JISTEM - Journal of Information Systems and Technology Management
Revista de Gestão da Tecnologia e Sistemas de Informação
Vol. 13, No. 3, Set/Dez., 2016 pp. 533-552
ISSN online: 1807-1775
DOI: 10.4301/S1807-17752016000300010

A SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO E O COMPORTAMENTO DOS USUÁRIOS

INFORMATION SYSTEMS SECURITY AND USERS' BEHAVIOR

Alexandre Manuel Santareno Pimenta
Escola Superior de Gestão e Tecnologia, Instituto Politécnico de Santarém (ESGT-IPS), Santarém, Portugal
Rui Filipe Cerqueira Quaresma
Escola de Ciências Sociais – Universidade de Évora, Évora , Portugal

---

RESUMO

Numa sociedade cada vez mais global e em constante mutação, onde as organizações necessitam ter sempre disponível a informação necessária e útil para desenvolver, de uma forma rápida e eficaz, as suas atividades no dia-a-dia, garantir a segurança da informação é um fator fundamental para sustentar a sua continuidade e sucesso.Neste estudo procura-se saber em que medida os comportamentos e as atitudes dos usuários dos sistemas de informação constituem um risco ou uma proteção para a segurança destes sistemas. Para alcançar este objetivo foi primeiramente realizada uma revisão bibliográfica baseada em fontes secundárias, que permitiu desenvolver o questionário para coleta de dados; seguidamente, e usando um questionário *online*, foram recolhidas respostas de 780 sujeitos, que maioritariamente trabalham em Portugal. Os dados obtidos foram objeto de um tratamento estatístico simples, nomeadamente análise de frequências e médias. A principal conclusão do estudo revela que os usuários, de uma forma geral, constituem uma proteção para a segurança dos sistemas de informação nas organizações.

Palavras-chave: sistemas de informação; tecnologias de informação e comunicação; segurança dos sistemas de informação; comportamento dos usuários.

ABSTRACT

To guarantee their continuity and success in an increasingly global and changing society, where organizations need to have useful and necessary information always

---

Manuscript first received/Recebido em: 02/03/2015 Manuscript accepted/Aprovado em: 12/07/2016
Address for correspondence / Endereço para correspondência

Alexandre Manuel Santareno, Mestre em Gestão pela Universidade de Évora, Portugal Especialista de Informática do Gabinete de Apoio à Informática da Escola Superior de Gestão e Tecnologia do Instituto Politécnico de Santarém, Santarém, Portugal. E-mail: correio@esg.ipsantarem.pt.

Rui Filipe Cerqueira Quaresma, Doutorado em Gestão pela Universidade de Sevilha, Espanha Professor Auxiliar do Departamento de Gestão da Escola de Ciências Sociais da Universidade de Évora, área de Negócio e Governo Eletrónico, Gestão de Operações e Empreendedorismo e Inovação Membro do Centro de Estudos e Formação Avançada em Gestão e Economia da Universidade de Évora (CEFAGE-UE). E-mail: quaresma@uevora.pt.

Published by/ Publicado por: TECSI FEA USP – 2016 All rights reserved

available in a fast and efficient manner in order to develop their daily activities, information security becomes a key factor. This study is meant to know whether the behavior and actions of Information Systems users are a risk or a protection to these systems security. In order to reach this objective we carried out a bibliographical review based on secondary sources that allowed us to develop a questionnaire for data collection. Secondly we used an online questionnaire to gather answers from 780 subjects who worked mainly in Portugal. The collected data were subject to a simple statistical treatment, specially frequency and analysis of means. The main conclusion derived from this study shows that in general users are considered to be a protection for the information systems security in organizations.

Keywords: information systems; information and communication technologies; information systems security; users' behavior.

1. INTRODUÇÃO

Num mundo cada vez mais competitivo, onde a informação é vital para todas as organizações, estas procuram ter sempre disponível a informação de forma rápida, íntegra e confidencial. 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 e confidencialidade da informação que recolhem, processam, armazenam e distribuem, há um fator muito importante a ter em consideração, para além da tecnologia propriamente dita e de todos os mecanismos de segurança que venham a adotar, que são os usuários dos SI/TI. Se estes não tiverem observarem um conjunto de práticas e regras na utilização dos SI/TI, corre-se o risco de gerar informação incoerente, desfasada da realidade e, consequentemente, levar a tomadas de decisão incorretas. Segundo (Kruger & Kearney, 2008), os usuários devem ser sensibilizados para as questões de segurança, nomeadamente para os efeitos negativos que uma falha ou quebra de segurança podem provocar. De acordo com(Furnell & Thomson, 2009), um dos grandes problemas e ameaças verificados na implementação de práticas e procedimentos na segurança da informação são os usuários. Por este fato, torna-se necessário promover dentro da organização uma cultura de segurança e assegurar que as boas práticas são uma componente natural do comportamento dos usuários.

Os usuários 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 corretas e seguras no desempenho das suas tarefas.

Assim, com este trabalho pretende-se saber em que medida os comportamentos (conjunto de ações observáveis) e as atitudes (maneira de pensar, sentir e reagir que leva a um determinado comportamento) dos usuários constituem um risco ou uma proteção para a segurança dos SI nas organizações.

A realização deste trabalho, além da pesquisa bibliográfica sobre o assunto, assentou na recolha de dados efetuada através de um questionário *online*, tendo sido construído e disponibilizado um *Website* para esse efeito, o qual esteve disponível entre os dias 31 de janeiro de 2011 e 31 de março de 2011. O pedido de resposta ao questionário foi efetuado através de uma mensagem de correio eletrónico, que teve como destinatários os usuários dos SI/TI nas organizações.

2. REVISÃO DA LITERATURA

Devido às constantes mudanças que ocorrem no seu meio ambiente, como a globalização dos mercados e a evolução das Tecnologias de Informação (TI), as organizações deparam-se com novas realidades e formas de realizar o seu negócio, pelo que, de acordo com(Serrano & 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. O SI é definido por (Rodrigues, 2002) como um conjunto de procedimentos, atividades, pessoas e tecnologias envolvidos na coleta de dados relevantes, armazenamento enquanto necessário, processamento dos dados e na disponibilização de informação a quem necessite da mesma. (Dhillon, 2005) refere também 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 usuários, a alteração de rotinas, regras e responsabilidades.

A informação tratada pelos SI, segundo(Varajão, 1998), 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 ações ou decisões de quem os utiliza. No entanto, esta nova 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 atividade das organizações.

Segundo (Dhillon, 2004), a definição de segurança da informação abarca a confidencialidade, a integridade, a responsabilidade, a honestidade das pessoas, a confiança e a ética. Para além destes aspectos, (Gaivéo, 2008) refere que associado às questões de segurança da informação, existem ameaças, vulnerabilidades, ataques e riscos que podem afetar a atividade dos SI nas organizações, pelo que é essencial proceder à sua identificação e caracterização para uma melhor resposta e proteção dos SI no caso de se verificar alguma destas ocorrências.

A informação representa o 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 fator humano. (Ng, Kankanhalli, & Xu, 2009) referem que os usuários nas organizações têm um papel crucial na prevenção e detecção das violações de segurança. Para que exista uma segurança realmente eficaz, os usuários têm que agir de uma forma consciente, cumprir as políticas de segurança da organização e adotar comportamentos que não comprometam a segurança dos SI. Os usuários estão conscientes da importância do seu papel na segurança da informação na realização do seu trabalho (Furnell & Thomson, 2009) e (Kruger, Drevin, & Steyn, 2006).

