Instituto Politécnico de Setúbal

Escola Superior de Ciências Empresariais

O IMPACTO DA IMPLEMENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO NA USABILIDADE DOS SISTEMAS DE INFORMAÇÃO

Caso de Estudo

Manuel Tomás Martins Sequesseque

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de

MESTRE EM SISTEMAS DE INFORMAÇÃO ORGANIZACIONAIS

Orientador: Professor Doutor José Manuel Gaivéo

Setúbal, 2017

Dedicatória

À minha mãe Amélia e aos Sequesseques (irmãos), pelo amor e carinho, apesar da distância…

À minha noiva Raquel, pelo apoio incondicional.

Agradecimentos

A Deus pelo dom da vida e pela oportunidade que me concedeu em frequentar um curso de mestrado.

Ao meu orientador Professor Doutor José Gaivéo, pela pronta disponibilidade, sapiência, assertividade, rigor, bibliografia recomendada e pelo senso crítico apurado, atributos que constituíram uma base segura para a concretização deste projeto.

À Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal, nomeadamente aos professores do curso de Mestrado em Sistemas de Informação Organizacional e aos meus colegas, em particular à pela disponibilidade e interação ao longo do período curricular.

À minha mãe e aos meus irmãos pelo apoio e dedicação constante.

À minha noiva pela compreensão dos momentos que ficou privada de estar comigo, pelo encorajamento e pela crença em mim, e pela sabedoria demonstrada para dar ideias.

Aos amigos e familiares pelo constante apoio e pela motivação.

Agradeço também a todos os colaboradores do AT, que permitiram a realização da recolha de dados, pela sua disponibilidade e pela rápida devolução das respostas aos questionários.

E de uma forma geral, a todos os que, de forma direta ou indireta, contribuíram para a concretização deste trabalho.

Índice Geral

Índice de Figuras

Índice de Gráficos

Índice de Tabelas

Siglas e Acrónimos

AT	*Angola Telecom*
DFTI	Direção de Fábrica de TI
EDP	*Electronic Data Processing*
IHC	Interação Humano-Computador
IHCSec	Interação Humano-Computador e Segurança
IN	*Inteligence Netework*
ISO	*International Organization for Standardization*
ITGI	*IT Governance Institute*
NVD	*National Vulnerability Database*
NIST	*National Institute of Standard and Technology*
PDCA	*Plan Do Check Act*
PSSI	Política de Segurança de Sistemas de Informação
QuestGes	Questionário aos Gestores
QuestTec	Questionário aos Técnicos
QuestUF	Questionário aos Utilizadores Finais
QUIS	*Questionnaire for User Interface Satisfaction*
SGSI	Sistema de Gestão da Segurança da Informação
SI	Sistema de Informação
SIBC	Sistema de Informação Baseado em Computador
SOA	*Service Oriented Architectures*
TI	Tecnologia de Informação
TIC	Tecnologia de Informação e da Comunicação
USB	*Universal Serial Bus*

Resumo

Atualmente a informação é um recurso muito importante nas organizações, de tal modo que, o diferencial das empresas, a competitividade e o seu sucesso está ligado à valorização que dão à informação e ao Sistema de Informação (SI), termo utilizado para descrever um sistema que abrange pessoas, máquinas, e/ou métodos organizados para coletar, processar, transmitir e disseminar dados que representam informação para o utilizador. Portanto, com o intuito de assegurar que o SI esteja protegido ao máximo contra a quebra da confidencialidade, contra o comprometimento da integridade e contra a indisponibilidade de acesso aos recursos, as organizações investem na Segurança da Informação.

Um SI deve ser projetado tendo em atenção o utilizador em cenário de utilização, nomeadamente, a facilidade de utilização. Neste âmbito, surge usabilidade como característica do SI com objetivo de assegurar-se que a sua utilidade e a qualidade da interação se adequem aos requisitos dos utilizadores, às atividades da tarefa e ao contexto em que será utilizado.

O principal objetivo desta dissertação foi procurar avaliar os impactos da implementação da Segurança da Informação na usabilidade dos SI, isto é, após implementação da Segurança da Informação, perceber as alterações positivas ou negativas na facilidade de utilização dos SI.

Neste âmbito, para caracterizar o problema em estudo, foi realizado um enquadramento teórico que discorreu sobre, Informação, Sistemas de Informação e Tecnologias da Informação e Comunicação, abordou também sobre a introdução ao conceito de Usabilidade e Segurança da Informação. Também foi feita a descrição da relevância da Usabilidade no contexto da Segurança da Informação, dando importância ao fator humano como o principal elemento para a segurança em cenário de utilização do SI.

Optou-se pela realização de um caso de estudo numa empresa angolana de telecomunicações. Para a recolha dos dados foram feitos inquéritos por questionário entregue aos colaboradores que estão há vários anos na organização e que viram a implementação da Segurança da Informação podendo descrever as alterações ao nível da segurança e da usabilidade do SI. Também aos colaboradores que estão há pouco tempo na organização e que não viram a implementação da Segurança da Informação e que ainda assim podem descrever os impactos positivos ou negativos que a segurança tem na facilidade de uso do SI.

Palavras-chave: Segurança da Informação, Sistema de Informação, Usabilidade.

Abstract

Actually, information is a very important resource into organizations. By the way, the companies differential, competitiveness and success are related to the value given to the information and Information System (IS), which is used to describe a system that includes people as well as machines and organized methods to collect, process, transmit and disseminate data representing information for the user. Then, because the goal of the companies is to ensure that de IS is protected against the confidentiality, risk of integrity and inaccessibility to the resources, the organizations invest in information security.

An Information System must be designed according to the user, to make it easily useful. IS has a characteristic which objective is to ensure that its usefulness and quality of interaction match with the user, with the work activities and with the context that it will be used.

The main objective of this dissertation is to evaluate the impact of the Information Security using the IS, that is, after the implementation of the Information Security, to understand the positive and negative changes on how the IS are used.

Characterizing the problem, in case, a theoretical framework was developed around the Information, around the Information System and around Information of technology and communication. An introduction was given to understand better the concepts of Usefulness and Information Security. One also, described the relevance of Usefulness in the context of Information System, pointing to the importance of Human factor as the main element for the security when IS is used.

We chose to carry out the case study, a firm of telecommunication in Angola. The data used was collected by using questionnaires answered by the collaborators who work for long in the firm, once they have seen the implementation of the security of the information what make them able to describe the changes on security and usefulness of IS. The same questionnaire was applied to those collaborators that work for the firm for not so long, in spite of that, they still can describe the positive and negative impacts of security using IS, making it easily used.

Keywords: Information Security, Information Systems, Usability.

1 Introdução

Atualmente interagir com sistemas computacionais deixou de ser privilégio de profissionais da área de computação e tornou-se em algo comum. Os desenvolvedores de Sistemas de Informação (SI) têm sido colocados em posição de influenciar a sociedade. Deste modo, é imperativo que eles desempenhem bem o seu trabalho, especificamente, no projeto de sistemas computacionais interativos onde há interação entre ser humano e computador e têm como função essencial prover suporte à atividade humana. Tal sistema habilita o ser humano a realizar as suas tarefas mais rapidamente, com menos erros, com aprendizado menor, com qualidade resultante maior e com satisfação também maior (Nielsen, 1993). Isto, contudo, depende de facilidade de utilização do sistema.

O SI de uma organização deve contemplar todos os elementos que sejam úteis à condução dos negócios da mesma. Portanto os SI devem ser projetados de forma a adaptarem-se às organizações, gerando as informações necessárias e importantes ao desenvolvimento das suas atividades. Por seu lado, a organização deve estar aberta às influências geradas pelo SI, eventualmente alterando a sua forma de trabalho. Todo o esforço representado pela implementação e manutenção dos SI é devida a importância da informação para a organização, deste modo justificando todo o empenho realizado, visando garantir a sua proteção e segurança, assegurando a continuidade das atividades que deles dependam.

Entre os vários componentes de um SI, a interface gráfica tem um papel de destaque na maioria das aplicações, já que ela está em contacto direto com o utilizador. Para este, a interface gráfica é o próprio sistema, ou seja, a perceção que o utilizador tem do SI é aquela oferecida pela interface (Galitz, 2002).

Por mais que um SI seja bem desenvolvido quanto à complexidade computacional e à integridade dos dados, caso a interface com o utilizador não seja adequada, toda a segurança do processo será afetada (Pereira & Paiva, 2011).

Perante isto, qualquer SI para ser bem-sucedido deve respeitar a facilidade de utilização (Carrol, 2009), que é tida frequentemente como inversamente proporcional à segurança da informação (Pereira & Paiva, 2011). Yee (2004) atribui esse conflito aos

desenvolvedores de sistemas que tratam a segurança e a facilidade de utilização, como complementos para um produto já acabado. Portanto é preciso haver um equilíbrio entre ambas, pois, não existe utilidade para um sistema inseguro, assim como não há necessidade de segurança num sistema que não seja utilizado.

A segurança da informação diz respeito à proteção de determinados dados, com a intenção de preservar os seus respetivos valores para uma organização ou um indivíduo (Pfleeger & Pfleeger, 2003). O conceito de segurança da informação é abrangente, pois ele está presente em qualquer atividade desenvolvida nos SI (Mamede, 2006). Envolve todos os colaboradores da organização, sendo sustentado por diferentes aspetos como culturais, tecnológicos e legais. Pode observar-se a complexidade tanto na quantidade de envolvidos (com diferentes especializações), como na diversidade de fatores e tecnologias a serem consideradas.

O presente trabalho tem como tema o impacto da implementação de segurança da informação na usabilidade dos SI. Pretende-se saber quais as maiores mudanças notadas pelos utilizadores finais, após a implementação dos *standards*, as principais vantagens e inconvenientes da implementação da segurança na facilidade de utilização do SI, de maneira a conhecer os seus impactos.

1.1 Objetivos

O trabalho tem como objetivo geral avaliar os impactos da implementação da Segurança da Informação na usabilidade dos SI, isto é, após implementação da Segurança da Informação, perceber as alterações positivas ou negativas na facilidade de utilização dos SI.

Como objetivos específicos:

Analisar os impactos decorrentes da implementação da Segurança da Informação na usabilidade dos SI:

I) Analisar se os utilizadores conseguem atingir os seus objetivos a nível de eficiência e de eficácia.

II) Avaliar a satisfação da utilização do SI.

III) Analisar a redução ou aumento de erros dos utilizadores com a utilização do SI.

IV) Perceber que relação de confiança têm os utilizadores com o SI.

1.2 Metodologia

A metodologia estuda todos os elementos que ajudam à condução da investigação a uma direção correta, descrevendo os vários métodos e técnicas específicas de recolha de dados para se obter resposta às questões levantadas no estudo.

Freixo (2010) e Fortin (2009) afirmam que as metodologias de investigação estão assentes num conjunto de meios que permitem realizar a investigação; enquanto, o método é uma forma de selecionar a técnica e a forma de avaliar alternativas para ação científica. Esta diferenciação indicia que uma metodologia pode recorrer a utilização de vários métodos.

As metodologias de investigação agrupam-se em dois tipos: metodologia quantitativa e metodologia qualitativa. A quantitativa é caracterizada pela sua objetividade, perfil mensurável e possível de ser generalizado a outros contextos; e a qualitativa é definida como sendo uma compreensão interpretativa da ação social (Minayo, 2005).

Neste trabalho, optou-se como metodologia o Estudo de Caso, porque, por um lado apresenta-se como a melhor forma de atingir os objetivos específicos traçados, por outro, deve-se ao facto de estes ajudarem a desenvolver e a melhorar a identificação de problemas. Optou-se por uma óptica qualitativa, porque o fenómeno que se pretende estudar neste trabalho é complexo e para se conseguir analisar os impactos decorrentes da implementação da Segurança da Informação na usabilidade dos SI. Para recolha de dados a opção é o inquérito por questionário.

Para Mazzotti (2006), o estudo de caso como estratégia de pesquisa caracteriza-se exatamente por esse interesse em casos únicos e não pelos métodos de investigação, os quais podem ser de carácter qualitativos ou quantitativos. Por seu lado, Yin (1994) afirma que a parte fundamental de um estudo de caso e orientação central entre todos os tipos, é

que ele tenta iluminar uma decisão: Porque elas foram tomadas? Como foram implementadas? E com que resultados?

De acordo com Yin (2005), a necessidade de estudar fenómenos sociais complexos é o motivo pelo qual realizam-se estudos de caso. Para o autor, os estudos de caso devem usar-se quando se lidam com situações e contextos específicos, confiando que essas situações podem ser pertinentes na investigação.

1.3 Estrutura da dissertação

O presente trabalho está estruturado em 6 capítulos:

- No capítulo 1 (**Introdução**) é feita a contextualização do trabalho, é apresentada a caracterização da problemática do tema, os objetivos e a metodologia.

- O capítulo 2 (**Enquadramento Teórico**) proporciona o enquadramento teórico acerca da temática, o conceito de Sistemas de Informação, os conceitos relacionados (Informação e Tecnologia da Informação e da Comunicação), os conceitos de Segurança da Informação e Usabilidade e a relevância da Usabilidade no contexto da Segurança da Informação.

- No capítulo 3 (**Caracterização da Organização**) – é feita a descrição da organização em estudo, a Angola Telecom, missão, visão e valores, organograma e caracterização do SI.

- O capítulo 4 (**Estudo de caso**) apresenta estudo de caso, a caracterização da população-alvo, a técnica de recolha de dados e refere a amostra usada. Apresenta-se ainda a elaboração dos questionários.

- O capítulo 5 (**Análise de Resultados**) faz a apresentação, análise crítica e discussão dos resultados obtidos através dos inquéritos, para tal foi realizada a sumarização e tratamento estatístico desses dados.

- O capítulo 6 (**Conclusão e perspetivas de trabalho futuro**) faz as conclusões dos resultados obtidos e apresenta as perspetivas de trabalho futuro que poderão dar continuidade ao estudo realizado.

Por fim são apresentadas as referências bibliográficas e os anexos, que são formados pelo Questionário Gestor (Anexo A), Questionário Técnico (Anexo B), Questionário Utilizadores Finais (Anexo C) e Resultados dos Questionários (Anexo D).

2 Enquadramento Teórico

Neste capítulo faz-se a revisão das diferentes abordagens existentes na literatura sobre os conceitos de SI e usabilidade dos SI nas organizações, e a forma como pode ser gerida. Neste contexto, é ainda dada especial relevância à satisfação do utilizador do SI e as suas métricas para avaliar o sucesso dos SI e melhorar a forma como a organização o utiliza. Posteriormente são referidas diferentes perspetivas e abordagens à Segurança da Informação e medidas de satisfação do utilizador do SI com as Práticas de Segurança da Informação.

