	3,8
Total	26	100,0

Tabela 13 - Questão III-4.4: Lista de outras situações e respectiva distribuição das respostas não válidas

III - 6. Distrito local trabalho

	Frequências	Percentagem
Aveiro	13	1,7
Beja	6	0,8
Braga	26	3,3
Bragança	2	0,3
Castelo Branco	99	12,7

Coimbra	33	4,2
Évora	41	5,3
Faro	5	0,6
Guarda	19	2,4
Leiria	28	3,6
Lisboa	**189**	**24,2**
Portalegre	4	0,5
Porto	51	6,5
Santarém	163	20,9
Setúbal	37	4,7
Viana do Castelo	10	1,3
Vila Real	8	1,0
Viseu	38	4,9
Região Autónoma dos Açores	5	0,6
Região Autónoma da Madeira	0	0,0
Fora de Portugal	3	0,4
Total	780	100,0

Tabela 14 - Questão III-6: Distribuição das respostas válidas por distrito

	Frequências	**Percentagem**
Aveiro	0	0,0
Beja	0	0,0
Braga	1	2,7
Bragança	1	2,7
Castelo Branco	**11**	**29,7**
Coimbra	2	5,4
Évora	3	8,1
Faro	0	0,0
Guarda	1	2,7
Leiria	0	0,0
Lisboa	6	16,2
Portalegre	1	2,7

Porto	0	0,0
Santarém	10	27,0
Setúbal	0	0,0
Viana do Castelo	0	0,0
Vila Real	0	0,0
Viseu	0	0,0
Região Autónoma dos Açores	0	0,0
Região Autónoma da Madeira	1	2,7
Fora de Portugal	0	0,0
Total	37	100,0

Tabela 15 - Questão III-6: Distribuição das respostas não válidas por distrito

III – 6.21 Fora de Portugal

	Frequências	Percentagem
Brasil.	1	33,3
España	1	33,3
Inglaterra	1	33,3
Total	3	100,0

Tabela 16 - Questão III-6.21: Lista de Países fora de Portugal e respectiva distribuição das respostas válidas

III – 7. Sector da actividade da organização

	Frequências	Percentagem
Agricultura, produção animal, caça, floresta e pesca	6	0,8
Indústrias extractivas	1	0,1
Indústrias transformadoras	12	1,5
Electricidade, gás, vapor, água quente e fria e ar	3	0,4
Captação, tratamento e distribuição de água	1	0,1
Construção	13	1,7
Comércio por grosso e a retalho	14	1,8
Alojamento, restauração e similares	5	0,6
Actividades de informação e de comunicação	19	2,4

Actividades financeiras e de seguros	13	1,7
Actividades imobiliárias	3	0,4
Actividades de consultoria, científicas, técnicas e	40	5,1
Actividades administrativas e dos serviços de apoio	14	1,8
Administração Pública e defesa	50	6,4
Educação	**481**	**61,7**
Actividades de saúde humana e apoio social	14	1,8
Actividades artísticas, de espectáculos, desportivas	6	0,8
Outras actividades de serviços	32	4,1
Outra	53	6,8
Total	780	100,0

Tabela 17 - Questão III-7: Distribuição das respostas válidas por sector de actividade

	Frequências	**Percentagem**
Indústrias transformadoras	2	5,4
Comércio por grosso e a retalho	1	2,7
Actividades de informação e de comunicação	1	2,7
Actividades de consultoria, científicas, técnicas e	1	2,7
Actividades administrativas e dos serviços de	2	5,4
Administração Pública e defesa	1	2,7
Educação	**15**	**40,5**
Actividades de saúde humana e apoio social	1	2,7
Actividades artísticas, de espectáculos,	2	5,4
Outras actividades de serviços	2	5,4
Actividades das famílias empregadoras de …	1	2,7
Outra	8	21,6
Total	37	100,0

Tabela 18 – Questão III-7: Distribuição das respostas não válidas por sector de actividade