As organizações têm que desenvolver ações, e adaptar a sua estrutura para evitar atitudes fraudulentas, corrupção, dano e distorção da informação pelos usuários (Dhillon & Backhous, 2000)(Leach, 2003).

Para (Knapp, Morris, Marshall, & Byrd, 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. 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 aspetos sociais (Dhillon, 2004).

De acordo com (Knapp, Morris, Marshall, & Byrd, 2009), a definição, planejamento e controle de políticas de segurança da informação passa por estabelecer o

(cc) BY

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. Para (Kruger & Kearney, 2008), a implementação efetiva de controles de segurança depende da criação e divulgação de um conjunto de boas práticas e comportamentos que sejam percebidos e adotados por todos os elementos da organização. As organizações, além de definirem procedimentos de segurança dos SI, devem motivar os usuários a aplicá-los, mostrando-lhes através de simulações que as suas ações podem provocar vulnerabilidades e, consequentemente, ataques aos SI da organização (Workman, Bommer, & Straub, 2008).

De acordo com (Rhee, Cheongtag, & Ryu, 2009), (Kruger & Kearney, 2008), (Workman, Bommer, & Straub, 2008), (Albrechtsen, 2007), os usuários devem, além dos mecanismos de segurança definidos, adotar as seguintes medidas de segurança no seu posto de trabalho:

- Aplicar as atualizações de segurança recomendadas
- Utilizar e atualizar com frequência os programas antivírus e *antispyware*
- Realizar cópias de segurança com regularidade
- Utilizar senhas 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 compartilhar ou divulgar as suas senhas com os outros
- Ser responsável e cuidadoso na utilização da Internet e do correio eletrônico
- 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 atos praticados têm consequências
- Utilizar um *firewall*.
- Bloquear o computador quando se ausentar
- Não utilizar *software* ilegal ou de compartilhamento de arquivos.

Para (Dhillon, 2001), os problemas relacionados com a segurança ocorrem devido à ausência de medidas de segurança da informação na organização. E até pode existir uma estrutura de medidas na organização, no entanto, é preciso transmiti-la corretamente aos colaboradores através dos canais de comunicação adequados.

3. METODOLOGIA

Considerando o objetivo principal deste trabalho, a população alvo deste estudo são todos aqueles que para realizar as suas tarefas numa organização utilizam SI/TI. Como o universo dos usuários 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. O instrumento selecionado para efetuar a coleta de dados é o questionário *online*, que

(cc) BY

esteve disponível para resposta entre 31 de janeiro e 31 de março de 2011; os dados obtidos, de respondentes que trabalham principalmente em Portugal, foram depois objeto de uma análise estatística quantitativa.

O questionário é composto por 3 grupos de questões, sendo que no grupo I as questões foram elaboradas tendo por base os procedimentos de segurança recomendados por diversos autores. A primeira questão do grupo I é utilizada como filtro para identificar quais os respondentes que cumprem os requisitos para preencher a totalidade do questionário, a segunda questão tem 27 alíneas que contém um conjunto de afirmações em que o respondente tem que escolher qual a opção que melhor caracteriza a sua opinião; na terceira questão são apresentadas 18 afirmações em que o respondente tem que escolher qual o seu grau de concordância ou discordância. O grupo II é composto por uma questão destinada a registar comentários ou sugestões, não sendo obrigatório o seu preenchimento; no grupo III são solicitados os dados de caracterização dos respondentes. Na questão dois do grupo I utilizou-se uma escala nominal e na questão três deste grupo utilizou-se uma escala ordinal, através de uma escala não comparativa de *Likert* de 1 a 5. Tanto na questão dois, como na três, algumas alíneas foram elaboradas na negativa com o intuito de obrigar o respondente a fazer uma análise cuidada da questão antes de responder.

A divulgação e o apelo à participação no questionário foram realizados através de uma mensagem de correio eletrônico dirigida aos usuários dos SI/TI nas organizações, onde se apresentava o objetivo do estudo, a forma de coleta dos dados, a hiperligação para o *Website* do questionário e a garantia de confidencialidade.

4. RESULTADOS E DISCUSSÃO

O questionário obteve um total de 817 respostas, das quais 37 foram excluídas. Assim, foram admitidos no estudo 780 elementos, passando a designar-se por "respostas válidas", uma vez que a população alvo deste estudo desenvolve a sua atividade usando o computador como recurso.

A. Caracterização dos respondentes

Neste ponto é apresentada uma caracterização do perfil dos elementos (780) que compõem o estudo, e que desenvolvem a sua atividade profissional nas organizações como recurso o computador (ver Tabela I). Apenas 3 elementos indicaram desempenhar a sua atividade fora de Portugal, 1 no Brasil, 1 em Espanha e 1 em Inglaterra.

Das 780 respostas válidas, 55,1 % são do sexo feminino e 44,9% do masculino; no que se refere ao escalão etário, 63,7% situam-se no escalão 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.

TABELA I. Caracterização dos respondentes

Característica		**Número**	**%**
Gênero	Masculino	350	44,9
	Feminino	**430**	**55,1**
Idade	16 - 29 anos	109	14,0
	30 - 49 anos	**497**	**63,7**

(cc) BY

	50 - 64 anos	170	21,8
	Mais de 64	4	0,5
Habilitações Literárias	**Curso Superior (B/L)**	**371**	**47,6**
	Curso Pós-Graduado	310	39,7
	Ensino Secundário (12º)	68	8,7
	Outros níveis	31	4,0
Nº Funcionários Organização	Menos de 10	47	6,0
	10 a 49	89	11,4
	50 a 249	**335**	**42,9**
	250 ou mais	271	34,7
	Não sei	38	4,9

Em termos do grau de ensino mais elevado concluído pelos respondentes, constata-se que 87,3% têm formação superior (47,6% + 39,7%), aspecto bastante importante na medida em que, quanto maior o nível de formação maior a capacidade para entenderem as questões relacionadas com a segurança da informação.

Quanto ao número de trabalhadores da organização, 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 com menos de 10 funcionários e 4,9% não sabe o número de funcionários da organização onde trabalham.

B. Análise dos resultados

Os resultados a seguir apresentados resultam das 27 alíneas da questão 2 e das 18 afirmações da questão 3 do grupo I, que tinham como objetivo identificar se os comportamentos e atitudes adotados pelos respondentes estão de acordo com os procedimentos de segurança recomendados.

Atualizações de segurança

Cerca de 75% dos respondentes efetuam as atualizações de segurança do sistema operativo e também consideram importante efetuar as atualizações das mesmas (figura 1), o que são comportamentos e atitudes corretas.

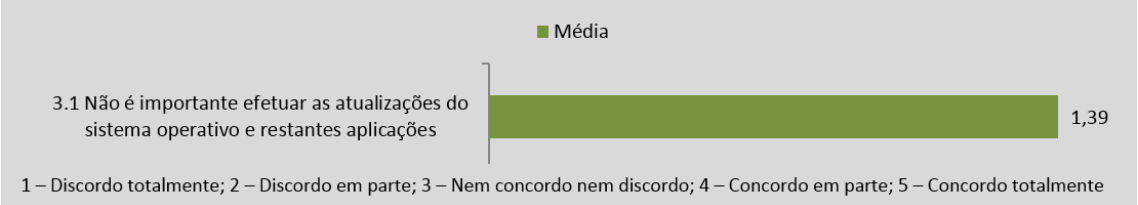


Figura 1 - Respostas ao procedimento atualizações de segurança

(cc) BY

Em face a estes resultados, fica comprovado que os usuários apresentam um comportamento e uma atitude de acordo com o recomendado, como referem (Rhee, Cheongtag, & Ryu, 2009), que mencionam que os usuários devem, além dos mecanismos de segurança definidos, aplicar as atualizações de segurança recomendadas.