2.1 Informação, Sistemas de Informação e Tecnologias da Informação e Comunicação

Neste subcapítulo serão abordados e explorados alguns dos aspetos fundamentais da realidade das organizações e SI, procurando-se estabelecer um enquadramento conceptual rigoroso de partida para o trabalho a desenvolver nos capítulos seguintes. São abordados aspetos importantes das organizações humanas, da atividade de gestão, da informação e do SI organizacional. São também tecidas diversas considerações sobre o papel e a importância da informação e do SI nas organizações.

2.1.1 Informação

O mundo vive atualmente num modelo em que a informação é um recurso valioso, exigindo das organizações uma gestão estratégica eficiente, a qual pode ser facilitada pela utilização de recursos inteligentes oferecidos pelas Tecnologias de Informação e da Comunicação (TIC). As transformações decorrentes do desenvolvimento tecnológico nas áreas de informação e comunicação afetaram significativamente a sociedade. Para acompanhar essas transformações, tanto as pessoas quanto as organizações têm procurado formas mais rápidas para se inserir nesse modelo atual de mercado chamado ‘Era da informação’.

De acordo com Ward e Griffiths (1996) a informação é reconhecida como sendo importante para as organizações atuais, constituindo, senão o mais importante, pelo menos um dos recursos cuja gestão e aproveitamento mais influência o sucesso das organizações. Mas, mais que ser reconhecida apenas como qualquer outro recurso a informação é também considerada e utilizada em muitas organizações como um fator estruturante e um instrumento de gestão da organização (Zorrinho, 1991), pelo que as organizações que têm maior acesso e melhor gestão da informação destacam-se no mercado. Entretanto, ter a dominância da informação não garante a estagnação estratégica dos concorrentes (Gartzke, 2013; Sheldon, 2011).

Porém, caracterizar informação implica caracterizar dados, isto é, para ser possível ter uma perceção total de informação torna-se necessário que se defina previamente o que são dados.

Dados são conjuntos de factos simples representando eventos ocorridos numa organização ou no seu ambiente físico, antes de serem organizados e ordenados num formato que as pessoas possam entender e usar (Laudon & Laudon 2000).

Os dados são a exposição das características dos elementos de forma simples, como dizem Qi et al., (2006), é a descrição abstrata de objetos, ou seja, o material em bruto utilizado para gerar informação e conhecimento útil. O entendimento dos autores aponta para uma hierarquização dos conceitos dados, informação e conhecimento, e assume que os dados são o ponto de partida para a obtenção dos restantes.

De acordo com McGarry (1999), a palavra "informação" tornou-se popular logo após a invenção da imprensa no século XV, quando normalmente se utilizava uma palavra em latim para expressar uma nova ideia ou conceito. A raiz do termo vem de *formatio* e *forma*, ambos são sinónimos de moldar ou dar forma a algo indeterminado.

Muitas definições de informação partilham da ideia base acima exposta, como é o caso do conceito proposto por Galliers e Baets, (1997), que diz que a informação é aquele conjunto de dados que quando fornecido de forma e a tempo adequado, melhora o conhecimento da pessoa que o recebe ficando ela mais habilitada a desenvolver determinada atividade ou a tomar determinada decisão.

Tendo em conta que uma organização passa por um processo para converter dados em informação, os seus processos de decisão, a sua estrutura administrativa e a sua forma de trabalhar começam a transformar-se (Drucker, 1993). Isto leva-nos a considerar que a quantidade de informação e os dados donde ela provém, são, para a organização, um importante recurso que necessita e merece ser gerido.

A diferenciação das organizações atuais faz-se ao nível da sua capacidade de gestão interna e de criação de informação. Pois de acordo com Siqueira (2005) a informação representa, atualmente, uma importante ferramenta no processo de tomada de decisões, uma vez que a sua análise permite à empresa perceber oportunidades e ameaças à sua operação, e a deteção de problemas e tendências. Desta forma, é inequívoca a relação entre a utilização e gestão da informação e a obtenção de vantagens competitivas.

De acordo com Siqueira (2005) o conhecimento é derivado das informações percebidas, decodificadas, interpretadas e armazenadas através dos processos cognitivos. Isto é, conhecimento deriva da informação assim como esta, dos dados.

De acordo com Davenport e Prusak (1998), o conhecimento pode ser comparado a um sistema vivo, que cresce e se modifica à medida que interage com o meio ambiente. Portanto, o conhecimento está estreitamente condicionado às capacidades humanas de perceção sensorial, de filtragem e processamento da informação e de armazenagem na memória. Ele existe dentro das pessoas e por isso é complexo e imprevisível.

2.1.2 **Sistemas de Informação**

Nos últimos tempos, a constante evolução dos modelos ligados aos processos produtivos, tem originado mudanças constantes e acentuadas na forma como as sociedades e as organizações lidam com a globalização, a informação disponível e com necessidade de racionalizar a informação. Esta evolução motivou a mudança da sociedade para uma sociedade da informação e do conhecimento (Castells, 2003). Na sociedade do conhecimento impera uma necessidade eminente por sistemas, tecnologias, mecanismos de gestão da informação imprescindíveis para que os próprios processos produtivos possam evoluir com a firmeza e rapidez necessárias (Starec et al., 2006).

Os SI pertencem aos modernos sistemas inteligentes, que surgiram como uma forma de contrariar a ideia de que qualquer sistema pode ser entendido se estudar as suas partes individualmente, ou seja, a ideia que o todo é igual à soma de suas partes. Segundo Morville (2014), o mundo é sistêmico e o todo não pode ser totalmente compreendido somente pelas suas partes constituintes, devendo para o efeito, observar-se ver o todo e a interação entre as partes.

No contexto atual os SI podem fazer a diferença entre o sucesso e o fracasso, perante os mercados onde as organizações se vêm forçadas a competir. As organizações cada vez mais recorrem a utilização de SI para suportar o crescente fluxo de informação, tanto internas como externas, com objetivo de facilitar e melhorar o processo de decisão (Khauaja & Campomar, 2007).

Um SI pode ser definido como um conjunto de componentes inter-relacionados trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir a informação com a finalidade de facilitar o planeamento, o controlo, a coordenação, a análise e o processo de decisão nas empresas e organizações (Laudon & Laudon, 2012). Trata-se de uma combinação estruturada de informação, recursos humanos, TI e práticas de trabalho, organizado de forma a permitir o melhor atendimento dos objetivos das empresas (Cassaro, 2011).

Por seu lado, Alter (1999) define SI como sendo sistemas que usam as TICs para capturar, transmitir, armazenar, recuperar ou disponibilizar informação. Usam as TICs como mecanismos de suporte à gestão da informação imprescindíveis para que os processos de gestão da organização possam evoluir.

De acordo com Zorrinho (1995), o SI tem, por um lado, a função de reduzir a incerteza e apoiar a decisão, e por outro, criar representações da realidade que auxiliem a empresa a atingir os seus objetivos. A relação entre negócio e tecnologia funciona em duas perspetivas. A estratégia do negócio dá sentido à utilização das TICs, e estas alteram os pressupostos da estratégia tradicional. O ponto fulcral desta relação de aproximação é que as TICs não devem ser utilizadas apenas para melhorar ou acelerar os processos, mas também para conceber a própria organização.

Antes da automatização por computador, as informações acerca das organizações eram mantidas e salvaguardadas como registos em papel, dispersos em unidades de negócio e organizacionais distintas. Pelo que um SI pode ou não envolver a utilização de computadores mas, mesmo que conceptualmente seja aceitável a existência de SI sem a participação de computadores, a observação da realidade permite concluir que são muito raras as organizações que não integram computadores no seu SI (Bretschneider & Wittmer 1993).

Atualmente, o Sistema de Informação Baseado em Computador (SIBC), é muitas vezes sinónimo do conceito de SI em geral (excluindo no entanto, deste contexto, os sistemas operativos) Lopes et al. (2005). Os autores sugerem, no caso dos que se suportam nas Tecnologia de Informação (TI), devem ser referidos como SIBC, notando que estes constituem um subsistema do SI organizacional. Neste mesmo âmbito consideram a utilização do termo ‘sistema informático como sinónimo de SIBC.

A exigência do mercado competitivo, dinâmico e principalmente globalizado motiva as empresas a operarem com um SI eficiente, garantindo níveis mais elevados de produtividade e eficácia. Nesse contexto, Anunciação e Zorrinho (2006) declaram que o alinhamento organizacional implica o ajuste estrutural, contemplando a integração entre atividades de negócio, SI e TIC.

2.1.3 **Tecnologia da Informação e da Comunicação**

Segundo Amaral (1994) TIC, não é um conceito com um entendimento universal, pois, o referido conceito depende do ponto de vista da análise que cada pessoa faz. As TICs são alvo de grande número de definições possíveis sob perspetiva diferentes, mas não fugindo da sua essência, uma vez que todos os estudiosos apresentam praticamente a mesma ideia.

O conceito de TIC surge como conjunto de conhecimentos, baseados quer em equipamentos e programas quer na sua criação e utilização a nível pessoal e empresarial. Para Serrano et al., (2004), as TI envolvem, cada vez mais, não só *hardware* e *software*, mas também os sistemas de telecomunicações, levando por isso a uma utilização mais frequente, assumindo a abrangência do termo.

De acordo com Rascão (2004), TIC é o conjunto de conhecimentos, de meios materiais (infraestruturas) e de *know-how*, necessários à produção, comercialização e ou utilização de bens ou serviços relacionados com o armazenamento temporário ou permanente da informação, bem como o processamento e a comunicação da mesma.

De acordo com Sttaford e Hillyer (2012), TIC é tudo aquilo que suporta a cultura digital, desde o *hardware* até ao *software*. Com o passar do tempo tem existido um grande avanço e incorporação das TICs na vida quotidiana, na medida em que a criação e a gestão da informação bem como as comunicações passaram a assumir uma posição central face a todas as outras atividades.

De acordo com Lopes (2009), a capacidade tecnológica e desenvolvimento regional influenciam-se reciprocamente. A um padrão elevado espacial de adoção de novas tecnologias, corresponderá a novas atividades inovadoras, originando novas estruturas territoriais, através da instalação de empresas mais avançadas ou da reestruturação das existentes, mais eficientes e competitivas.

2.2 Introdução ao conceito de Usabilidade

A interface com o utilizador é parte fundamental dos SI. Por ser a parte visível do *software*, por meio da qual os utilizadores comunicam-se com os sistemas para executarem as suas tarefas, é necessário que ela seja amigável. Referir SI amigáveis, no sentido da facilidade de utilização, corresponde a um termo *user-friendly* surgido no início dos anos 80 referindo-se a um ecrã mais organizado e claro.

Segundo Heckel (1991), para se projetar boas interfaces, deve-se pensar mais em comunicação do que em computação. Afinal, atingir as expectativas e atender questões subjetivas das pessoas é tarefa para um bom comunicador que, ao escolher o tipo adequado de interface e os seus elementos, satisfaz o utilizador e incentiva a interação, num diálogo sem barreiras. Para Pressman (2006) se um programa não for *user-friendly* frequentemente estará condenado ao fracasso, mesmo que as funções que ele executa sejam valiosas.

O termo usabilidade começou a ser usado na década de 1980 para substituir a expressão *user-friendly* nas áreas da Psicologia e da Ergonomia. A substituição teve lugar

porque os utilizadores aperceberam-se que não precisam que as máquinas sejam amigáveis, mas sim que estas não interfiram nas tarefas que eles desejam realizar. Uma vez que um sistema pode ser considerado amigável para um utilizador e não tão amigável para outro, porque as necessidades são diferentes de um utilizador para outro (Dias 2003). Portanto a usabilidade passou a estar relacionada com o suporte aos utilizadores para atingirem um objetivo e não apenas uma característica da gestão da interação com o utilizador (Cockton, 2012).

Novas abordagens para a expressão interface com utilizador e para o campo da Interação Humano-Computador (IHC) surgiram: "um conjunto de processos, diálogos e ações por meio dos quais um ser humano utiliza e interage com um computador" (Baecker & Buxton, 1987). Para Barbosa e Silva (2010), IHC é uma área interdisciplinar de pesquisa aplicada e prática de *design* que realiza o estudo formal na relação cognitiva entre as atividades das pessoas, o artefacto do computador, e as suas relações.

A IHC, segundo Te'Eni et al. (2007), não é só a interface entre o utilizador e a tecnologia, mas também é a forma de aprimorar tal relação. É o *design* que produz a ligação entre o utilizador, a máquina, e os serviços requeridos, a fim de uma boa performance. Na mesma perspetiva, Carroll (2013) diz que a IHC abrange compreender à ligação das infraestruturas e ferramentas às práticas humanas contemporâneas.

O conceito de usabilidade foi evoluindo continuamente e tornou-se cada vez mais abrangente. Atualmente a usabilidade integra, qualidades como diversão, bem-estar, eficácia coletiva, estética, criatividade, suporte para o desenvolvimento humano, etc. Com a proliferação das novas tecnologias (TIC) da chamada Sociedade da Informação, apareceram novas preocupações à IHC, dando origem a um outro conceito ainda mais significativo do que a usabilidade: a experiência do utilizador (Cockton, 2012). A experiência do utilizador vai além da eficiência, qualidade das tarefas e satisfação do utilizador, pois considera os aspetos cognitivos, afetivos, sociais e físicos da interação.

2.2.1 **Engenharia da Usabilidade**

A Engenharia da Usabilidade é uma área no domínio da IHC cuja meta fundamental é o desenvolvimento de sistemas usáveis a partir da aplicação, de forma estruturada e

sistemática, de diferentes métodos nos diferentes estágios do projeto e do processo de desenvolvimento, assim como da integração de iniciativas de avaliação da usabilidade desde os estágios iniciais do projeto (Lecerof & Paternò 1998).

É uma abordagem de projeto de sistemas onde são utilizados vários níveis de usabilidade especificados quantitativamente numa etapa anterior ao seu desenvolvimento e tendo como objetivo a tomada de decisões de engenharia que vai ao encontro das especificações através de medidas chamadas métricas.