III - 7.21 Outra

	Frequências	Percentagem
Em Branco	5	9,4
Administração Fiscal	1	1,9
Administração Local	3	5,7
Advocacia	1	1,9
Artesanato	1	1,9
Ass.	1	1,9
Associação	2	3,8
Audiovisuais	1	1,9
Autarquia	1	1,9
Autarquia Local	2	3,8
Comercio a Retalho de Combustíveis	1	1,9
Comércio de pedras e metais preciosos	1	1,9
Consultoria	1	1,9
Cooperativa de Educação e Reabilitação	1	1,9
Defesa	1	1,9
Defesa	2	3,8
Desenvolvimento Local	1	1,9
Distribuição e Logística	1	1,9
Docente	1	1,9
Empresa de construção civil e obras publicas - recursos	1	1,9
Energias Alternativas	1	1,9
Ensino	1	1,9
Ensino Superior	3	5,7
Ensino Superior e Investigação	1	1,9
ESCOLA	1	1,9
Estabelecimento de Ensino Superior	1	1,9
Forças Armadas	1	1,9
Fotografia	1	1,9
Gestor de Vendas Online.	1	1,9
Industria Alimentar	1	1,9
Industria Farmacêutica	1	1,9
Informatica	1	1,9
Informática	1	1,9
Investigação Académica	1	1,9

Militar	1	1,9
Não se aplica.	1	1,9
Operador de Gasolineira	1	1,9
PRODUÇÃO DE NÃO TECIDOS, GEOTEXTEIS E	1	1,9
Sinalização Ferroviária, Sistemas de Segurança e	1	1,9
Telecomunicações	1	1,9
Transportes e Logística	1	1,9
Turismo	1	1,9
Total	53	100.0

Tabela 19 - Questão III-7.21: Lista de outras actividades e respectiva distribuição das respostas válidas

	Frequências	**Percentagem**
Em branco	2	25,0
...	1	12,5
Educação na área da agricultura	1	12,5
Historia	1	12,5
Informática	1	12,5
Logística	1	12,5
Nenhuma	1	12,5
Total	8	100,0

Tabela 20 - Questão III-7.21: Lista de outras actividades e respectiva distribuição das respostas não válidas

Anexo 5 – Análise dos resultados

I - 2. Leia as afirmações seguintes sobre os comportamentos no uso dos Sistemas de Informação e seleccione, para cada uma delas, a alternativa que melhor corresponde ao seu caso:

	Sim		Não		Não sei	
	N	%	N	%	N	%
2.1 Efectuo com regularidade as actualizações de segurança do sistema operativo;	589	75,5%	160	20,5%	31	4,0%
2.2 Já fui infectado por vírus ou spyware no meu computador;	560	71,8%	182	23,3%	38	4,9%
2.3 Efectuo com regularidade cópias de segurança da informação do meu computador de trabalho;	492	63,1%	281	36,0%	7	0,9%
2.4 Utilizo a mesma palavra-passe para aceder aos diversos programas informáticos que uso;	327	41,9%	450	57,7%	3	0,4%
2.5 Por vezes envio dados confidenciais através de correio electrónico (por exemplo: números/NIB de contas bancárias, palavras-passe ou número de identificação fiscal, etc.);	263	33,7%	514	65,9%	3	0,4%
2.6 Não partilho ficheiros do meu computador de trabalho com outros utilizadores dentro ou fora da organização;	336	43,1%	430	55,1%	14	1,8%
2.7 Partilho a(s) minha(s) palavra(s)-passe com outros utilizadores na organização;	90	11,5%	689	88,3%	1	0,1%
2.8 Tenho conhecimento que os colegas que visualizam o correio electrónico da organização abrem os anexos de todas as mensagens que são recebidas;	242	31,0%	248	31,8%	290	37,2%
2.9 No meu computador de trabalho ligo dispositivos de armazenamento externo de outras pessoas;	406	52,1%	361	46,3%	13	1,7%
2.10 Quando detecto algum tipo de "comportamento" estranho no meu computador (por exemplo desligar-se sem motivo aparente) aviso logo o meu superior ou o responsável do sector da informática;	536	68,7%	221	28,3%	23	2,9%
2.11 Na construção das minhas palavras-passe utilizo a conjugação de números, letras e caracteres especiais (por exemplo #, *, !, etc.);	390	50,0%	387	49,6%	3	0,4%
2.12 Não aplico as políticas e controlos de segurança definidos pela organização;	179	22,9%	481	61,7%	120	15,4%
2.13 O meu computador de trabalho tem instalado e activo um mecanismo de segurança para protecção contra intrusões de terceiros (firewall);	666	85,4%	44	5,6%	70	9,0%