Programas antivírus e *antispyware*

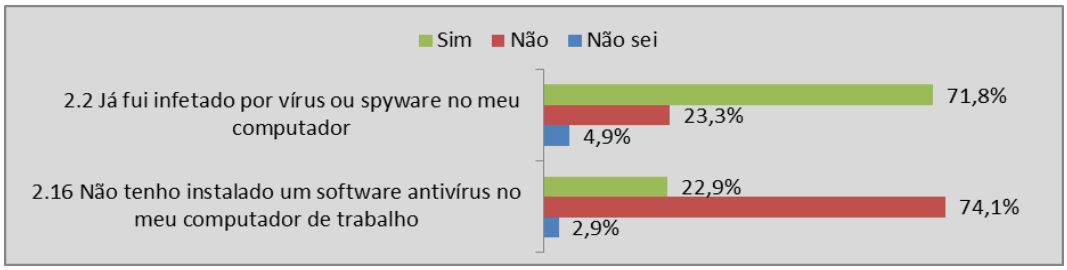


Figura 2 - Respostas ao procedimento antivírus e *antispyware*

A análise das figuras 2 e 3 permite verificar que os respondentes, têm um comportamento e uma atitude considerados adequados, pois não só têm instalado *software* antivírus no seu computador, como atribuem a este tipo de programas capacidade de proteção do computador. No entanto, a grande maioria revela que já foi infectada por vírus, razão pela qual os usuários devem ter maior atenção neste ponto e não adotar comportamentos de risco. Como mencionam (Mamede, 2006) e (Rhee, Cheongtag, & Ryu, 2009), embora as organizações possuam programas antivírus e *antispyware* instalados e atualizados, estes podem vir a relevar-se ineficazes devido às ações dos usuários.

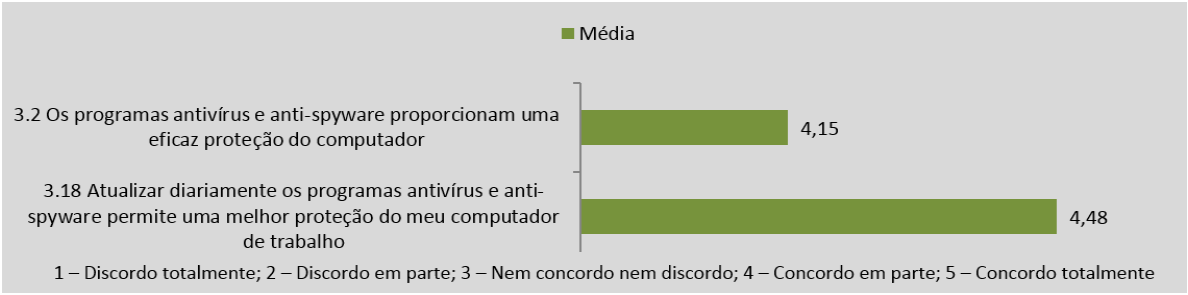


Figura 3 - Valor médio das respostas ao procedimento antivírus e *antispyware*

De fato, os programas antivírus e *antispyware* não garantem a proteção total, pois mesmo com estes tipos de programa é necessário algum cuidado por parte dos usuários, que não devem adotar comportamentos de risco. A atitude dos usuários em relação a estes tipos de programa (figura 3), indicia uma consciência de que não há proteção total.

Cópias de segurança

(cc) BY

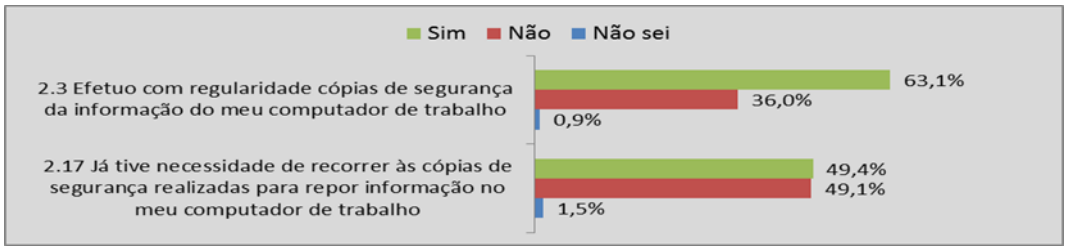


Figura 4 - Respostas ao procedimento cópias de segurança

Embora a maioria dos usuários (63,1%) apresente um comportamento adequado, ao indicar que efetua com regularidade cópias de segurança, há ainda uma percentagem de usuários, 36,0%, que não estão devidamente sensibilizados para a importância da sua realização.

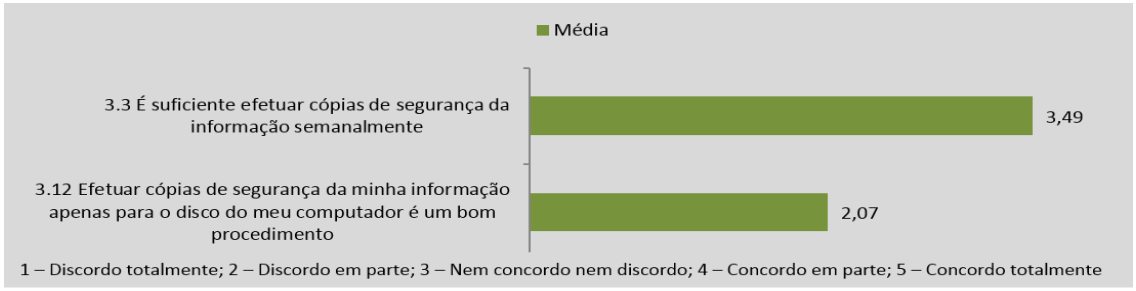


Figura 5 - Valor médio das respostas ao procedimento cópias de segurança

Tendo em atenção os valores obtidos nestas questões (figuras 4 e 5), podemos considerar que os usuários apresentam comportamentos e atitudes aceitáveis quanto à realização das cópias de segurança. Em nossa opinião, a percentagem dos usuários que realizam com regularidade cópias de segurança deveria estar próxima dos 100% e, por outro lado, a atitude dos usuários em relação a este tema também pode ser melhorada. Como referem (Rhee, Cheongtag, & Ryu, 2009), os usuários devem estar conscientes da importância de realizarem com regularidade as cópias de segurança.