A solução do problema de comunicação entre o homem e os computadores não é resolvido somente com argumentações de interfaces mais *user-friendly* do que as outras, mas sim através de uma abordagem disciplinada e iterativa do estudo do desempenho humano no uso de sistemas interativos. É nesse contexto que surge a Engenharia de Usabilidade, uma metodologia que visa à interação homem-computador (Zancheta, 2004).

2.2.2 **Usabilidade**

Usabilidade é a capacidade de utilização de um produto por um ou mais tipos de utilizadores. Ela é alcançada quando um produto ou serviço é realmente utilizável, isto é, o indivíduo pode fazer o que ele quer da forma como ele espera ser capaz de fazê-lo, sem entraves, hesitação ou perguntas. O que torna algo usável é a ausência de frustração em usá-lo, ser agradável, de forma que o utilizador fique satisfeito ao usá-lo (Rubin & Chisnell, 2008).

De acordo com Lowdermilk (2013), a usabilidade está relacionada à forma como os fatores humanos se relacionam com diferentes tipos de produtos e a como se relaciona ao *design*, à avaliação, ao desenvolvimento de sistemas computacionais interativos e aos principais fenómenos que os cercam. O autor destaca a utilidade percebida do produto, dizendo que o maior indicador da usabilidade de um produto é se ele é bem utilizado. A questão fundamental da usabilidade é que o produto seja fácil de usar. Um sistema deve ser adequado às tarefas para as quais é destinado, ao utilizador e ao contexto em que será usado (Moraes, 2013).

Para Ravden e Johnson (1989), a usabilidade refere-se até que ponto um utilizador final é capaz de realizar com sucesso as tarefas necessárias, e sem dificuldades, utilizando uma aplicação de um sistema de computador. Atualmente os utilizadores procuram aplicativos para facilitar suas atividades do dia-a-dia e que satisfaçam suas necessidades (Nuckles, 2014).

De acordo com Badre (2002), a facilidade de uso está relacionada à realização de uma tarefa com sucesso através de um número mínimo de ações. Tornando-se assim uma medida de usabilidade importante para operadores experientes.

Para Nielsen (1993), o conceito de usabilidade está associado a cinco parâmetros passíveis de mensuração: fácil de aprender, eficiente para usar, fácil de memorizar, pouco sujeita a erros, e agradável de usar. Fácil de Aprender, o utilizador deve compreender com facilidade a interface, os diferentes percursos e o que pode fazer no sistema, aprendendo as opções de navegação e a funcionalidade dos botões; eficiente para usar, uma vez que o utilizador tenha aprendido a interagir com o sistema, deve usá-lo com altos níveis de produtividade localizando a informação que precisa; fácil de memorizar, o sistema deve ser fácil de lembrar, de maneira que o utilizador ocasional seja capaz de voltar a utilizá-lo sem ter que reaprender; pouco sujeita a erros, num sistema com poucos índices de erros, o utilizador é capaz de realizar as suas tarefas sem grandes problemas, recuperando de erros, caso aconteçam; agradável de usar a utilização do sistema deve ser agradável para que os utilizadores fiquem satisfeitos com a sua utilização.

A satisfação advém da reação do utilizador à interface, ao conteúdo, à estrutura da página, ao processo de interação e de navegação, às ajudas disponíveis. Segundo Cybis (2010), cada utilizador, ao interagir com um sistema, utiliza de conhecimentos empíricos adquiridos com outras interfaces para tentar prever o funcionamento de um sistema. Este, portanto, deve proporcionar o máximo possível da satisfação do utilizador, não necessariamente numa avaliação direta, mas um bem-estar após a sua utilização.

Para Rogers et al. (2013) a usabilidade é normalmente relacionada com produtos interativos que sejam fáceis de aprender, fáceis de usar e agradáveis de utilizar na perspetiva do utilizador. As mesmas autoras referem que a usabilidade pode ser dividida nos seguintes objetivos: fácil de usar; eficiente; seguro de usar, utilidade; fácil de aprender e fácil de relembrar como usar.

Segundo a norma ISO 9241-11 (1998) usabilidade pode ser definida como a capacidade em que um produto pode ser utilizado por utilizadores específicos para alcançar objetivos específicos com eficácia, eficiência e satisfação num contexto específico. A eficácia pode ser entendida como a precisão com que os utilizadores atingem um objetivo específico, a eficiência como o esforço e recursos utilizados para alcançar o objetivo e a satisfação como o conforto e atitude positiva face à utilização do produto. Preece et al (2005), por sua vez apresentam seis metas de usabilidade: ser eficaz no uso (eficácia), eficiente no uso (eficiência), segurança no uso (Segurança), de boa utilidade (utilidade), capacidade de aprendizagem (aprendizagem), capacidade de memorização (memorização).

Usabilidade é uma expressão empregada para descrever a qualidade de interação de utilizadores com algum tipo de interface. É um atributo de qualidade dos produtos que permite aferir se uma interface com o utilizador é fácil de utilizar (Nielsen, 2006 e 2012).

2.2.3 **Avaliação heurística de usabilidade de nos SI**

Muitos são os conceitos empregados para representar recomendações de usabilidade e esta variedade costuma confundir estudantes e profissionais, como afirmam (Preece et al., 2005).

Nesta secção é feita uma abordagem à avaliação heurística de Nielsen (1994), criadas a partir da análise de especialistas e profissionais da área de *design* e IHC, mas sem um foco específico ou contexto de uso, entretanto elas podem ser aplicadas em qualquer tipo de sistema. O motivo é porque esta forma de avaliação é a mais popular de medição de usabilidade, dada a sua facilidade de entendimento e agilidade de aplicação, ou seja, é um método rápido, barato e fácil de avaliação de usabilidade onde o avaliador procura problemas de usabilidade, numa interface através da análise e interpretação de um conjunto de princípios ou heurísticas (Pearrow, 2007).

Este método poder ser realizado por pessoas com pouca ou nenhuma experiência para a avaliação da usabilidade, mas Nielsen (1993 e 1994) diz que é preferível que o seja realizado por especialistas. Nielsen (1993) refere que os especialistas em usabilidade detetam 2.7 vezes mais problemas quando comparados com avaliadores com experiência

na óptica da utilização de computadores, mas que não são especialistas em usabilidade. O autor recomenda que a avaliação seja aplicada por vários indivíduos de forma isolada, para garantir a independência das diferentes avaliações e evitar a ocorrência de desvios, como consequência da interação entre os avaliadores. Mesmo que essa modalidade de avaliação possa ser conduzida por um único indivíduo, a sua efetividade aumenta com o número de avaliadores (Nielsen, 1993).

Nielsen (1994) demonstrou que as dez heurísticas eram suficientes para detetar a maior parte dos problemas de usabilidade. Entretanto, Pearrow (2007) considera que as heurísticas sugeridas por Nielsen constituem uma base inicial, ou seja, um ponto de partida, pelo que no momento da avaliação podem ser consideradas apenas algumas dessas heurísticas e acrescentadas outras.

Em seguida, é apresentada a lista das dez Heurísticas de Nielsen:

i. Visibilidade do estado do sistema: o sistema deve sempre manter os utilizadores informados sobre o que se está a passar, através de feedback adequado e dentro de um espaço de tempo razoável;

ii. Concordância entre o sistema e a realidade: o sistema deve utilizar a mesma linguagem que o utilizador, com palavras, frases e conceitos que sejam familiares ao utilizador, ao invés de termos técnicos orientados ao próprio sistema. Devem ser seguidas convenções do mundo real, de maneira que a informação seja apresentada numa ordem lógica e natural;

iii. Liberdade e controlo do utilizador: as vezes, os utilizadores selecionam funções do sistema de forma não intencional, motivo pelo qual o sistema deve garantir uma "saída de emergência" para que estes possam sair do estado indesejado. O sistema deve suportar "Anular" e "Repetir";

iv. Consistência e normas: os utilizadores não devem necessitar de considerar se diferentes palavras, situações e ações significam a mesma coisa. Devem-se seguir as convenções da plataforma;

v. Prevenção de erros: é recomendável a utilização de mensagens de erro claras, mas preferível a ter boas mensagens de erro é ter um *design* que evite a ocorrência de problemas. O sistema deve eliminar condições que propiciem erros ou deve ser capaz de

verificá-las e apresentar aos utilizadores uma opção de confirmação antes de cometerem o erro;

vi. Reconhecimento e memorização: deve ser minimizada a carga na memória do utilizador, os objetos, ações e opções devem estar visíveis. O utilizador não deve ser obrigado a decorar informação de uma parte do diálogo para o outro. As instruções para se manusear o sistema devem ou estar visíveis ou serem de fácil acesso caso seja necessário;

vii. Flexibilidade e eficiência de uso: os atalhos permitem aos utilizadores mais experientes a execução de operações mais rapidamente. Os atalhos também permitem aos utilizadores o acesso a informações que, de outro modo, obrigariam a navegar através de várias páginas para as aceder.

viii. Estética e *design* minimalista: os diálogos não devem conter informação irrelevante ou que só ocasionalmente é necessária. Cada unidade de informação no diálogo ocupada com informação desnecessária compete com a informação relevante, diminuindo a sua visibilidade;

ix. Ajudar os utilizadores a reconhecer, diagnosticar e recuperar dos erros: as mensagens de erro devem ser expressas em linguagem simples (sem códigos), indicar claramente qual o problema e disponibilizar soluções úteis e construtivas;

x. Ajuda e documentação: apesar de ser preferível que o sistema seja utilizável sem recorrer a documentação, pode ser necessário providenciar ajuda e documentação. Toda a informação deve ser fácil de pesquisar, focada nas tarefas do utilizador, listar os passos que se devem tomar e não ser demasiado longa.

2.3 Satisfação dos utilizadores dos SI organizacionais

Diversos estudos são realizados para avaliar o sucesso dos SI, entre eles, a satisfação do utilizador final e o impacto das Tecnologias de Informação (TI) no trabalho (Delone & Mclean, 1992). Vários pesquisadores desenvolveram na década de 70 e 80 do século passado modelos teóricos para tentar explicar porque é que alguns SI eram mais rapidamente aceites pelos utilizadores do que outros (Petter et al., 2008). O facto de serem aceites não significa que tenham sucesso, mas sim um requisito ou condição para o mesmo

(Friedman & Wyatt, 2006). O conceito de sucesso é amplamente aceite na literatura como adequado para nos referirmos à avaliação de SI. Porém explicar o termo sucesso não é fácil, já que, segundo Petter et al., (2008), é algo complexo, interdependente e multidimensional.

.A satisfação do utilizador é, provavelmente, a medida mais usada para avaliar o sucesso de SI, e serve como uma medida substituta tangível para determinar o desempenho de qualquer SI (Ainin et al., 2012). A satisfação do utilizador final com SI afeta o impacto individual do colaborador, por sua vez afeta a performance da organização (Doll & Torkzadeh, 1988). Por outro lado, o comprometimento organizacional refere-se à forma como o colaborador se identifica e está envolvido com a organização, e em que medida este está disposto a dar algo de si mesmo e de contribuir para a melhoria organizacional (Meyer et al., 2002). Esse comprometimento poderá afetar a satisfação do utilizador com o SI e como consegue melhorar a sua performance enquanto trabalhador através do uso do sistema.

O conceito de satisfação do utilizador sugere que SI que cubram as necessidades dos utilizadores reforçam a sua satisfação. Os estudos para o efeito ajudam a determinar o valor do SI para a organização, avaliando as suas necessidades e funcionalidades (Ives et al., 1983).

Para Al-Debei et al., (2013), a satisfação do utilizador refere-se ao sentimento de prazer ou de desagrado que resulta da agregação de todos os benefícios que uma pessoa espera receber a partir da interação com o SI. A reação do utilizador e a importância dadas a esses fatores determinam o grau de satisfação. Segundo Bailey e Pearson (1983), os utilizadores satisfeitos têm um desempenho superior ao dos insatisfeitos e se o SI ajudar o utilizador a ter um melhor desempenho, o sistema obterá sucesso.

Doll e Torkzadeh (1988) definem satisfação do utilizador referindo-se à atitude afetiva perante uma aplicação informática específica por alguém que interage diretamente com o aplicativo. Os autores propõem que a satisfação do utilizador com o uso do SI seja medida através de um modelo composto por cinco fatores: conteúdo do sistema, precisão do sistema, formato do sistema, facilidade de uso do sistema e entrega da informação em tempo.

Segundo Au et al. (2008) a satisfação do utilizador é a avaliação afetiva e cognitiva do utilizador em relação ao nível de experiência agradável de utilização do SI. Essa abordagem visa entender os processos psicológicos que transformam o desempenho do SI em diferentes níveis de satisfação ou insatisfação do utilizador.

A experiência deve estar relacionada com a previsão do comportamento ou com o desempenho do sistema. A experiência de uso de um produto começa antes mesmo do primeiro contato direto. Já existe um grande conhecimento prévio, oriundo de todo o histórico do utilizador com experiências anteriores seja com produtos similares ou com as perceções do mundo de modo geral (Norman, 2013).

Dado o caráter multidimensional do modelo de DeLone e McLean (2003), é possível produzir análises acerca das relações entre as várias dimensões. Assume-se que a satisfação dos utilizadores dos SI está diretamente relacionada com a sua intenção para o uso e com a intensidade com que, realmente, recorrem aos recursos dos sistemas (Wu & Wang, 2006). SI com qualidade, robustos e fáceis de usar, que incorporem dados fiáveis, como é natural, tendem a ter utilizações mais intensas e apropriadas, permitindo, assim, a geração de benefícios em larga escala para a atividade das organizações (DeLone & Mclean, 2003).

2.3.1 **Medidas de satisfação dos utilizadores com o SI**

As medidas de satisfação do utilizador com SI são baseadas na pesquisa realizada nos anos 80, por Bailey e Pearson (1983). Estes criaram uma lista de 39 fatores que afetam a satisfação do utilizador, tais como flexibilidade do sistema, integração do sistema, facilidade de uso, utilidade percebida, segurança dos dados, documentação, formato, relevância, precisão, idioma, pontualidade, velocidade, expectativas, etc. Essa lista foi empiricamente comparada com as respostas de entrevistas realizadas junto a 32 gestores de oito organizações diferentes. Os autores desenvolveram e testaram um questionário, a partir de uma técnica de escalonamento, para medir a satisfação dos utilizadores de computador independente da interação dos mesmos com o sistema. Concluíram que as definições de satisfação consistem na soma ponderada de reação positiva ou negativa de um utilizador em relação ao conjunto de 39 fatores.