2.14 No meu local de trabalho, quando me afasto do meu computador para tratar de algum assunto mesmo que rápido, costumo terminar a sessão ou aplicar a protecção de ecrã;	415	53,2%	360	46,2%	5	0,6%
2.15 Tenho conhecimento que colegas de trabalho costumam utilizar software e sites de partilha de ficheiros, efectuando downloads no local de trabalho (por exemplo: Kazaa, pirata tuga, rapidshare, etc.);	162	20,8%	389	49,9%	229	29,4%
2.16 Não tenho instalado um software antivírus no meu computador de trabalho;	179	22,9%	578	74,1%	23	2,9%
2.17 Já tive necessidade de recorrer às cópias de segurança realizadas para repor informação no meu computador de trabalho;	385	49,4%	383	49,1%	12	1,5%
2.18 Tenho dificuldade em memorizar todas as minhas palavras-passe;	188	24,1%	587	75,3%	5	0,6%
2.19 Para não esquecer as minhas palavras-passe escrevo-as num papel;	164	21,0%	613	78,6%	3	0,4%
2.20 Na minha organização não existe uma política definida para a utilização da Internet e do correio electrónico;	293	37,6%	384	49,2%	103	13,2%
2.21 Se detectar algum colega a praticar algum tipo de quebra nas políticas de segurança estabelecidas aviso imediatamente o meu superior ou o responsável pela segurança informática;	212	27,2%	430	55,1%	138	17,7%
2.22 Na minha organização partilho o meu computador e respectiva informação com outros utilizadores;	288	36,9%	486	62,3%	6	0,8%
2.23 Quando envio informações através de formulários na Internet tenho o cuidado de verificar se existe alguma informação que indique que os mesmos são transmitidos de forma protegida;	519	66,5%	220	28,2%	41	5,3%
2.24 Quando altero a palavra-passe do meu computador de trabalho, transmito a mesma a algum colega, para este poder aceder ao meu computador;	121	15,5%	651	83,5%	8	1,0%
2.25 Tenho conhecimento que alguns colegas aproveitam a boa velocidade de navegação da Internet na organização para efectuarem pesquisas de assuntos particulares;	410	52,6%	201	25,8%	169	21,7%
2.26 As minhas palavras-passe estão registadas num papel que coloco junto ao computador;	15	1,9%	763	97,8%	2	0,3%
2.27 Detectei um colega de trabalho a fornecer os seus dados de acesso ao computador a terceiros, mas para evitar problemas ignorei o caso;	66	8,5%	615	78,8%	99	12,7%

Tabela 21 - Questão I-2: Distribuição das respostas pelo grupo de questões 2

I - 3. Indique para cada uma das afirmações o seu grau de concordância relativamente à adopção de comportamentos no uso dos Sistemas de Informação nas Organizações:

	1		2		3		4		5	
	N	%	N	%	N	%	N	%	N	%
3.1 Não é importante efectuar as actualizações do sistema operativo e restantes aplicações;	640	82,1%	69	8,8%	12	1,5%	23	2,9%	36	4,6%
3.2 Os programas antivírus e anti-spyware proporcionam uma eficaz protecção do computador;	11	1,4%	61	7,8%	38	4,9%	358	45,9%	312	40,0%
3.3 É suficiente efectuar cópias de segurança da informação semanalmente;	51	6,5%	112	14,4%	145	18,6%	349	44,7%	123	15,8%
3.4 É importante proceder à alteração das minhas palavras-passe uma vez por ano;	72	9,2%	74	9,5%	153	19,6%	233	29,9%	248	31,8%
3.5 O envio de informações confidenciais através de formulários na Internet, sem que exista a indicação que a mesma é enviada de forma protegida, é seguro;	439	56,3%	131	16,8%	102	13,1%	74	9,5%	34	4,4%
3.6 Partilhar a palavra-passe do meu computador de trabalho com um colega é seguro;	437	56,0%	162	20,8%	61	7,8%	100	12,8%	20	2,6%
3.7 Não é importante analisar o assunto de uma mensagem de correio electrónico, antes de a abrir;	604	77,4%	85	10,9%	29	3,7%	21	2,7%	41	5,3%
3.8 Guardar informação em dispositivos de armazenamento externos próprios, depois de os ligar a outros computadores, é um procedimento prudente;	163	20,9%	207	26,5%	174	22,3%	137	17,6%	99	12,7%
3.9 Considero que é importante a organização apresentar, através de um documento escrito, as políticas de segurança que tenho que respeitar;	14	1,8%	12	1,5%	69	8,8%	183	23,5%	502	64,4%
3.10 Na organização, a existência de software antivírus e contra intrusões por terceiros (firewall) instalados no computador é sinónimo de segurança;	18	2,3%	44	5,6%	51	6,5%	421	54,0%	246	31,5%
3.11 Não existe qualquer risco em deixar o meu computador de trabalho ligado quando tenho que ir à casa de banho, por exemplo;	209	26,8%	172	22,1%	104	13,3%	193	24,7%	102	13,1%
3.12 Efectuar cópias de segurança da minha informação apenas para o disco do meu computador é um bom procedimento;	377	48,3%	178	22,8%	63	8,1%	119	15,3%	43	5,5%
3.13 Quando é necessário alterar uma palavra-passe, é um procedimento normal colocar uma fácil de memorizar;	166	21,3%	155	19,9%	76	9,7%	217	27,8%	166	21,3%