Senhas robustas e diferentes

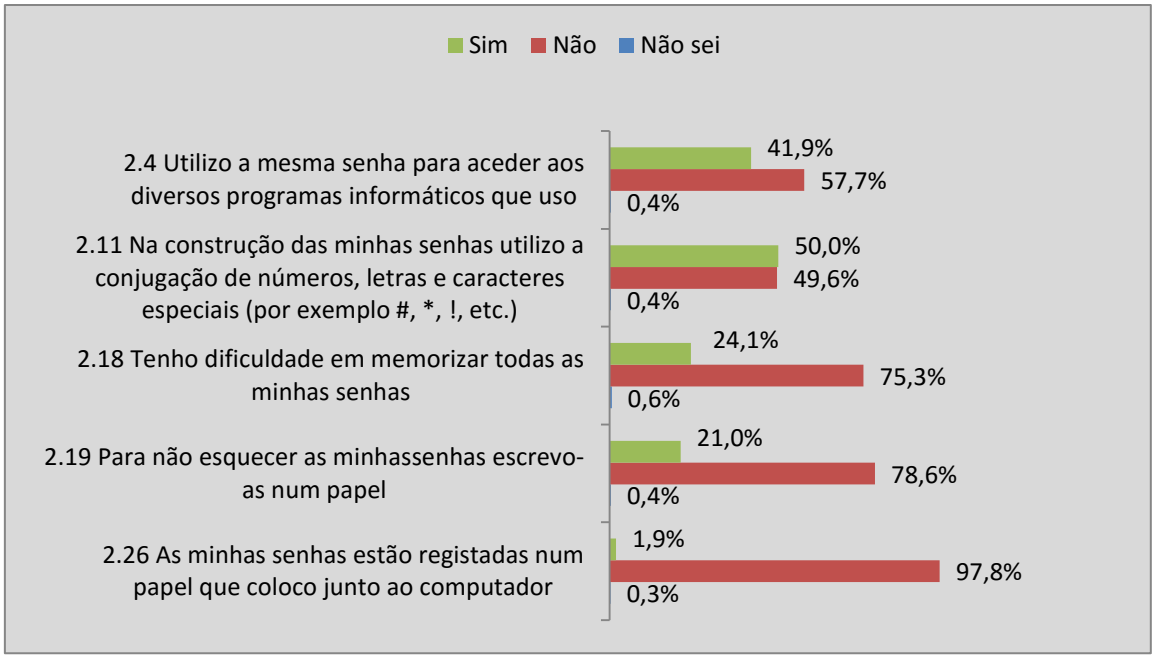


Figura 6 - Respostas ao procedimento de construção das senhas

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

De acordo com o observado na figura 7, os respondentes parecem concordar que é uma atitude correta alterar as senhas uma vez por ano, no entanto quando são solicitados a proceder à sua alteração optam pelas fáceis de memorizar, o que não é a atitude mais correta, devendo os usuários procurar utilizar senhas robustas como referem (Rhee, Cheongtag, & Ryu, 2009).

Figura 7 - Valor médio das respostas ao procedimento de construção das senhas

Como se observa pelas figuras anteriores, só metade dos usuários aplica as regras de construção das senhas, o que é um valor baixo; como refere (Mamede, 2006), na construção das senhas os usuários, devem combinar sinais, caracteres e números.

Em face aos valores obtidos, os usuários apresentam comportamentos e atitudes positivas na utilização das senhas, contudo ainda há aspectos a melhorar,

(cc) BY

nomeadamente quanto à sua robustez e à periodicidade da sua alteração. Por outro lado, e como referem (Rhee, Cheongtag, & Ryu, 2009), os usuários devem utilizar senhas diferentes para programas informáticos diferentes; contudo, esta situação nem sempre é possível, pois algumas organizações integram todos os seus sistemas, o que implica a utilização de uma única senha.

Encriptação da informação

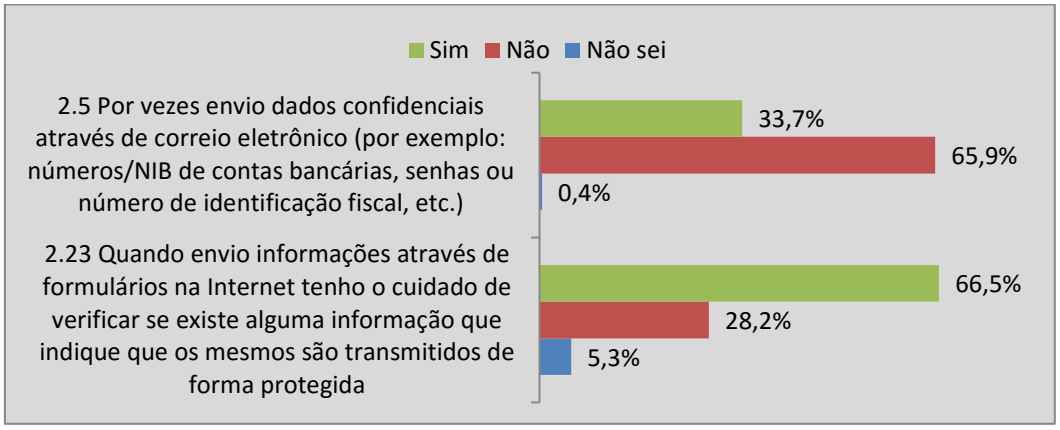


Figura 8 - Respostas ao procedimento de envio da informação encriptada

Como se pode observar na figura 8, a maioria dos respondentes tem 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, Cheongtag, & Ryu, 2009), e coincide com a atitude revelada pelos respondentes. Dado que esta questão foi colocada na negativa, o valor médio "desejável" deveria ser 1,0.

Figura 9 - Valor médio das respostas ao procedimento de envio da informação encriptada

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

(cc) BY

Comartilhamento da informação e do computador

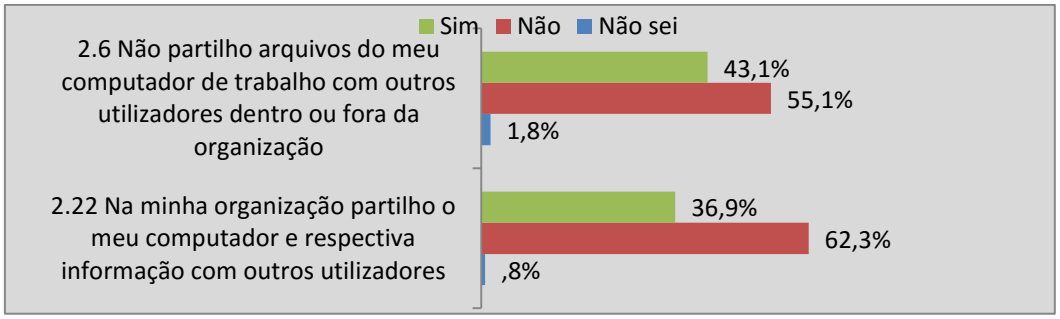


Figura 10 - Respostas ao procedimento de compartilhamento de informação

Neste procedimento, e segundo o ilustrado, mais de metade dos respondentes (55,1%) compartilham informação com outros usuários. No entanto, este fato é uma inevitabilidade na maioria dos locais de trabalho, pois os usuários necessitam compartilhar informação. Os usuários referem também (36,9%) que compartilham o seu computador e respe tiva informação com outros usuários, o que pode vir a comprometer a segurança da informação. Em face deste cenário, os usuários têm que estar cientes do perigo que representam estes comportamentos, devendo ser cautelosos e adotar as medidas necessárias de modo a garantir a integridade e segurança dos SI, como referem (Rhee, Cheongtag, & Ryu, 2009). Em concreto, e se for necessária ocompartilhamento de equipamentos, devem ser definidas áreas de trabalho distintas, uma para cada usuário, além de instalar e usar mecanismos de proteção, como os programas antivírus.