Numa pesquisa posterior, num esforço para otimizar a consistência e a segurança, Ives et al. (1983), desenvolveram um instrumento na forma de questionário mais sucinto, eliminando para isso os fatores de Bailey e Pearson (1983), o que segundo os autores representará um progresso substancial em direção a criação de uma técnica de medição padrão para satisfação dos utilizadores do SI.

Mais tarde, Baroudi e Orlikowski (1988) apoiam-se na pesquisa de Ives et al. (1983), reforçam e revalidam os fatores destes, como uma forma eficaz de medir a satisfação dos utilizadores. Os autores utilizaram uma amostra com 358 funcionários de 12 empresas. O instrumento é composto por 13 fatores elaborados a partir de Ives et. al (1983), com dois itens por fator. O estudo apresentou três categorias: Produto da informação, Pessoal e Serviços de EDP (Electronic Data Processing) e Conhecimento e Envolvimento do utilizador. O instrumento reduzido apresentou confiabilidade e validade na mensuração da satisfação do utilizador com o SI (Baroudi & Orlikowski, 1988). No entanto, a maioria destes instrumentos está, direcionada para a avaliação de uma determinada aplicação e têm um problema que é uma visão estreita do processo de avaliação, considerando a satisfação do utilizador como simples constructo, limitando-se a medir o impacto da TI sobre a produtividade (Torkzadeh & Doll, 1999).

O instrumento desenvolvido por Doll e Tarkzadeh (1988) é uma exceção. Estuda o impacto da TI sobre um aspeto multidimensional. O instrumento foi elaborado a partir de pesquisas anteriores, composta inicialmente por 38 itens, os quais foram reduzidos a 12 itens distribuídos em 5 fatores: conteúdo, precisão, formato, facilidade de uso e pontualidade. Uma amostra de 618 respondentes foi utilizada para a análise dos dados. Os indicadores da pesquisa tiveram a seguinte distribuição: quatro itens para conteúdo, dois itens para precisão, dois itens para formato, dois itens para facilidade de uso e dois itens para pontualidade. O instrumento final possui confiabilidade e validade adequadas para objetivos acadêmicos e corporativos.

Posteriormente DeLone e McLean (1992) desenvolveram uma taxonomia alternativa para compreender as diferentes medidas de sucesso de SI, classificadas em seis categorias: qualidade do sistema, qualidade da informação, uso do sistema satisfação do utilizador, impacto individual e impacto organizacional. De acordo com os autores, a medida de satisfação tem um elevado grau de validade e os instrumentos derivados de Bailey e

Pearson (1983) têm proporcionado instrumentos confiáveis para medir a satisfação do utilizador como uma medida de sucesso e também porque é difícil negar o sucesso de um sistema do qual os utilizadores dizem gostar.

O modelo de DeLone e McLean (1992) assume que a qualidade do sistema e a qualidade da informação separadamente ou conjuntamente afetam o uso do sistema e a satisfação do utilizador. Considera que, o uso do sistema pelos utilizadores pode afetar o grau de satisfação do utilizador positiva ou negativamente e vice e versa. O uso do sistema e a satisfação do utilizador são os antecedentes diretos do impacto individual e, finalmente, o seu impacto sobre o desempenho individual deve eventualmente ter algum impacto organizacional, resultando no modelo proposto (DeLone & McLean, 1992). A figura 1 apresenta o modelo:

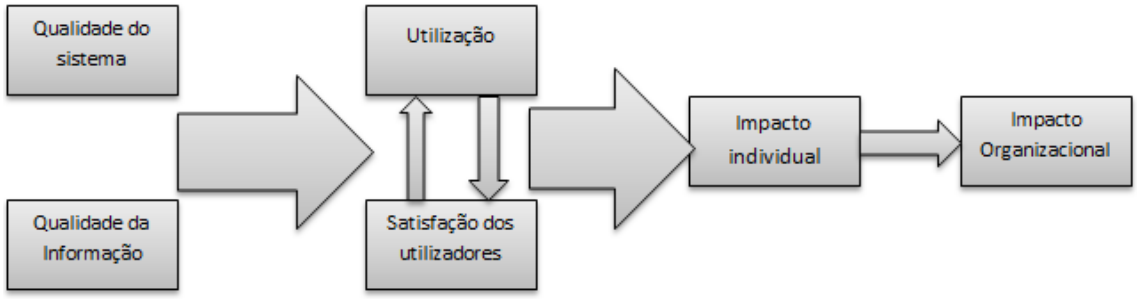


Figura 1- Modelo de Sucesso de SI DeLone e Mclean

(Adaptado de DeLone e McLean , (1992))

Uma década depois, o modelo de DeLone e McLean (2003) foi alvo de uma atualização do anterior modelo desenhado em 1992, adicionando a dimensão qualidade do serviço como uma categoria para verificar a qualidade do suporte ao SI. Além disso, as dimensões impacto individual e impacto organizacional foram unificadas e transformaram-se numa única dimensão denominada benefícios líquidos. Este novo instrumento também sofreu adaptações para ser utilizado na avaliação do *e-commerce.*

Para Chin e Lee (2000), a satisfação do utilizador é medida pela comparação entre as expetativas deste face ao sistema e a perceção do que realmente o sistema oferece. Baseado no instrumento de Doll e Torkzadeh (1988), Chin e Lee (2000) criaram um instrumento com fatores mais aprofundados com um novo foco para os cinco fatores existentes: conteúdo, precisão, formato, facilidade de uso e pontualidade. Foi incluído o

fator velocidade do sistema, que foi definido como pela satisfação que o utilizador de um SI possui com a velocidade operacional do sistema.

Au et al, (2008) realizaram uma pesquisa na qual consideraram que a satisfação do utilizador com o SI está relacionada com fatores cognitivos, para fundamentar o estudo, os autores basearam-se em três teorias da psicologia relacionadas à motivação: Teoria da Confirmação da Expetativa de Oliver a Teoria da Equidade Laboral de Adams e a Teoria das Necessidades de Alderfer. O instrumento tinha o objetivo de testar chaves e ligações entre a satisfação do utilizador com a motivação. O modelo proposto foi elaborado a partir de 6 fatores: desempenho de SI, desempenho no trabalho, relacionamento no trabalho, auto desenvolvimento no trabalho, expetativa de desempenho de SI e satisfação do utilizador. O instrumento com 63 itens foi elaborado e operacionalizado numa escala do tipo Likert de sete pontos. Uma pesquisa com 922 funcionários foi utilizada para avaliação do modelo. O instrumento final sofreu uma redução para 34 itens baseado em quatro fatores (Au et al., 2008).

2.4 Segurança da informação

Nos dias atuais é percetível que os negócios das organizações são, na grande maioria dos casos, suportados pela informática. Diante desse fato podemos afirmar que a informação é um bem cujo valor é perfeitamente possível de ser medido e que a sua importância levou ao surgimento de um novo modelo de economia, que tem justamente a informação como base (Mello et al., 2010). Portanto, a informação deve ser mantida em segurança, assim como o ambiente e os equipamentos utilizados para o seu processamento. As organizações sabem da necessidade de se praticar Segurança da Informação com urgência.

A questão da Segurança da Informação é tão urgente e se mostra ainda mais complexa, que os especialistas afirmam que há uma guerra cibernética e que as redes de computadores do governo de vários países têm sido ocultamente monitoradas (Jones, 2014). Alguns analistas acreditam que o ciberespaço será o principal espaço de operações da guerra do futuro (Clarke & Knake, 2015).

A Segurança da Informação está relacionada com proteção e salvaguarda da informação que constitui valor para a Organização e as partes interessadas. Trata da preservação da confidencialidade, integridade e disponibilidade dos dados armazenados nos SI que requer uma gestão envolvendo a supervisão e a tomada de decisão para alcançar os objetivos do negócio, por meio da proteção dos ativos de informação da organização (ISO/IEC 27001:2013).

Segundo Pfleeger e Pfleeger (2003) o objetivo da segurança é conseguir fazer a prevenção contra a exploração das vulnerabilidades do sistema. Os autores consideram a confidencialidade, a integridade e a disponibilidade como os requisitos base da segurança da informação. Confidencialidade refere-se a restringir o acesso aos dados apenas às pessoas autorizadas, integridade refere-se à preservação dos valores dos dados de modo que não seja modificados de forma não autorizada, e disponibilidade significa que os dados apenas são acedidos por pessoas autorizadas sempre que necessário (Dhillon & Backhouse, 2000).

A informação só poderá ser considerada segura se satisfizer três princípios: a disponibilidade, a confidencialidade e a integridade (Kim & Solomon, 2012). O grande desafio é encontrar o balanceamento correto entre estes princípios (Pfleeger & Pfleeger, 2003). A figura 2 apresenta os requisitos da segurança da informação.

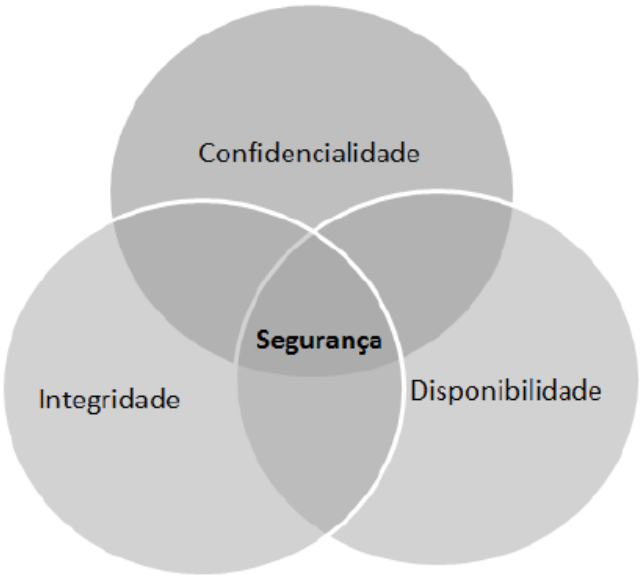


Figura 2- Requisitos da Segurança da Informação

(Adaptado de Pfleeger e Pfleeger (2003))

Segundo Reddick (2010), a segurança da informação não é só um problema tecnológico, envolve também questões relacionadas com a gestão que necessitam de recursos especiais e competências próprias para fazer face a essas questões. Dito de outra forma, a gestão da segurança da informação, preocupa-se com as pessoas, processos e tecnologia. Os processos e as pessoas são influenciados pelo ambiente onde estão inseridos. Para o autor a maior causa dos problemas de segurança apontam frequentemente ser a negligência dos colaboradores, mais do que os ataques vindos do exterior.

Jonhson (2011) define a segurança da informação como o ato de proteger a informação e os sistemas que a armazenam e processam. A proteção é contra qualquer risco que possa conduzir ao acesso não autorizado, uso, divulgação, disrupção, modificação ou destruição da informação. O autor distingue o conceito de segurança dos sistemas de informação do conceito de segurança da informação defendendo que o primeiro concentra os esforços de proteção da informação independentemente da forma ou do processo e o segundo foca-se na proteção da segurança durante o processo e o seu uso. A disponibilidade normalmente expressa a quantidade de tempo para os utilizadores fazerem uso dos sistemas, das aplicações ou dos dados. A integridade relaciona-se com a validade e precisão dos dados. A confidencialidade significa guardar a informação de toda a gente que não possua o direito ao seu acesso.

A norma ISO/IEC 27000 refere ainda, que a segurança da informação é a proteção da informação de um conjunto alargado de ameaças de forma a garantir a continuidade do negócio, minimizar os riscos de negócio, e maximizar o retorno dos investimentos e das oportunidades de negócio.

2.4.1 **Segurança no uso dos SI**

O foco da segurança dos SI deve respeitar não apenas os aspetos tecnológicos, mas também o comportamento das pessoas nas organizações e, mais concretamente, o respeito pelas políticas de segurança pré-definidas (Denis et al. 2007). Segundo de Holgate et al., (2012), as soluções técnicas são necessárias, mas insuficientes para enfrentar desafios de Segurança da Informação em ambientes sociotécnicos complexos e em constante mudança.

Demonstrar confiança nos colaboradores da organização é importante, mas o ideal é prevenir através de controlos, pois os motivos para que uma pessoa comprometa a segurança da empresa são os mais diversos, podendo ser para obter ganhos financeiros, vingança, necessidade de aceitação ou respeito, idealismo, curiosidade ou busca de emoção, anarquia, aprendizado, ignorância, espionagem industrial e ou nacional (Calder, 2008).

Estudos desenvolvidos sobre a segurança da informação e os serviços TI relatam que as políticas reportam-se a um conjunto de práticas que devem orientar de forma a salvaguardar a informação de eventuais ataques, vulnerabilidades, ameaças ou riscos. Para Zúquete (2008), as políticas de segurança definem fundamentalmente requisitos de segurança que devem ser respeitados pelos utilizadores para garantir um determinado resultado. A ISO/IEC 27003 (2010) define política como sendo "uma declaração de intenção e direção como formalmente expresso pela gestão".

A adesão e implementação de tecnologias de segurança estão ligadas ao uso de *software* bem como a outros recursos tecnológicos para proteção do SI. As práticas de segurança referem-se ao comportamento do utilizador em relação a segurança da informação e constituem ações preventivas que conduzem ao uso seguro do computador. As práticas de segurança, combinadas com o uso de tecnologias de segurança, diminuem a vulnerabilidade dos SI. (Rhee et al., 2009).

O comportamento dos utilizadores ligados as práticas de segurança que mais influenciam a segurança da informação, são a gestão de *passwords*, atualização de *software* de antivírus, gestão de arquivos anexos nos *emails* e cuidados na partilha de arquivos (Besnard & Arief, 2004). Segundo Albrechtsen (2007), os utilizadores de uma empresa devem, ter um papel ativo na segurança dos SI através da prevenção de incidentes tais como: proteção dos bens materiais e não materiais de uma organização, reação a incidentes e durante o dia a dia, através de ações como: bloquear o acesso ao seu computador, não escrever a *password* de acesso em nenhum local visível e acessível por terceiros, terem cuidados com a utilização de *emails* e da internet, evitarem o uso de *software* não licenciado e reportar todas as falhas de segurança ao departamento de SI. Aytes e Connoly (2004) apontam como práticas importantes o uso correto de *passwords*, cuidados com o *email* e manter *backup* dos dados do computador.

O papel do utilizador em relação à segurança é crucial para a segurança da informação. De acordo com Tillery (2010), a vulnerabilidade das empresas persistirá se os seus colaboradores não compreenderem como as suas decisões e comportamentos são determinantes para a segurança dos SI. Siponen et al. (2009) dizem que os resultados de estudos existentes indicam que 91% das organizações empregam colaboradores que falham no cumprimento das políticas de segurança da informação. Os colaboradores pouco cuidadosos, que não cumprem com as políticas de segurança da informação constituem um sério risco para as organizações.