3.14 Não é necessário informar o meu superior ou o responsável pela segurança informática quando o meu computador de trabalho reinicia sozinho, sem motivo aparente;	444	56,9%	148	19,0%	102	13,1%	61	7,8%	25	3,2%
3.15 As formações sobre as políticas de segurança da organização são importantes;	6	,8%	8	1,0%	51	6,5%	196	25,1%	519	66,5%
3.16 A utilização da Internet na organização para efectuar downloads de filmes e jogos, não representa qualquer ameaça para a segurança dos Sistemas de Informação dessa organização;	541	69,4%	117	15,0%	65	8,3%	37	4,7%	20	2,6%
3.17 É um bom procedimento enviar para o lixo as mensagens de correio electrónico de remetentes que não conheço;	38	4,9%	46	5,9%	53	6,8%	252	32,3%	391	50,1%
3.18 Actualizar diariamente os programas antivírus e anti-spyware permite uma melhor protecção do meu computador de trabalho;	11	1,4%	13	1,7%	68	8,7%	187	24,0%	501	64,2%

Tabela 22 - Questão I-3: Distribuição das respostas pelo grupo de questões 3

Legenda dos valores da escala de medida:

1 - Discordo totalmente; 2 - Discordo em parte; 3 - Nem concordo nem discordo; 4 - Concordo em parte; 5 - Concordo totalmente

	N	Média	Desvio Padrão
3.1 Não é importante efectuar as actualizações do sistema operativo e restantes aplicações;	780	1,39	1,001
3.2 Os programas antivírus e anti-spyware proporcionam uma eficaz protecção do computador;	780	4,15	0,931
3.3 É suficiente efectuar cópias de segurança da informação semanalmente;	780	3,49	1,116
3.4 É importante proceder à alteração das minhas palavras-passe uma vez por ano;	780	3,66	1,268
3.5 O envio de informações confidenciais através de formulários na Internet, sem que exista a indicação que a mesma é enviada de forma protegida, é seguro;	780	1,89	1,206
3.6 Partilhar a palavra-passe do meu computador de trabalho com um colega é seguro;	780	1,85	1,167
3.7 Não é importante analisar o assunto de uma mensagem de correio electrónico, antes de a abrir;	780	1,47	1,057
3.8 Guardar informação em dispositivos de armazenamento externos próprios, depois de os ligar a outros computadores, é um procedimento prudente;	780	2,75	1,312
3.9 Considero que é importante a organização apresentar, através de um documento escrito, as políticas de segurança que tenho que respeitar;	780	4,47	0,857
3.10 Na organização, a existência de software antivírus e contra intrusões por terceiros (firewall) instalados no computador é sinónimo de segurança;	780	4,07	0,900
3.11 Não existe qualquer risco em deixar o meu computador de trabalho ligado quando tenho que ir à casa de banho, por exemplo;	780	2,75	1,416
3.12 Efectuar cópias de segurança da minha informação apenas para o disco do meu computador é um bom procedimento;	780	2,07	1,292

3.13 Quando é necessário alterar uma palavra-passe, é um procedimento normal colocar uma fácil de memorizar;	780	3,08	1,475
3.14 Não é necessário informar o meu superior ou o responsável pela segurança informática quando o meu computador de trabalho reinicia sozinho, sem motivo aparente;	780	1,81	1,126
3.15 As formações sobre as políticas de segurança da organização são importantes;	780	4,56	0,729
3.16 A utilização da Internet na organização para efectuar downloads de filmes e jogos, não representa qualquer ameaça para a segurança dos Sistemas de Informação dessa organização;	780	1,56	1,003
3.17 É um bom procedimento enviar para o lixo as mensagens de correio electrónico de remetentes que não conheço;	780	4,17	1,103
3.18 Actualizar diariamente os programas antivírus e anti-*spyware* permite uma melhor protecção do meu computador de trabalho;	780	4,48	0,833

Tabela 23 - Estatísticas do grau de concordância do grupo de questões 3