Partilha de senhas

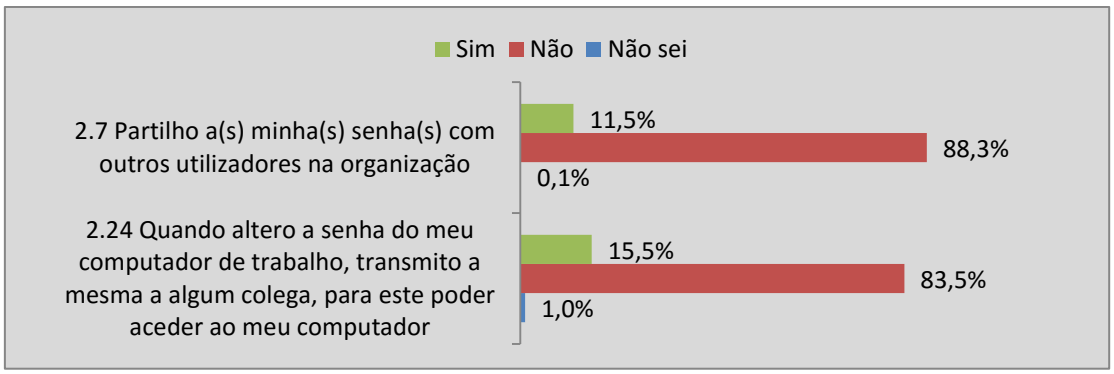


Figura 11 - Respostas ao procedimento do compartilhamento ou divulgação das senhas

As respostas às questões 2.7 e 2.24 revelam que 88,3% e 83,5% dos usuários respetivamente, não compartilham e não transmitem as suas senhas a outros usuários, portanto neste procedimento os respondentes apresentam um comportamento adequado como referem (Rhee, Cheongtag, & Ryu, 2009).

Da análise da figura 12 podemos visualizar que os respondentes têm uma atitude correta, ao indicarem que não é seguro a partilha das senhas com os colegas de trabalho. No entanto, o valor obtido nesta questão deveria ser a média de 1,0, dado que a questão foi colocada na negativa; há, assim, condições e necessidade de melhorar este indicador,

(cc) BY

pois como indicam(Herath & Rao, 2009), os usuários devem evitar o compartilhamento de senhas com outros usuários.

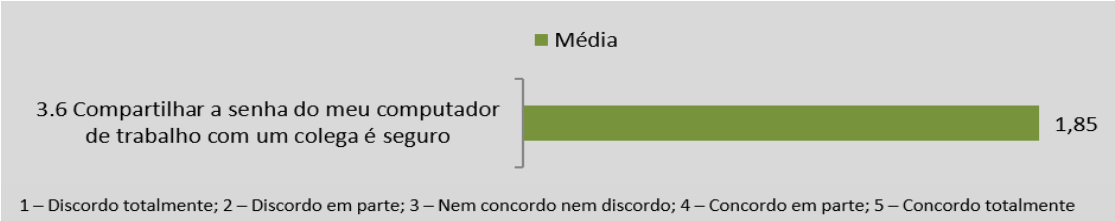


Figura 12 – Valor médio das respostas ao procedimento de compartilhamento das senhas

Pela observação dos resultados obtidos podemos considerar que neste procedimento os usuários apresentam um comportamento e uma atitude de acordo com o recomendado, embora ainda possa ser objeto de melhoria.

Internet e correio eletrônico

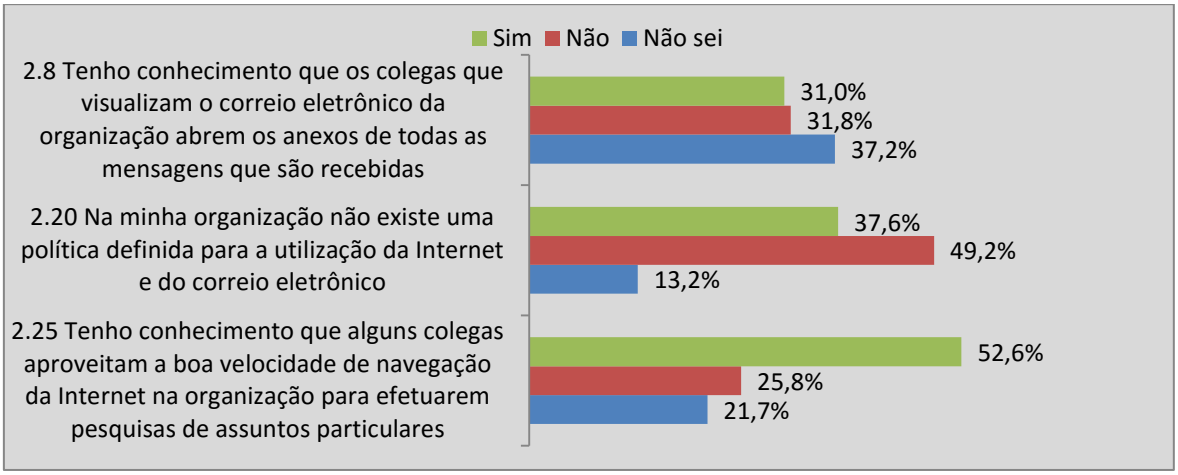


Figura 13 - Respostas ao procedimento de utilização da Internet e correio eletrônico

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 (37,6% + 13,2%) indica que não existe ou não sabe da existência de uma política definida para a utilização da Internet e do correio eletrônico, o que revela falta de sensibilização e cuidado por parte dos responsáveis das organizações onde os respondentes trabalham. (Kruger & Kearney, 2008) referem que os usuários têm que ser responsáveis e cuidadosos na utilização da Internet e do correio eletrônico e, para isso, é importante a definição e divulgação, no seio das organizações, de uma política para a utilização da Internet e do correio eletrônico. Relativamente à questão 2.8, e em face dos resultados obtidos, consideramos ser uma situação potencialmente perigosa para os SI das organizações o fato de alguns usuários abrirem todos os arquivosanexos das mensagens.

A análise da figura 14 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 eletrônico e enviarem para o lixo as mensagens de remetentes

(cc) BY

desconhecidos. É claro que o envio de mensagens de remetentes desconhecidos para o lixo implica algum bom senso. Ou seja, mesmo sendo de um remetente desconhecido, a eliminação da mensagem deve ser precedida de uma leitura do respetivo assunto e uma análise do seu texto, para determinar se a mensagem é cível e, consequentemente, merecedora de atenção.

Figura 14 - Valor médio das respostas ao procedimento de utilização da Internet e correio eletrônico

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

Equipamentos de armazenamento externos

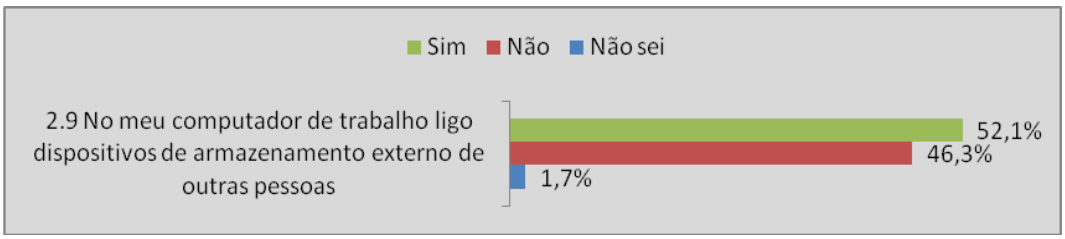
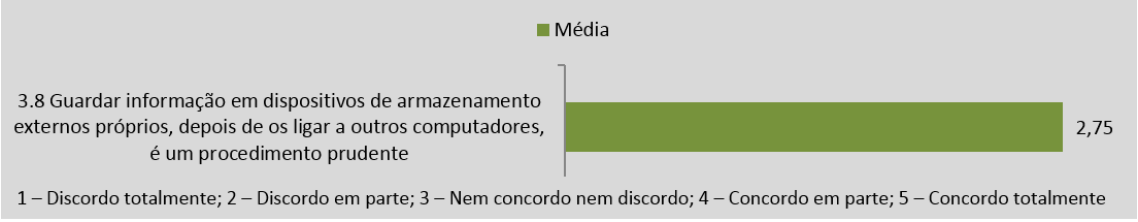


Figura 15 - Respostas ao procedimento de utilização de equipamentos de armazenamento externo

Como se pode observar na figura 15, 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 & Kearney, 2008), os usuários devem estar sensibilizados e ser cuidadosos na utilização de equipamentos de armazenamento externo. Os respondentes, como se pode comprovar pela figura 16, 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 & Kearney, 2008).