Segundo Fleming (2007) é imperiosa a necessidade das organizações criarem uma cultura coletiva de segurança, que serve como a base para sensibilizar os colaboradores para a necessidade de cumprirem com as políticas e procedimentos definidos. A cultura organizacional é parte estratégica para o gestor que pretende tornar o SI da sua organização mais seguro. As formações e os programas de consciencialização sobre segurança da informação são os meios mais efetivos de dar a conhecer os utilizadores sobre a necessidade de proteger os SI (Aytes & Connoly, 2004).

A literatura apresenta várias formas de promover o cumprimento das normas e políticas de segurança pelos colaboradores de uma empresa, como é o recurso a sanções e dissuasões, campanhas de marketing e formação (Karjalainen & Siponen, 2011). De todas as abordagens, a formação de utilizadores é a mais comummente utilizada pelas organizações.

De acordo com Guo et al., (2011), algumas das violações mais comuns que os colaboradores das empresas podem cometer são o roubo de informação, a utilização de *software* não licenciado, o acesso a informação confidencial, a cópia ilegal de *software*, a copia de informação sensível e confidencial, a utilização de USB (*Universal Serial Bus*) infetadas, a desativação de configurações de segurança, a não alteração de *passwords*, a não realização de *backups* ou de *updates* de *patches.*

Para que o nível de segurança da informação desejado seja alcançado, é necessário implementar e consolidar uma política de segurança com a participação dos colaboradores na avaliação de riscos de segurança do SI (Denis et al. 2007). Isso afeta positivamente no aumento da consciência do colaborador sobre riscos de segurança, no maior alinhamento da segurança com os processos de negócios e no desenvolvimento de controlos de

segurança eficientes. O conhecimento do colaborador sobre os processos de negócios contribui no desenvolvimento de controlos de segurança do SI mais efetivos, além de maior proteção de informações sensíveis (Spears & Barki, 2010).

A implementação bem-sucedida das políticas de segurança da informação requer comprometimento e liderança dos gestores da empresa. Os gestores têm a responsabilidade de formular a estratégia de proteção dos ativos de informação, definindo orçamento que otimize a segurança da informação, minimizando perdas e danos causados por possíveis ataques. Os gestores devem avaliar as capacidades da segurança da informação, identificando falhas entre as capacidades atuais e futuras (Anderson & Choobineh, 2008).

2.4.2 **Gestão da Segurança da Informação**

A segurança da informação é uma questão mais de gestão, que de tecnologia (Corby, 2002). Quer dizer, a tecnologia encarrega-se em apresentar os meios e como será garantida a segurança da informação, enquanto a gestão pretende responder ao que será feito para garantir a segurança da informação.

Atualmente não se pode tratar a gestão da segurança da informação como um projeto como outros, por exemplo, comerciais, no ambiente organizacional (Martins, 2003). Melhores práticas devem ser incorporadas pelas organizações modernas para assegurar o monitoramento contínuo dos dados e a integridade das informações corporativas.

A informação é um ativo cada vez mais valorizado, tem impacto direito na continuidade dos negócios e na sua credibilidade. Por isso, as organizações procuram soluções para mitigar esses riscos, estabelecendo um conjunto de boas práticas por meio de políticas de segurança geridas em diferentes instâncias com funções e responsabilidades bem definidas. Tudo isso para garantir o nível de segurança adequado ao negócio. Por seu lado, Alaboodi (2006) afirma que a segurança da informação é parte integrante nos processos de negócios das organizações atuais, mas ela não deve ser uma competência básica da organização, ela deve estar presente na cultura e nos processos de negócio da organização, para que seja possível garantir que os riscos da informação e os controlos estejam em equilíbrio.

O panorama da Gestão da Segurança da Informação afeta a criação de processos ligados ao monitoramento contínuo da integridade das informações, à prevenção de ataques e ao furto dos dados, garantindo em casos de emergências o pronto restabelecimento dos SI e o acesso seguro às informações das organizações (Anderson, 2003). A conceção de um projeto de Segurança da Informação numa organização deve estar suportado por um Sistema de Gestão de Segurança da Informação que precisa ser planeado e organizado, implementado, mantido e monitorado.

Eloff e von Solms (2000) apresentam um modelo de Sistema de Gestão de Segurança da informação baseado em tecnologia e processos, enquanto Eloff e Eloff (2003), apresentam um modelo fundamentado em processos e padrões elevados ao topo no ambiente organizacional, visando questões ligadas diretamente aos utilizadores de caráter cultural, ético, social e legal.

A norma Internacional ISO/IEC 27001 (2013) define a gestão de segurança da informação, como um processo de gestão estruturado que permite garantir os principais requisitos de segurança da informação, apresentando um modelo para estabelecer, implementar, operar, monitorar, rever, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

O SGSI é uma parte do sistema geral de gestão, baseando-se numa abordagem ao risco do negócio, para estabelecer, implementar, operar, monitorar, rever, manter e melhorar a segurança da informação. (ISO/IEC 27000, 2014). A abordagem do processo para o SGSI baseia-se na exploração do princípio adotado nas normas ISO de gestão do sistema, conhecido como processo PDCA (*Plan – Do – Check – Act*) (ISO/IEC27001, 2013). *Plan* - Planear significa estabelecer os objetivos e fazer planos (analisando a situação da organização, estabelecendo os objetivos e desenvolvendo planos para os alcançar). *Do* - Os planos são postos em prática e implementados (fazer o que foi planeado para fazer). *Check* - Verificação dos resultados (monitorização da realização dos objetivos planeados).*Act* - As atividades são corrigidas e melhoradas (aprender com os erros). A aplicação do ciclo de desenvolvimento de melhoria contínua, conhecido como modelo PDCA, serve para se obter padronização e indicadores de controlo na elaboração da política de segurança

A figura 3 apresenta o ciclo PDCA, considera as entradas de requisitos de segurança de informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos e expectativas (ISO/IEC 27000, 2013).

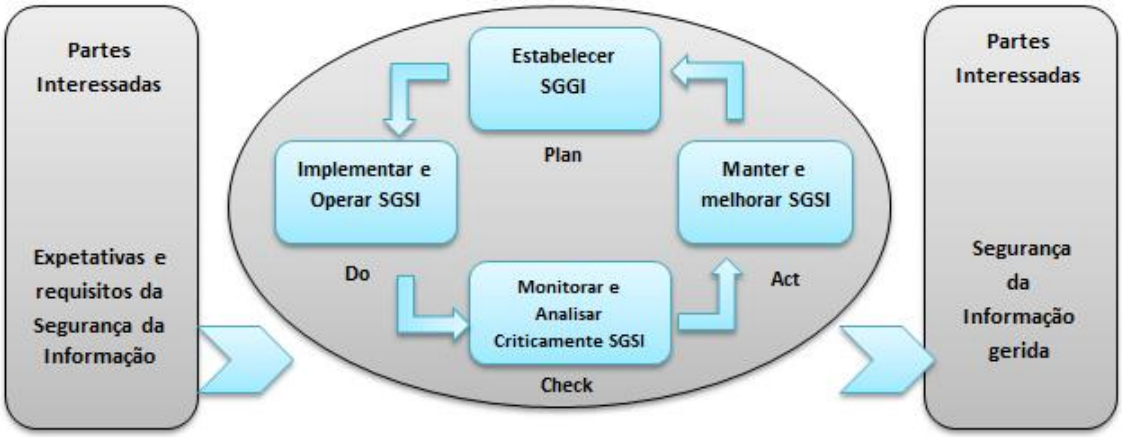


Figura 3- Modelo PDCA aplicado aos processos do SGSI

(Adaptado de (ISO/IEC 27000, 2013))

A gestão da segurança da informação possui diversos documentos com padrões internacionais que servem como base para tratar de questões técnicas e não técnicas relacionadas à segurança. Documentos elaborados por entidades como International Organization for Standardization (ISO), IT Governance Institute (ITGI) e National Institute of Standard and Technology (NIST), servem de base para as organizações definirem políticas de segurança da informação, aspetos legais, aspetos éticos e culturais de segurança da informação, servem também para que as organizações adotem por um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um SGSI. Esses documentos auxiliam na definição dos níveis de autoridade, assim como seus papéis e responsabilidades de cada membro da empresa (Kritzinger & Smith, 2008).

O objetivo da Gestão de Segurança de Informação é manter a qualidade das informações. E a qualidade dessas informações depende da confidencialidade, integridade e disponibilidade das mesmas. Esse princípio foi desenvolvido de modo a se tornar o padrão global de SI: o conjunto de ISO/IEC 27000. Um dos principais papéis da gestão de segurança da informação é fornecer a política e código de conduta de utilização do SI para

a organização. Através dessas políticas e códigos de conduta, a gestão de topo almeja influenciar o comportamento dos colaboradores relacionados à segurança.

A política de segurança é, assim, expressa por meio de valores e instruções de uso dos ativos de informação da organização. A implementação bem-sucedida de políticas e condutas de segurança deve considerar o utilizador como um agente ativo, que pode fornecer informações importantes que aumentem a segurança e facilitem o uso dos SI (Hedström et al., 2011). Para isso, a implementação deve abordar fatores críticos à segurança e deve ser vista pela gestão do topo não como um conjunto de ações com um objetivo final traçado, mas como um conceito que faça a projeção de uma nova cultura de preservação e comprometimento voltado para a proteção da informação. Estes conceitos podem ser alcançados através de definições de políticas de segurança da informação (Ferreira & Araújo, 2006), estas por sua vez devem ser o mais claras possíveis e abordar as reais necessidades da organização estando alinhada com os objetivos do negócio.

2.4.3 **Métricas de avaliação da Segurança da Informação**

Nesta secção mostra-se a necessidade de pesquisas para identificar as principais métricas usadas para avaliar o nível de segurança da informação e discutir os benefícios e a relevância de tais métricas.

Os desafios enfrentados pelas organizações com relação ao tratamento e prevenção às ameaças de segurança são grandes e exigem muitos cuidados. Por isso, são propostos diversos meios para analisar e representar a segurança dos SI. O emprego da abordagem quantitativa, em particular, é objeto de discussões dos pesquisadores da área ao longo das últimas duas décadas (Jansen, 2009).

A ideia de quantificação aplicada a segurança da informação envolve desde o desenvolvimento de métricas de segurança até estudos sobre impactos económicos, avaliação de risco e modelos para medir segurança (Verendel, 2009). A utilização de métricas de segurança em SI impõem-se, por ser um tópico fundamental para investigar as motivações dos ataques, avaliar a eficiência dos controlos implementados e consequentemente fornecer uma visão geral sobre os problemas de segurança enfrentados pela organização. Também permitir medir a perceção do que pretendia ser o sistema que

está em uso após a implementação do sistema de segurança. Chew et al. (2008) afirmam que a implementação de métricas de segurança pode proporcionar diversos benefícios às organizações.

De acordo com Gaivéo (2008) devem destacar-se os impactos da segurança nas atividades das Pessoas e das organizações e devem ser considerados em padrões adequados que permitam garantir que as atividades associadas ao planeamento, à implementação e ao teste da segurança, são abrangidas por um conjunto de métricas que possibilitem a sua posterior avaliação.

Para Brotby (2009), métrica é um termo utilizado para indicar uma medida baseada numa referência. No caso da segurança, as métricas devem refletir o nível de segurança relativo a certo objetivo e auxiliar a tomada de decisão para tratar ou evitar ameaças.

Métricas são ferramentas desenvolvidas para facilitar a tomada de decisão e melhorar o desempenho e responsabilidade através da recolha, análise e reporte dos dados relevantes relacionados com desempenho (Swanson et al., 2003). Os autores referem que as métricas de segurança devem ser baseadas nas metas e objetivos de desempenho da segurança dos SI e das TICs que estabelecem os resultados desejados para o programa de implementação da segurança.

As métricas de segurança são aplicações de análises quantitativas, estatísticas ou matemáticas para mensuração dos custos da segurança funcional, benefícios, sucessos, falhas, tendências e carga de trabalho. Contribuem para promover melhorias e efetuar correções nos processos de segurança (Kovacich & Halibozek, 2006). Com o uso das métricas de segurança as organizações podem verificar se os mecanismos de proteção estão a ser executados de forma apropriada, avaliar continuamente a evolução do nível de segurança do seu ambiente de TIC e avaliar se os investimentos realizados estão a ter o retorno esperado.

A gestão do topo nem sempre está confiante sobre o nível de segurança de sua organização e se os investimentos realizados estão a dar o devido retorno. Para resolver essas questões, deve adotar processos de cálculo e análise de métricas de segurança, pois de acordo com Abreu et al., (2010), os estudos sobre a gestão de qualidade de produtos de

software associada ao investimento de desenvolvimento auxiliaram na criação de técnicas e métricas para dar suporte à gestão de recursos, estimativas e qualidade de *software*.

A partir da coleta de dados em todo o ambiente da organização, os gestores podem gerar métricas que ajudarão a avaliar continuamente a evolução do nível de segurança do seu ambiente de TI. Porque, as métricas de *software* podem ser facilmente calculadas, entendidas e testadas e independem do observador que as aplica (Abreu et al., 2010).

As métricas não são por si só a resposta para os problemas organizacionais de segurança. Não se deve apenas medir e quantificar, mas sim partir para a solução do problema. As organizações devem ter essa abordagem e analisar o tempo de medição de um indicador. Um ponto importante é desenvolver métricas ou indicadores que sejam simples e que possam prover a usabilidade para a gestão da Segurança da Informação, conciliando com os objetivos propostos. As métricas têm que estar alinhada com a organização para demonstrar algum tipo de progresso (Chapin & Akridge, 2005). Esta abordagem de evolução temporal na medição sustenta a avaliação por maturidade.

Para Payne (2006), um programa de métricas de segurança, independentemente do modelo, deve ter em consideração estes passos: definir metas e objetivos do programa de métricas; decidir as métricas a criar; desenvolver modelos para a criação das métricas; definir critérios de comparação; estabelecer métodos para reportar as métricas; criar um plano de ação para implementar as métricas; estabelecer um programa contínuo de revisão e atualização das métricas.

Para Swanson et al. (2003) o processo de desenvolvimento das métricas de segurança dos SI passa por seis fases distintas, integradas em duas atividades principais: identificação e definição do atual programa de segurança dos SI e desenvolvimento e seleção de métricas específicas para medir a implementação, eficácia e eficiência e o impacto dos controlos de segurança, como ilustrado na figura 4.

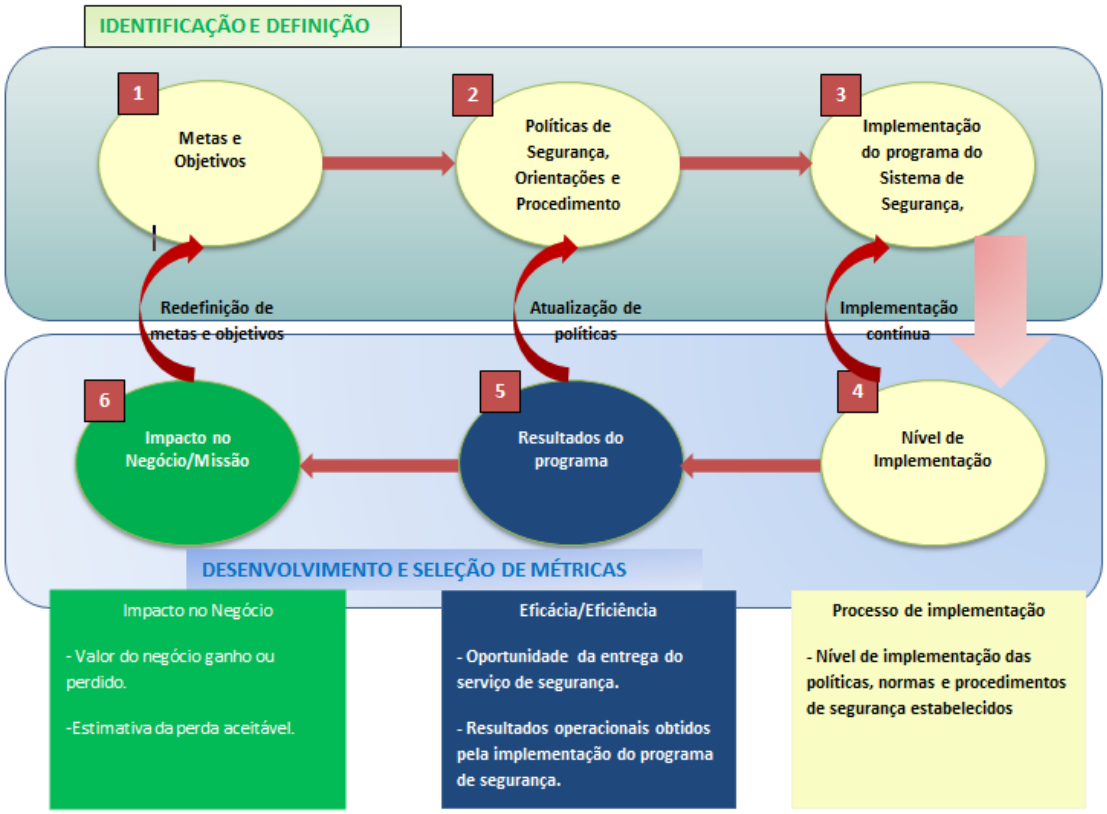


Figura 4- Processo de desenvolvimento das métricas de segurança dos SI

(Adaptado de Swason et al., (2003))

Swanson et al. (2003) definem três tipos de métricas:

1- Métricas de implementação servem para medir a implementação da política de segurança, ou seja, para mostrar a evolução da implementação das políticas e procedimentos nos controlos de segurança;

2- Métricas de eficácia/eficiência avaliam os resultados da entrega de serviços de segurança, sendo utilizadas para monitorar os resultados da implementação dos controlos de segurança;

3- Métricas de impacto são aquelas que medem o impacto no negócio ou na missão dos eventos e atividades de segurança, através da quantificação da poupança de custos que advêm da aplicação do programa de segurança.

As métricas podem fazer parte de um mesmo programa de segurança, ou seja, ser utilizadas ao mesmo tempo e complementando-se, mas a sua utilidade varia consoante a maturidade de cada programa de segurança da informação (Chew et al., 2008).

2.5 Relevância da Usabilidade no contexto da segurança da informação

As preocupações inerentes à segurança da informação, à usabilidade de sistemas e os impactos de ambos na atividade organizacional impõem a pertinência de se proceder à avaliação da relação existente entre elas do ponto de vista de alguns autores, uma revisão da vários métodos de segurança da informação que são utilizados, avaliar as questões de usabilidade, e desenvolver uma taxonomia para organizar estas questões. A intenção é fazer uma chamada de atenção para a necessidade de análises sistemáticas de usabilidade e para o desenvolvimento de métricas de usabilidade para segurança da informação.

A ideia de um SI apresentado ao utilizador de forma clara e fácil (Preece et al., 2005) é um desafio contínuo, sendo necessários constantes testes e pesquisas sobre o comportamento deste a fim de entender diferenças de perfis, limitações, formas de utilização e outros. São evidentes as expectativas do utilizador quanto à necessidade de sistemas ágeis, fáceis e que consumam pouco tempo de operação (Nielsen & Loranger, 2007). O utilizador nem sempre tem conhecimento das necessidades de segurança, principalmente técnicas. E isso pode causar conflitos entre os seus intentos e os controlos de segurança. Portanto, segundo Pereira e Paiva (2011) os especialistas de engenharia de *software* devem desenhar tanto os requisitos funcionais quanto os de segurança, e os especialistas em segurança da informação deverão escolher os controlos técnicos.

É importante que um SI seja bem desenvolvido quanto à complexidade computacional e à integridade dos dados, mas a interface com o utilizador é tão ou mais importante para garantir a segurança do processo, porque segundo Moran (1981), é através da interface que os utilizadores têm acesso às funções da aplicação. Fatores como a satisfação subjetiva, a eficiência, e a segurança, dependem de um bom *design* de interface.

Segundo Pereira e Paiva (2011) há um pensamento de que efetuar melhorias em usabilidade afeta a segurança de modo negativo, e vice-versa, ou seja, quanto maior facilidade de usar um SI, maiores são os riscos à sua proteção. Isso acontece por um lado, pelo conflito de interesses que existe entre os desenvolvedores de sistemas e os utilizadores, isto porque existem relatos de que muitas vezes os SI não atendem as necessidades dos utilizadores (Ramos, 2000). Por outro lado, Yee (2004) atribui esse conflito aos desenvolvedores de sistemas que tratam a segurança, ou a usabilidade, como complementos para um produto já acabado. Pereira e Paiva (2011) discordam da perspetiva

de que usabilidade é inversamente proporcional à segurança, afirmando que eficácia dos SI é diretamente proporcional à sua usabilidade. Os autores dizem que a usabilidade reduz falhas na segurança por parte dos utilizadores, quer seja intencionais ou não.

À área que estuda a relação homem-computar foi acrescentada a questão da segurança e daí aparece a Interação Humano-Computador e Segurança (IHCSec), que surgiu devido à necessidade identificada pelos especialistas em IHC de melhorar a usabilidade de sistemas seguros. Flechais (2005) diz que a IHCSec está mais voltada em melhorar a interface do utilizador dos sistemas, o que por si só não é suficiente. Para Whitten (2004) a avaliação de usabilidade de *software* seguro não deve se concentrar em usabilidade a ponto de excluir a segurança e em certos casos é necessário até mesmo incluir comportamentos e tarefas de nível complexo aos utilizadores para garantir a segurança. O autor destaca diferenças entre *softwares* seguros e demais *softwares*.

Gaivéo (2008) refere que garantir a segurança pode afetar a usabilidade dos SI e das TICs, por causa das implicações que impõe a utilização dos SI e das TICs, onde a aceitação das tecnologias e consequentemente das necessidades de segurança da informação poderá ser afetada se essas necessidades não forem entendidas pelas Pessoas como úteis e como uma grande ajuda para aumentar a eficácia e eficiência do seu próprio desempenho.

A responsabilidade sobre a segurança da informação dentro da empresa é de todos, não somente da gestão do topo. De acordo com Rezende e Abreu (2000), as organizações devem procurar dar mais atenção ao ser humano, pois é através dele que são executadas as práticas empresariais. Dessa forma, é importante destacar que o elo mais fraco de um processo de segurança é o ser humano, e ao mesmo tempo é ele o responsável por garantir a fidelidade da informação. Portanto a segurança da informação deve abranger todos os colaboradores da organização, pelo que é imperioso que todos conheçam a engenharia da usabilidade e tenham em atenção de que ela é uma poderosa ferramenta para reduzir riscos na segurança dos SI, visto que, de acordo com Pereira e Paiva (2011) não existe utilidade para um sistema inseguro, assim como não há necessidade de segurança num sistema que não tenha utilidade.

3 Caracterização da Organização

A Angola Telecom (AT) é uma empresa angolana de telecomunicações e multimédia, fundada em 1992, disponibilizando serviços comerciais de voz e dados (AT, 2016).

Com mais de 1040 colaboradores distribuídos pelas 18 províncias, a AT, é hoje um dos principais *players* na telefonia fixa e móvel e na disponibilização de um serviço combinado de voz e dados e internet assente altas tecnologias em Angola. Está presente em vários sectores de atividade como o Financeiro, Telecomunicações e Media, Administração Pública e Indústria; a sua atividade estrutura-se na venda de soluções inovadoras.

A AT foi criada pelo Decreto Nº 10/92 de 06 de Março como resultado da fusão das anteriores Empresas estatais ENATEL e EPTEL. A EPTEL, Empresa Pública de Telecomunicações foi criada por Decreto Nº 95/76 de 23 de Dezembro como resultado da aquisição pelo estado do património da Companhia Portuguesa Rádio Marconi que operava em Angola explorando as ligações internacionais. Deu início a sua atividade em 1977 como operador público de telecomunicações no regime internacional, tendo a então Direção dos Serviços de Correios e Telecomunicações continuado a explorar o serviço público no regime interno. A ENATEL, Empresa Nacional de Telecomunicações foi criada pelo Decreto Nº17/80 de 13 de Fevereiro por decisão da Direção dos Serviços de Correios e Telecomunicações que deu origem a Empresa de Correios de Angola (AT, 2016).

Assim, a partir de 1980 e até a efetiva constituição da Angola Telecom, as telecomunicações em Angola foram asseguradas por dois Operadores públicos, mutuamente complementares, dedicando-se a EPTEL às comunicações internacionais e a ENATEL às comunicações domésticas.

3.1 Missão, Visão e Valores

A empresa rege a sua atividade, tendo por base a sua **missão**: "proporcionar serviços de telecomunicações acessível e de qualidade à todo o país, garantindo a

autossustentabilidade da empresa e contribuindo na linha da frente para o desenvolvimento de Angola" (AT, 2016).

No que diz respeito ao plano a longo prazo, a empresa tem como linha orientadora a **visão**: "Ser líder em ligar Angola ao mundo e ao futuro, merecendo, todo os dias, a confiança dos nossos clientes e a sua preferência pelos nossos serviços de telecomunicações" (AT, 2016).

A empresa acredita e guia-se pelos seguintes **valores**: *confiança*: a AT encara os clientes como parceiros, estabelecendo uma relação de confiança nos objetivos de cada um; *diferenciação*: a AT é diferente pela positiva, age com rapidez e eficiência; *excelência*: procurar a excelência, através da melhoria continua em tudo o que a empresa faz; *integridade*: a empresa assume e cumpre os seus compromissos com transparência e integridade; *inovação*: a empresa é inovadora nas suas ofertas de serviços; *desenvolvimento*: a AT é um espaço de desenvolvimento pessoal e profissional (AT, 2016).

3.2 Organograma

Na Figura 5, está representada a Estrutura Organizacional da AT, caracterizada hierarquicamente no nível de topo pela Administração, seguida pelos Órgãos de Assessoria e Apoio e pelas áreas de Gestão e Controlo.

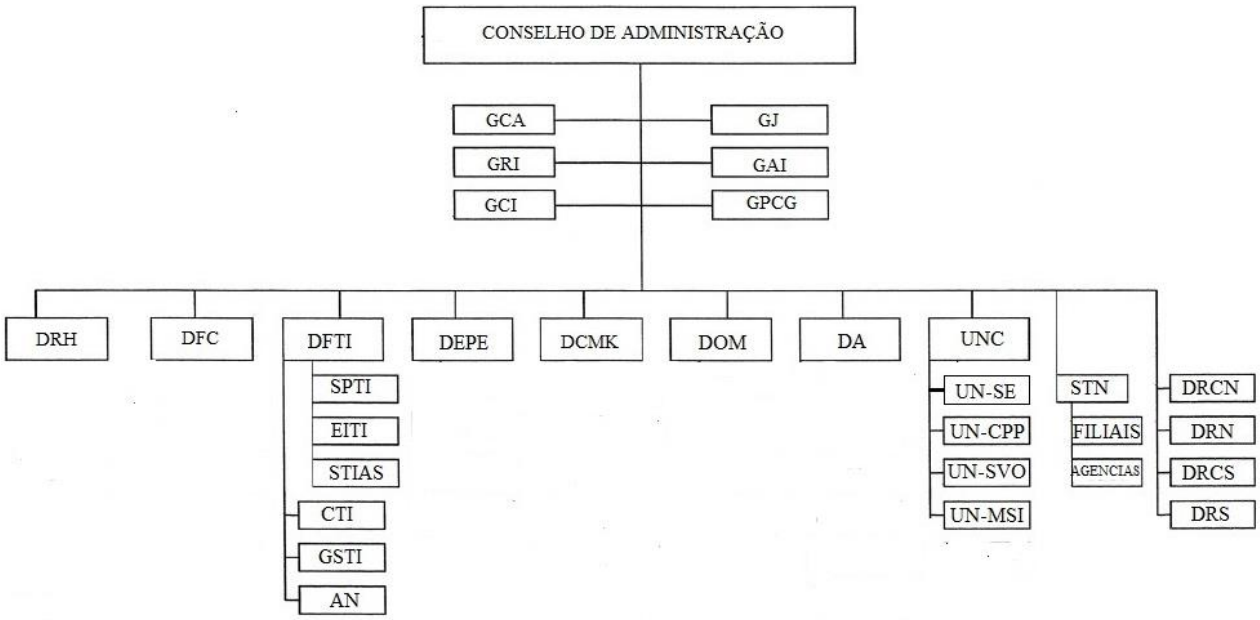


Figura 5- Organograma da AT

(AT, (2016))

Esta dissertação tem como área de estudo os SI, por isso o departamento de SI, aqui denominado por Direção de Fábrica de TI (DFTI) é alvo de atenção especial. A figura 6 representa o organograma do DFTI.