(cc) BY

Figura 16 - Valor médio das respostas ao procedimento de utilização de equipamentos de armazenamento externo

Neste procedimento os usuários 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 atividades, portanto os usuários devem estar cientes dos perigos que advêm desta situação, devendo utilizar de forma racional e cuidadosa os dispositivos de armazenamento externo.

Incidentes com os sistemas de informação

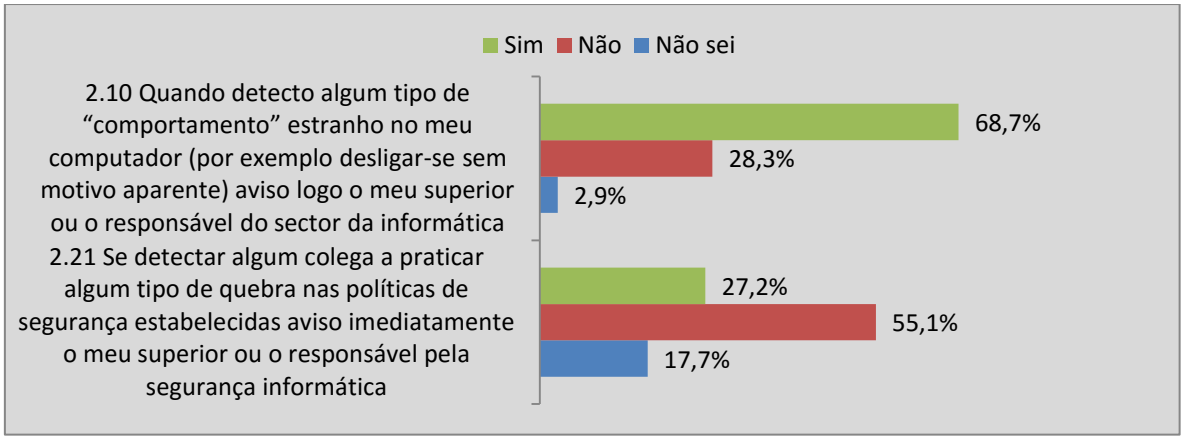


Figura 17 - Respostas ao procedimento de incidentes com vírus, roubos ou perdas de informação

Cerca de 69% dos respondentes revela que se detectar algum tipo de anomalia no seu computador comunica o sucedido ao seu superior ou responsável pela informática, como pode ser observado na figura 17, o que de acordo com (Kruger & Kearney, 2008) é um comportamento adequado. A maioria dos usuários, 55,1%, indica que se perceberalgum colega quebrando as políticas de segurança estabelecidas não toma a iniciativa de comunicar o sucedido aos superiores, situação que até pode ser compreensível, uma vez que a denúncia de um colega de trabalho é uma situação delicada.

Em termos de atitude, e como se pode observar pela figura 18, as respostas dos usuários indiciam que este é um aspecto a melhorar, dado que o valor deveria ser mais próximo de 1,0.

Figura 18 – Valor médio das respostas ao procedimento de incidentes com vírus, roubos ou perdas de informação

(cc) BY

Ou seja, é necessário sensibilizar os usuários para a importância e a necessidade decomunicar sempre qualquer anomalia, mesmo no caso de esta ser provocada por algum colega, tendo em contao perigo que pode representar para os SI da organização.

Consciência dos atos praticados

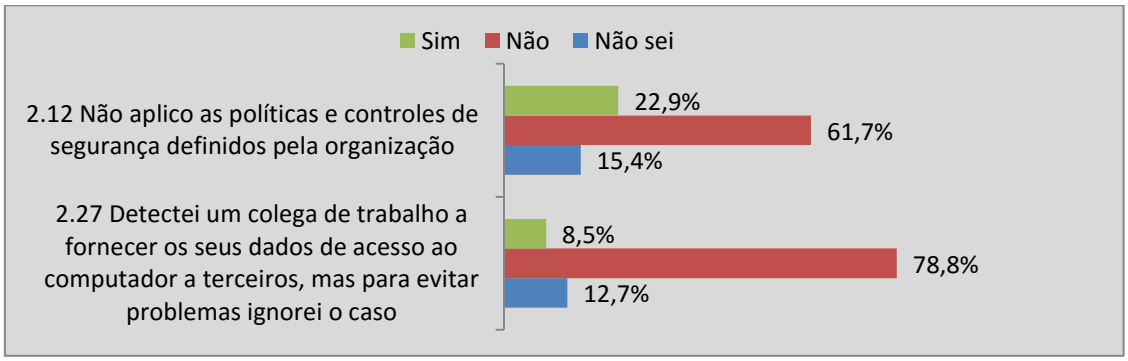


Figura 19 - Respostas às questões relacionadas com as consequências dos atos

Segundo o ilustrado na figura 19, 61,7%, dos respondentes revela que aplica as políticas e controles de segurança definidos pela organização, o que é um comportamento adequado segundo (Kruger & Kearney, 2008). Embora o resultado seja positivo, fica aquém do valor desejável, 100%, pois a segurança dos SI da organização passa, também, pela aplicação das políticas e controles de segurança definidos.Por outro lado, 78,8%, dos respondentes indica que já detectou algum colega fornecendo os seus dados de acesso ao computador a terceiros e não ignorou a situação, o que demonstra que os usuários estão cientes das consequências nefastas que esta situação pode causar nos SI da organização.

A maioria dos respondentes reconhece a importância de a organização apresentar através de um documento escrito as políticas de segurança, bem como informações sobre as políticas de segurança, como se pode comprovar pelos dados da figura 20.

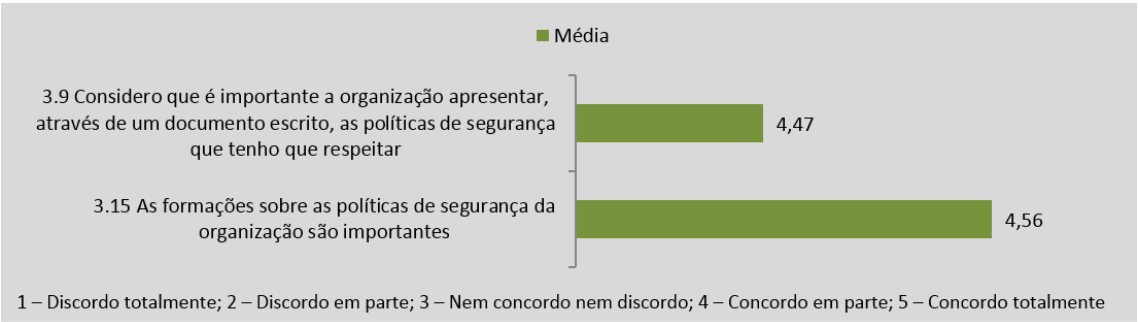


Figura 20 - Valor médio das respostas às questões relacionadas com as consequências dos atos

Em face aos resultados obtidos neste tópico, os respondentes apresentam um comportamento e atitudes de acordo com o recomendado.

(cc) BY

Utilização de *firewall*

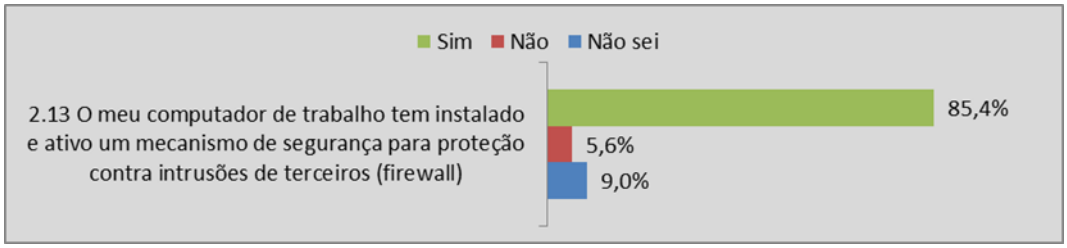


Figura 21 - Respostas ao procedimento de utilização de *firewall*

Os respondentes, 85,4%, indicam que têm instalado e ativo um mecanismo de segurança contra terceiros, como se pode observar na figura 21, o que é um comportamento de acordo com o recomendado.

Reconhecem também, como se pode visualizar na figura 22, a importância da utilização de *software* antivírus e contra a intrusão de terceiros (*firewall*) pela organização, o que revela uma atitude correta.

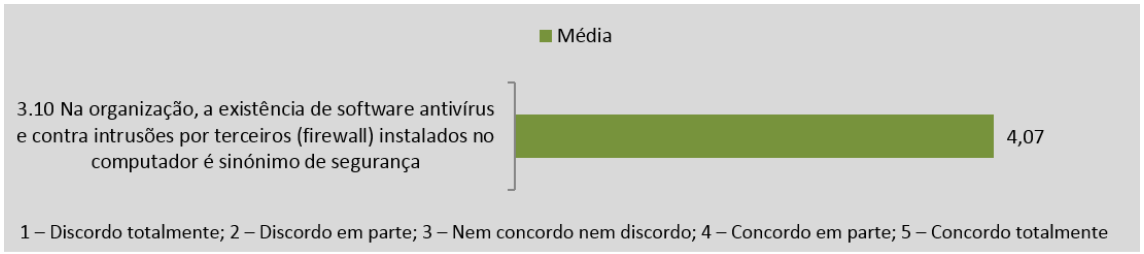


Figura 22 - Valor médio das respostas ao procedimento de utilização de *firewall*

De acordo com os resultados obtidos, os usuários reconhecem a importância destes mecanismos para a segurança da organização, o que é um comportamento e atitude que está de acordo com o proferido por (Workman, Bommer, & Straub, 2008).

Bloqueio do computador

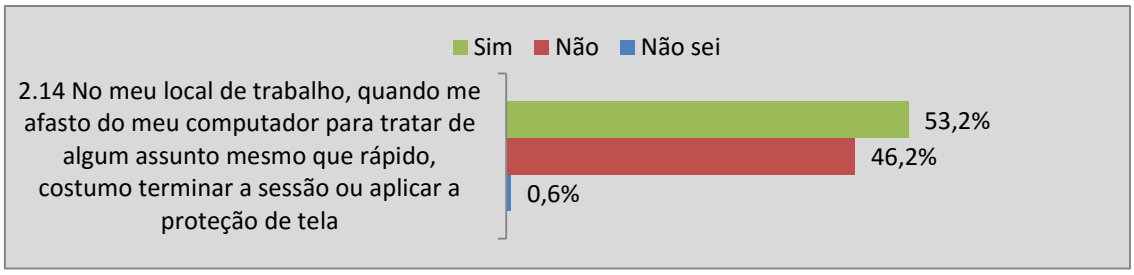


Figura 23 - Respostas ao procedimento bloqueio do computador quando se ausenta

Como se pode observar na figura 23, só 53,2%, dos respondentes é que termina a sessão ou aplica protecção de tela quando se afasta do seu computador. Este valor fica aquém do desejável, que deveria rondar os 100%, portanto neste procedimento os usuários apresentam um comportamento ainda longe do recomendado por (Albrechtsen, 2007).

(cc) BY

A análise da figura 24 revela que os respondentes ainda não têm uma atitude de acordo com o recomendado, considerando o valor de 2,75 de média das respostas, que indica não existir qualquer risco em deixar o computador ligado quando se afastam do mesmo.

Figura 24 - Valor médio das respostas ao procedimento bloqueio do computador quando se ausenta

Em face destes resultados, fica comprovado que neste procedimento os usuários devem rever e adequar o seu comportamento e atitude, bloqueando o computador quando se ausentam, como menciona (Albrechtsen, 2007).

Utilização de *software* ilegal

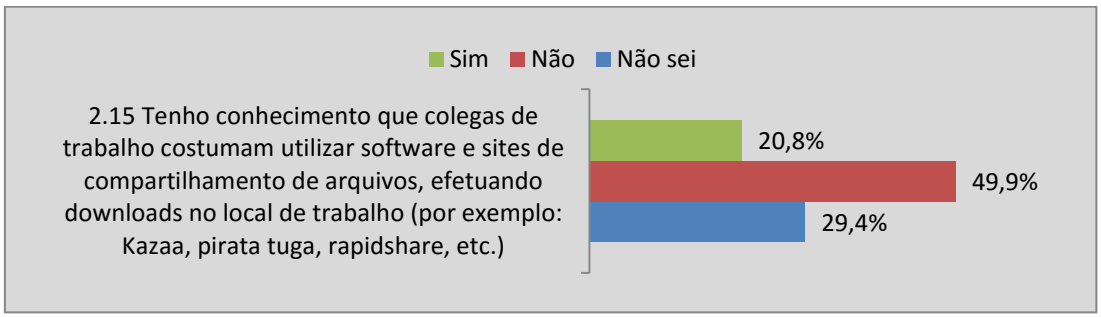


Figura 25 - Respostas ao procedimento não utilização de *software* ilegal

Só cerca de metade dos respondentes, 49,9%, indicam que os colegas de trabalho não utilizam *software* e *sites* de compatilhamento de arquivos , como se pode visualizar na figura 25, o que é um resultado manifestamente baixo, devido ao risco que este tipo de *software* representa para a segurança dos SI da organização.

De acordo com o observado na figura 26, os respondentes têm uma atitude correta ao reconhecerem que a utilização da Internet na organização para efetuar *download* de filmes e jogos representa uma ameaça para a segurança do SI.