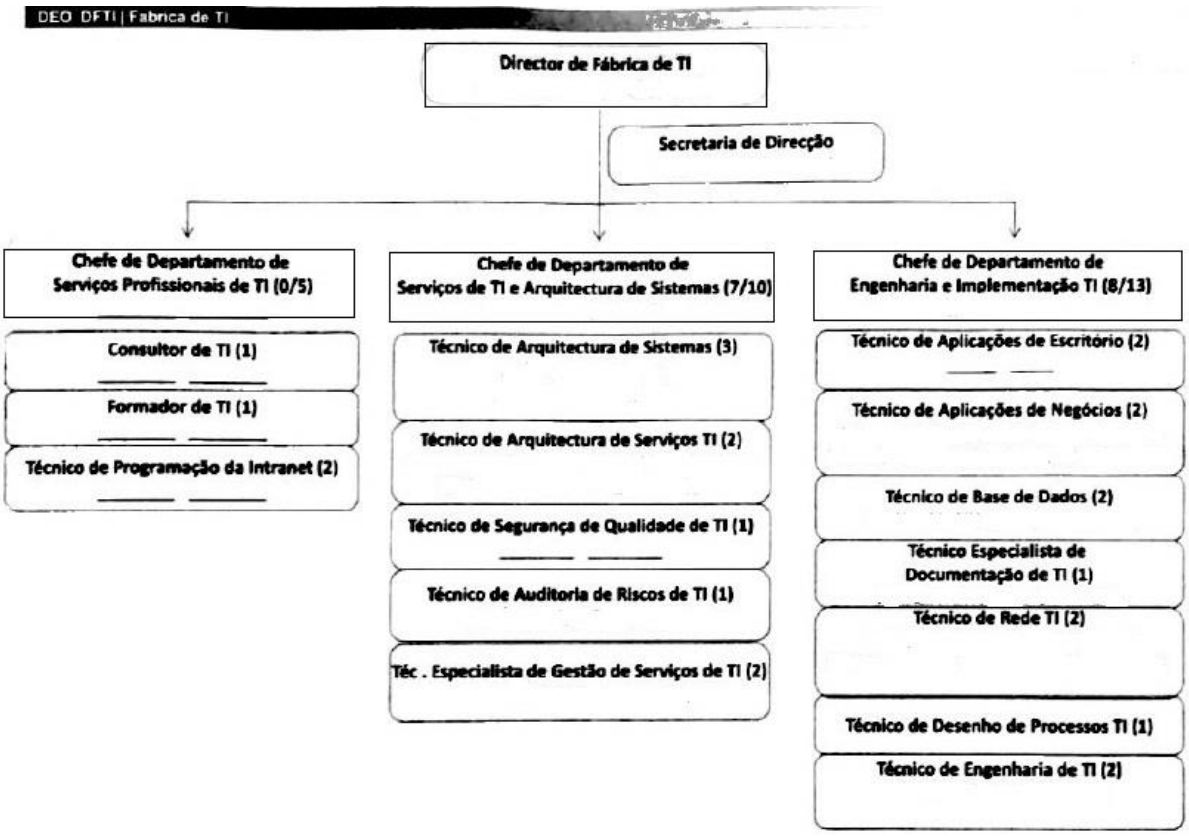


Figura 6- Organograma do DFTI

(AT, (2016)

3.3 Caracterização de SI

No que concerne aos SI, a AT aposta em sistemas de uso corporativo, visando uma maior uniformização de processos, de tecnologias e de integração entre os sistemas da organização.

A organização, em cooperação com parceiros internacionais têm projetos que consistem na implementação de Sistemas de Suporte às Operações (OSS) e Sistemas de Suporte ao Negócio (BSS) com soluções de *Order Management* e *Product Catalog* consideradas líderes de Mercado.

Os projetos de OSS para empresas fornecedoras de serviços de comunicações ajudam a reduzir drasticamente o custo operacional e impulsionam a agilidade através da racionalização de OSS. Também implica na gestão da integração de novas funções e

serviços dentro dos ambientes de OSS existentes, criando *Service Oriented Architectures* (SOA) onde antes existiam operações isoladas

Com mais de 100 colaboradores e ao longo dos últimos dois anos obteve as certificações CMMI3, ISO20000, MCSA, MCSE. Para além da aposta em certificações tecnológicas, conta ainda com mais de 100 colaboradores certificados nas práticas de gestão nomeadamente PMI, ITIL e 6 sigma.

A AT usa tecnologias da Rede Inteligente (IN – *Inteligence Netework*). A IN é um sistema que proporciona flexibilidade, confiança para base de dados e lida com as atuais e novas pesquisas e politicas dos serviços de telecomunicações.

A tecnologia IN tem vantagens na digitalização e comutação, gestão do sistema ou serviços de telecomunicações, monitoramento e execução de diferentes programas e permite aumentar a competição do negócio no mercado através da produção ou organização de novos serviços, detetar falhas no servidor e dar informações detalhadas aos técnicos. Para além de melhorar a evolução e o desenvolvimento dos serviços para os clientes ou utilizadores, a rede IN também tem a capacidade de gerir as invenções e criações dos padrões de telecomunicações.

Serviços como WIMAX e EVDO são duas soluções fundamentais na Internet que também trazem consigo um serviço de voz à disposição dos clientes da AT no empreendimento da rede comercial, oferecendo soluções DUAL para eles.

Para fazer face à demanda pelos serviços de *Cloud Platform*, nomeadamente nas áreas da virtualização, gestão, armazenamento, funcionamento em rede, infraestrutura de ambiente de trabalho virtual, proteção de acessos e informações, Web e plataforma de aplicações, entre outras, a AT o Windows Server 2012 R2.

A AT tem uma Política de Segurança da Informação com o objetivo de estabelecer requisitos para garantir o nível apropriado de proteção da Informação de todos os SI, incluindo plataformas de serviços de telecomunicações, que suportam as suas operações e o seu negócio.

A Política de Segurança da Informação aqui descrita é aplicável a todos os funcionários, fornecedores, consultores, incluindo os colaboradores de entidades externas ou outras entidades e/ou pessoas que acedam aos SI da AT, pelo que a todos deverá ser

disponibilizada para o desempenho das suas funções, sendo exigido destes o respeito pelos controlos de segurança implementados e o cumprimento dos seguintes valores:

Integridade – prevenção contra a modificação e/ou destruição não autorizada de Informação, salvaguardando a respetiva fiabilidade e origem;

Confidencialidade – prevenção contra o acesso e/ou divulgação não autorizados de Informação;

Disponibilidade – garantia do acesso autorizado à Informação sempre e na medida do necessário.

4 Estudo de caso

Conforme mencionado anteriormente, na secção 1.2. Metodologia, em que se abordou as questões subjacentes às metodologias considerou-se que o Estudo de Caso seria o mais indicado para a condução do estudo em causa. Optou-se pelo Estudo de Caso pois, segundo Macedo et al (2005), esta metodologia baseia-se na investigação de um fenómeno contemporâneo no contexto de uma situação real numa organização. O que vai ao encontro do que foi definido como objetivo desta dissertação, onde se pretende analisar e verificar os impactos da implementação da Segurança da Informação na usabilidade dos SI numa empresa de telecomunicações. Os mesmos autores referem ainda que a metodologia estudo de caso é por norma utilizada na investigação em SI pois, permite analisar os problemas desta área, tendo em atenção a organização em causa, assim como a sua envolvente.

De acordo com a sugestão de Yin (2009) para um estudo caso, realizou-se uma revisão de literatura para o tema identificado, uma breve caracterização da Organização em estudo e por fim o último passo consistiu em recolher os dados.

Os estudos na área da segurança da informação visam abordar situações de implementação de SGSI baseado numa norma como decisão estratégica de uma organização, promovendo a adoção de diretrizes, boas práticas e mecanismos de controlo relativamente à segurança da informação existente na mesma, por considerar a informação como o seu ativo mais valioso.

No caso em estudo procura-se apurar os impactos que a implementação de segurança da informação tem na usabilidade dos SI, designadamente no processo normal de trabalho dos colaboradores da AT. Procura-se avaliar que alterações resultaram dessa implementação, tanto a nível funcional, ou seja a eficácia na utilização do SI e como a nível da satisfação e da confiança dos utilizadores do SI.

De modo a alcançar os objetivos da dissertação, foi necessário analisar as políticas de segurança da informação implementadas e a utilização dos SI, através de inquéritos por questionário, dirigido aos colaboradores da organização.

4.1 Caracterização da População-Alvo

A população-alvo do questionário é composta por um universo de 276 pessoas, às quais foram enviados os questionários para preenchimento, não estando incluído, por questões de logística e das atividades que desempenham, a totalidade do pessoal em serviço na AT, ou seja, não se incluiu o pessoal do trabalho de campo, operário, de limpeza e motoristas, devido ao facto de não disporem de acesso ao SI da organização.

A população-alvo está repartida pelos seguintes tipos: 10 Gestores, 55 Técnicos e 211 Utilizadores Finais.

O tipo Gestores inclui o pessoal da Administração Geral, os Órgãos de Assessoria e Apoio (Gabinete do Conselho de Administração, Gabinete Jurídico, Gabinete de Relações Institucionais, Gabinete de Auditoria Interna, Gabinete de Comunicação e Imagem e Gabinete de Planeamento Controlo e Gestão).

O tipo Técnicos inclui os colaboradores da DFTI – Direção de Fábrica de TI (Departamento de Engenharia e Implementação de TI, Departamento de Serviços Profissionais de TI e Departamento de Serviços de TI e Arquitetura de Sistemas).

O tipo Utilizadores Finais inclui os colaboradores dos restantes departamentos da AT.

4.2 Técnicas de recolha de dados

Neste trabalho a técnica de recolha de dados a aplicar é o inquérito por questionário a ser submetido ao público-alvo sobre a área que constitui a base de especificação do objeto do estudo. Foram realizados três inquéritos por questionário, um para cada tipo de população-alvo.

O questionário elaborado para os gestores denominado Questionário-Gestores (QuestGes), apresentado no anexo A, pretendia obter a informações sobre as alterações verificadas na organização com a implementação do SGSI, na perspetiva da gestão. Buscava também informações sobre políticas e planos de segurança da informação em concordância com a estratégia corporativa, a legislação em vigor e um adequado equilíbrio entre investimento e risco. Levantaram-se questões acerca dos principais desafios

enfrentados pela organização relativas à segurança da informação, dos principais problemas identificados na segurança antes da implementação do sistema, quais ativos serão protegidos e quais as ameaças e vulnerabilidades a serem consideradas.

Questionário-Técnico (QuestTec) é o inquérito submetido aos técnicos, que tinha como objetivo obter informações sobre os procedimentos e mecanismos de proteção atualmente implementados comparados com o período antes da implementação, na perspetiva mais técnica.

O Questionário-Utilizador Final (QuestUF) apresenta questões mais gerais, descurando-se dos aspetos técnicos e da gestão do negócio. Todas as questões deste questionário encontram-se nos outros dois. Visam obter a informações sobre os impactos causados na utilização do SI pelos procedimentos e mecanismos de proteção atualmente implementados comparados com o período antes da implementação.

As questões colocadas apresentam-se em três tipos distintos: de escolha única, de escolha múltipla, e de classificação (valores entre 1 e 6). Algumas das questões de escolha única destinam-se apenas a controlar o fluxo de preenchimento dos questionários.

Os três modelos do questionário encontram-se estruturados em 4 grupos de questões. O grupo A destina-se a caracterizar o(a) inquirido(a), os outros grupos têm questões ligadas aos objetivos da dissertação. O grupo B caracteriza o ato de realizar tarefas no SI, o grupo C trata da Segurança da Informação no SI e o grupo D avalia a satisfação da utilização do SI.

O grupo A **(Identificação/Caracterização do(a) inquirido(a))** faz a caracterização pessoal de cada inquirido(a), nomeadamente sexo, idade, habilitações literárias, área ou departamento onde presta serviço e há quanto tempo exerce funções na organização. A estrutura das questões não permite a identificação do(a) inquirido(a), ou seja os questionários são anónimos. Este grupo no QuestGes e no QuestUF apresenta 5 questões, no QuestTec apresenta 6 questões, quer dizer, foi acrescentada uma questão ligada às responsabilidades ou funções de administração ou de suporte desempenhadas pelos técnicos.

O grupo B **(Realizar tarefas no SI)** procura avaliar a utilização do SI para os colaboradores realizarem as suas tarefas. Para tal, era importante saber se os colaboradores

tinham recebido formação para utilizarem o SI, com que frequência acediam ao SI e quais tarefas eram realizadas no SI. As questões B10, B11 e B12 dão resposta ao primeiro objetivo específico da dissertação **(Analisar se os utilizadores conseguem atingir os seus objetivos a nível de eficiência e de eficácia).** Por outro lado, as questões B13, B14 e B15 estão ligadas ao terceiro objetivo específico da dissertação **(Analisar a redução ou aumento de erros dos utilizadores com a utilização do SI).** Este grupo em qualquer dos questionários apresenta as mesmas questões e são 20.

O grupo C **(Segurança da Informação no SI)** apresenta questões sobre a existência de um SGSI ou políticas de segurança, e a participação do(a) inquirido(a) na sua definição, registos de incidentes, ações de sensibilização. São também apresentadas questões sobre quais poderiam ser os maiores impedimentos para a segurança da informação. Este grupo no QuestGes apresenta 29 questões, 25 questões no QuestTec e 21 questões no QuestUF.

O grupo D **(Avaliar a satisfação da utilização do SI)**, as questões têm o objetivo de levar o(a) inquirido(a) a avaliar o impacto das práticas de segurança da informação na satisfação da utilização do SI. O grupo está relacionado ao segundo objetivo específico da dissertação **(Avaliar a satisfação da utilização do SI).** A questão D8 dá resposta ao quarto e último objetivo específico da dissertação **(Perceber quê relação de confiança têm os utilizadores com o SI)**. O grupo D apresenta 8 questões em qualquer dos questionários.

As questões D2, D3, D4 e D5 foram baseadas no QUIS (*Questionnaire for User Interface Satisfaction*). O QUIS é um inquérito de testes desenvolvido especificamente para medir a satisfação dos utilizadores, apresenta quatro factores: aprendizagem, terminologia e fluxo da informação, *output* do sistema, características do sistema Chin et al. (1988).