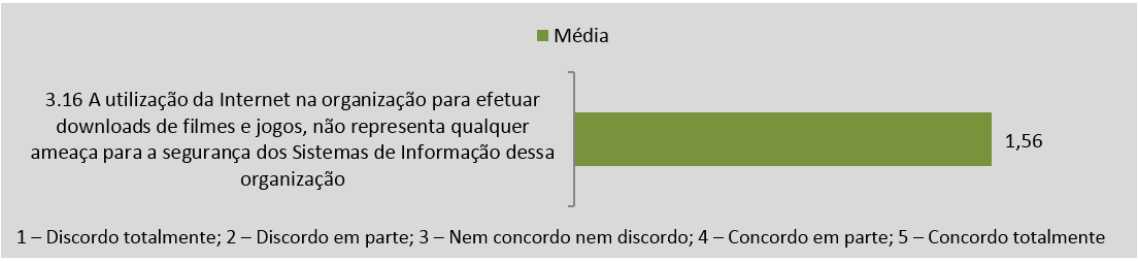


Figura 26 - Valor médio das respostas ao procedimento não utilização de *software* ilegal

(cc) BY

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

5. CONCLUSÕES DO ESTUDO

Este estudo teve como objetivo principal averiguar se os comportamentos e as atitudes dos usuários constituem um risco ou uma proteção para a segurança dos SI nas organizações.

Segundo (Workman, Bommer, & Straub, 2008), a principal ameaça à segurança é a falta de consciencialização dos usuários 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 análise dos dados deste estudo permitiu concluir que, de uma forma geral, os usuários apresentam-se como uma proteção para a segurança da informação nos SI das organizações, pelo fato de assumirem comportamentos e atitudes corretas na maioria dos procedimentos de segurança recomendados por diversos autores. Como positivo, no comportamento e atitude revelados pelos usuários, destacamos:

- Aplicam as atualizações de segurança recomendadas
- Utilizam e atualizam com frequência os programas antivírus e *antispyware*
- Realizam cópias de segurança com regularidade
- Utilizam senhas 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 senhas com os outros
- Informam no caso de incidentes com vírus, roubos ou perdas de informação
- Estão cientes que todos os atos praticados têm consequências
- Utilizam um *firewall*.

Já no que se refere aos comportamentos e atitudes revelados pelos usuários, e que são considerados negativos, é de destacar:

- A maioria já foi infetada por vírus
- Optam por senhas fáceis de memorizar, em detrimento das de construção robusta
- Utilizam a Internet na organização para fins pessoais
- Ligam dispositivos de armazenamento externo de outras pessoas aos computadores de trabalho
- Não bloqueiam o seu computador quando se ausentam

Considerando alguns dos comportamentos e atitudes menos corretos por parte dos usuários, apresenta-se a seguir um conjunto de recomendações para que os usuários possam contribuir ainda mais para a segurança do SI:

- Ter cuidado com os vírus e *spyware*, pois constituem uma das grandes ameaças à segurança dos sistemas e tecnologias de informação

(cc) BY

- Utilizarem senhas robustas, através da construção que conjugue letras, números e caracteres, proceder à sua mudança regularmente e não compartilha-las com terceiros
- Embora o compartilhamento de arquivos seja necessário, os usuários devem ter todo o cuidado ao fazê-lo e rejeitar todos os arquivos de origem desconhecida ou não fidedigna
- Serem cuidadosos na utilização da Internet e do correio eletrônico, navegar ou procurar informação em *sites* com alguma fidedignidade/credibilidade, sob pena de poderem ser infectados por algum vírus ou outro tipo de *software* malicioso
- Ter cuidado com a utilização de equipamentos de armazenamento externo; ligar dispositivos externos no computador de trabalho representa um perigo, não sendo possível determinar antecipadamente se o dispositivo está infectado com vírus;mesmo que possuam antivírus instalados e atualizados é sempre um risco
- Efetuar sempre que possível cópia de segurança da informação do computador, para compartilhar na rede da organização ou para um suporte externo, devendo estes serem guardados num local diferente da localização do computador
- Bloquear ou terminar a sessão no seu computador sempre que se ausentar do seu posto de trabalho; mesmo que por pouco tempo, deve proceder-se ao bloqueio do mesmo, pois um usuário, com segundas intenções, 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, que têm como objetivo a proteção dos SI das organizações contra as diversas ameaças e ataques.

Estas recomendações, dirigidas aos usuários dos SI, podem ser alavancadas se tiverem um reforço por parte das organizações. Isto é, as organizações podem conseguir uma maior adesão dos usuários relativamente a estas recomendações se, elas próprias, tomarem medidas nesse sentido, nomeadamente:

- Exigirem a construção de senhas robustas e a sua alteração periódica
- Definirem e divulgarem uma política de utilização da Internet e do correio eletrônico
- Aplicarem mecanismos de controle e bloqueio de utilização da Internet e do correio eletrônico
- Bloquearem a ligação de dispositivos de armazenamento externos
- Definirem rotinas de *backup* automático dos arquivos de trabalho para servidores específicos.

A realização deste trabalho teve, naturalmente, algumas limitações. A principal prende-se ao fato de se ter utilizado uma amostra não probabilística por conveniência, portanto os resultados e as conclusões não podem ser extrapolados para o universo dos usuários de SI/TI. Outra limitação que encontrámos, foi a escassez de estudos sobre os comportamentos e as atitudes dos usuários na segurança dos SI nas organizações, para se poder fazer algum tipo de comparação com o presente estudo.

Em termos de investigações futuras, pensamos que seria interessante fazer o cruzamento de algumas variáveis de caracterização, como a dimensão da organização, o gênero ou a idade dos respondentes, e analisá-las para verificar se existem diferenças em função daquelas variáveis de caracterização.

(cc) BY

REFERÊNCIAS

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26 (4)*, 276-289.

Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security, 20 (2)*, 165-172.

Dhillon, G. (2004). Realizing benefits on an information security program. *Business Process Management Journal, 10 (3)*, 260-261.

Dhillon, G. (2005). Gaining benefits from IS/IT implementations: interpretations from case studies. *International Journal of Information Management, 25 (6)*, 502-515.

Dhillon, G., & Backhous, J. (2000). Information systems security management in the new millenium. *Communications of the ACM, 43 (7)*, 125-128.

Furnell, S., & Thomson, K.-L. (2009). From Culture to disobedience: recognising the varying user acceptance of IT security. *Computer Fraud & Security, 2009 (2)*, 5-10.

Gaivéo, J. M. (2008). As pessoas nos sistemas de gestão da segurança da informação (tese de doutoramento). Lisboa, Portugal. Obtido de http://repositorioaberto.uab.pt/handle/10400.2/1272

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47 (2)*, 154-165.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28 (7)*, 493-508.

Kruger, H. A., & Kearney, W. D. (2008). Consensus Ranking - An ICT security awareness case study. *Computers & Security, 27 (7)*, 493-508.

Kruger, H. A., Drevin, L., & Steyn, T. (2006). A Framework for Evaluating ICT Security Awareness. *Proceedings of the 2006 Information Security South Africa Conference*, (pp. 1-11). Sandton.

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22 (8)*, 685-692.

Mamede, H. S. (2006). *Segurança informática nas organizações.* Lisboa: FCA Editora Informática.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46 (5)*, 815-825.

Rhee, H.-S., Cheongtag, K., & Ryu, Y. U. (2009). Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior. *Computers & Security, 28 (8)*, 816-826.

Rodrigues, L. S. (2002). *Arquitecturas dos sistemas de informação.* Lisboa: FCA Editora de Informática.

Serrano, A., & Jardim, N. (2007). *Disaster recovery: um paradigma na gestão do conhecimento.* Lisboa: FCA Editora de Informática.

Varajão, J. Q. (1998). *A Arquitectura da gestão de sistemas de informação.*Lisboa: FCA Editora de Informática.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24 (6)*, 2799-2816.

(cc) BY