Para uma melhor compreensão das questões colocadas, apresenta-se no início de alguns grupos dos questionários, definições consideradas essenciais acerca de aspetos relevantes e cujo significado possa ser desconhecido por parte de alguns dos(as) inquiridos(as), ou seja, mais concretamente as definições de: Sistema de Informação no grupo B, Segurança da Informação no grupo C e Usabilidade no grupo D. Também são apresentadas explicações através dos textos de ajuda dos questionários, sobre termos e conceitos nas questões mais difíceis de se interpretar.

Os questionários apresentam alguns termos e expressões que foram utilizados para caracterizar as mesmas situações, são os casos de: departamento e área da estrutura orgânica no QuestGes; e sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI e segurança da informação em todos os questionários.

Os inquéritos foram realizados com o suporte da ferramenta de realização de formulários *online*, do *Google Drive*. O *link* de acesso ao inquérito e a explicação e solicitação do seu preenchimento foi enviado aos(às) inqueridos(as) através de uma mensagem de *email*. O tratamento e a análise das respostas aos questionários foram feitos numa folha de cálculo do Microsoft Excel, pertencentes à mesma ferramenta, que também proporciona a realização de tabelas e gráficos dinâmicos.

Os questionários apresentam algumas questões ligadas aos objetivos específicos da dissertação, por isso são de resposta obrigatória. Não foram configuradas as demais questões como sendo de resposta obrigatória por causa do pouco tempo disponível para os(as) inqueridos(as) responderem.

5 Análise de Resultados

O uso da quantificação, tanto na recolha como no tratamento da informação, utilizando técnicas estatísticas, confere objetividade aos resultados e evita distorções de análise e de interpretação, adquire-se, assim, uma maior margem de segurança na investigação.

Com o objetivo de melhor se compreender e interpretar o impacto que a implementação da Segurança da Informação tem na usabilidade dos SI das organizações, realizaram-se três questionários (gestores, técnicos e utilizadores finais) tendo como público-alvo os funcionários dos diferentes departamentos da AT, e que contou um universo de 215 inquiridos. Possibilitaram a obtenção de uma visão mais aprofundada sobre a questão em estudo. Esperam-se por dois cenários: 1) Colaboradores que estão há vários anos na organização e que viram a implementação da Segurança da Informação podendo descrever as alterações ao nível da segurança e da usabilidade do SI. 2) Colaboradores que estão há pouco tempo na organização e que não viram a implementação da Segurança da Informação e que ainda assim podem descrever os impactos positivos ou negativos que a segurança tem na facilidade de uso do SI.

Neste capítulo, o objetivo é realizar a análise e discussão dos resultados obtidos através dos inquéritos, para tal foi realizada a sumarização e tratamento estatístico desses dados, podendo ser consultados na íntegra no Anexo D. Aqui optou-se por uma análise dos aspetos considerados mais relevantes e dos grupos de questões relacionadas aos objetivos específicos da dissertação.

A tabela 1 apresenta a dimensão da amostra e o número de respostas obtidas, ou seja, a totalidade dos questionários distribuídos por modelo, efetuando também a avaliação dos que foram respondidos e a respetiva percentagem relativamente aos que foram entregues.

Modelo do questionário	Entregues	Devolvidos	% Devolvidos
Questionário-Gestores	10	8	80,0
Questionário-Técnico	55	45	81,8

Questionário-Utilizador Final	211	162	76,7
Total de questionários	**276**	**215**	**77,8**

Tabela 1- Avaliação dos questionários

5.1 Identificação/Caracterização do(a) inquirido(a)

No que diz respeito à identificação dos inquiridos, no QuestGes verificou-se que a proporção é de 50% masculino e 50% feminino, o que revela que as mulheres reforçaram a presença no mercado do trabalho. Quanto ao escalão etário, observou-se que a maioria (75%) tem mais que 45 anos e o restante (25%) está na faixa de 30 a 45 anos. Não se verificou nenhum inquerido com menos de 30 anos. Quanto aos valores respetivos às habilitações literárias, constatou-se uma proporção de 50% para doutoramento e 50% para mestrado, habilitações frequentes de quem ocupa cargos na gestão de topo.

No que toca ao escalão etário no QuestTec verificou-se que os inqueridos encontram-se maioritariamente (60,0%) entre 25 a 40 anos. O mesmo acontece no QuestUF com 53,1%, dados que revelam que a organização tem uma força de trabalho jovem para a área operacional. Em termos de habilitações literárias, no QuestTec verifica-se que a Licenciatura é a resposta mais frequente (64,5%), o que se mostra suficiente para exercer a função, por seu lado, no QuestUF uma minoria das respostas (5,5%) foi para a opção Ensino Secundário, um número bastante elevado para os padrões atuais no tipo de atividade desenvolvida pela organização, mas Licenciatura (79,0%) é a resposta mais frequente.

Ainda dentro da caracterização dos inqueridos, a questão relativa à área ou departamento da organização em que exerce função é muito importante, pois através dela consegue-se perceber quais tarefas requerem mais o SI. No QuestGes a maioria dos inquiridos (62,5%) respondeu Órgãos de Assessoria e Apoio. No QuestUF a resposta mais frequente foi Direção de Operação e Manutenção. Mas mais importante é a questão relativa ao tempo de exercício de funções, pois ele revela quais inquiridos viram ou não a implementação de sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI. No QuestGes 87,5% dos inquiridos exerce funções há mais de 5 anos, no QuestTec metade das respostas (50,0%) foi para mais de 5 anos e a outra metade (38,1%) e (11,9%) de 1 a 5 anos e menos de 1

ano, respetivamente. No QuestUF verificou-se 45,7% para inquiridos que estão na organização de 1 a 5 anos e (35,8%) e (18.5 %) para mais de 1 ano e menos de 1 ano, respetivamente.

5.2 Realizar tarefas no SI

A análise dos resultados deste grupo será efetuada em função da ligação entre as questões B10, B11 e B12 com o objetivo específico da dissertação que visa analisar se os utilizadores conseguem atingir os seus objetivos a nível de eficiência e de eficácia; e entre as questões B13, B14 e B15 com o objetivo específico da dissertação que pretende analisar a redução ou aumento de erros dos utilizadores com a utilização do SI.

A tabela 2 apresenta os itens das questões B10, B11 e B12 dos três questionários.

Questões	QuestGes	QuestTec	QuestUF
Classifique o seu grau de facilidade em executar tarefas no SI. (6 para muito fácil e 1 para muito difícil)	B10	B10	B10
Indique o seu grau de desempenho ao executar tarefas no SI. (6 para elevado desempenho e 1 para baixo desempenho)	B11	B11	B11
Indique o quão rápido é executar tarefas no SI. (6 para muito rápido e 1 para muito lento)	B12	B12	B12

Tabela 2- Questões sobre a utilização do SI com eficiência e eficácia

No que respeita ao grau de facilidade em executar tarefas no SI, verificou-se que a totalidade (100%) dos inquiridos do QuestGes e do QuestTec respondeu o valor 6, ou seja, para eles é muito fácil. Já no respeitante aos inquiridos do QuestUF, a resposta maioritária (69,1%) também foi '6 - muito fácil', apesar disso, constata-se que a opção '1 – muito difícil' apresenta valores de realce (15,4%), possivelmente influenciada pelo facto de 4,9% dos inquiridos não ter recebido formação para a utilização do SI e 51,9% revelou ter tido formação uma única vez.

No que tange ao grau de desempenho ao executar tarefas no SI, as respostas do QuestGes e do QuestTec voltaram a ser absolutas (100%), respondendo '6 – elevado

desempenho'. No QuestUF 68,5% das respostas foram '6 – elevado desempenho' e 26,5% foram '5' que tende para o elevado desempenho.

Quanto a rapidez em executar tarefas no SI, as respostas do QuestGes e do QuestTec tiveram o mesmo comportamento em relação aos itens B10 e B11, ou seja, 100% dos inquiridos respondeu '6 – muito rápido'. Quanto ao QuestUF, a maioria (69,1%) optou pela '6 – muito rápido'.

Em função das respostas aos itens das questões B10, B11 e B12 dos três questionários, constata-se que os utilizadores conseguem atingir os seus objetivos a nível de eficiência e de eficácia, pois segundo Norman e Draper (1986) um SI orientado para a usabilidade possui uma interface que deve ser usada para se executar uma tarefa sem ser ela o centro das atenções, de modo a permitir que os utilizadores não precisem se concentrar na interface em si, mas apenas no trabalho que eles desejam executar.

A tabela 3 apresenta os itens das questões B13, B14 e B15 dos três questionários, sobre a redução ou aumento de erros na utilização do SI.

Questões	QuestGes	QuestTec	QuestUF
Classifique o SI quanto a prevenção de erros. (6 para elevado desempenho e 1 para baixo desempenho)	B13	B13	B13
O utilizador é avisado pelo SI se está a cometer um erro grave. (6 para concordo e 1 para discordo)	B14	B14	B14
O SI ajuda o utilizador a reconhecer, diagnosticar e recuperar dos erros. (6 para concordo e 1 para discordo)	B15	B15	B15

Tabela 3- Questões sobre a redução ou aumento de erros na utilização do SI

Todos os inquiridos (100%) do QuestGes e do QuestTec responderam '6 – desempenho elevado' para classificar o SI em relação à prevenção de erros. Em relação ao QuestUF, constatou-se que a maioria optou pela resposta '6 – desempenho elevado', no mesmo sentido, uma boa parte (33,3%) dos inquiridos optou por responder '5', que não é o máximo desempenho, mas é satisfatório.

Quanto à questão B14, os inquiridos de todos os questionários concordam que o SI emite mensagem para alertar quando o utilizador está na eminência de cometer um erro

grave, optando pela resposta '6 – desempenho elevado' 100% do QuestGes, 97,8% do QuestTec e 64,2% do QuestUF.

Os inquiridos do QuestGes e do QuestTec na sua totalidade (100%) considera que o SI ajuda o utilizador a reconhecer, diagnosticar e recuperar dos erros. No mesmo sentido, a maioria (63%) das respostas do QuestUF a opção foi '6 - concordo'.

Desta feita, os inquiridos dão indicações de que as mensagens de erro são claras e ajudam o utilizador a corrigir ou ultrapassar os erros. Segundo Nielsen, (2012), ainda melhor do que boas mensagens de erro é um projeto cuidadoso que impede que um problema ocorra em primeiro lugar ou eliminar as condições passíveis de erros ou buscar por eles e apresentar aos utilizadores uma opção de confirmação antes que eles cometam a ação.

5.3 Segurança da Informação no SI

A partir dos dados obtidos no grupo C - Segurança da Informação no SI, dos inquéritos à organização estudada, verificou-se um conjunto de questões consideradas relevantes para análise. A tabela 4 apresenta as referidas questões e as suas denominações nos questionários.

Questões	QuestGes	QuestTec	QuestUF
Desde a sua entrada na Organização foi feita alguma implementação de um sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI?	C1	C1	C1
Classifique a sua perceção acerca do funcionamento do SI depois da implementação do sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI. (6 para elevado, 1 para baixo)	C6	C6	C6
Quais os principais problemas identificados na segurança antes da implementação do sistema?	C14	C14	-
Quais os principais aspetos positivos identificados na segurança antes da implementação do sistema?	C15	C15	C13

Na sua opinião, qual é a importância que a segurança da informação tem no funcionamento da instituição e das suas atividades diárias no SI?	C16	C16	C14

Tabela 4- Questões relevantes sobre a Segurança da Informação

Relativamente à questão sobre implementação de um sistema de gestão de políticas de segurança do SI, constatou-se tendências diferentes nos três questionários. Essa questão é importante para os objetivos dessa dissertação, porque apresenta informação sobre os funcionários da organização que que testemunharam ou não a implementação da Segurança da Informação podendo descrever os seus impactos na usabilidade do SI. As respostas são influenciadas pelo tempo de trabalho na organização e pela área em que desempenha funções.

No QuestGes, as respostas positivas apresentaram uma percentagem de 87,5, ou seja, a maioria dos inquiridos respondeu 'Sim' quando questionados se desde a sua entrada na Organização tinha sido feita alguma implementação de um sistema de gestão de segurança do SI, contra 12,5% que respondeu 'Não'. Já no QuestTec as respostas positivas foram de 53,3% e 42,2% de 'Não', o restante (4,4%) de 'Não sabe'. Quanto ao QuestUF, 37,7% dos inquiridos respondeu 'Sim', 39,5% respondeu 'Não sabe' e 22,8 'Não'.

A questão da classificação da perceção dos funcionários acerca do funcionamento do SI depois da implementação do sistema de gestão de políticas de segurança, tinha uma escala de resposta (6 para elevada, 1 para baixa). Os resultados obtidos permitiram avaliar que todos os inquiridos (100%) do QuestGes e do QuestTec responderam '6 – elevada', no caso do QuestUF, os inquiridos revelaram ter uma elevada perceção do SI, tendo como resultados 75,4% optado '6' e 19,6% '5'.

A questão relacionada aos principais problemas identificados na segurança antes da implementação do sistema, só foi colocada no QuestGes e no QuestTec porque os seus inquiridos têm conhecimentos sobre aspetos importantes do negócio e sobre aspetos técnicos do SI respetivamente, tendo então a legitimidade para responderem à questão. A tabela 5 apresenta a referida questão.

C14 – Quais os principais problemas identificados na segurança antes da implementação do sistema? (Assinale todos os itens aplicáveis)		
	Gestores	Técnicos

	Nº	%	Nº	%
Perda de Confidencialidade	7	100,0	23	95,8
Perda de Integridade	7	100,0	23	95,8
Perda de Disponibilidade	7	100,0	23	95,8
Outro	0	0,0	0	0,0
Não Responderam	0	0,0	1	4,1
Total de Respostas	7		24	

Tabela 5- A questão relacionada aos principais problemas identificados na segurança antes da implementação do sistema

No que diz respeito aos resultados realça-se que tanto os inquiridos do QuestGes como os do QuestTec, unanimemente responderam que os principais problemas na segurança antes da implementação do sistema era a perda de confidencialidade de integridade, de disponibilidade.

Quanto à questão sobre os principais aspetos positivos identificados na segurança antes da implementação do sistema, verificou-se no QuestGes que os inquiridos na sua maioria (71,4%) optaram por responder por 'Outros' aspetos e 28% optaram por 'Rapidez na execução de tarefas'. Isto ficou a dever-se ao facto da visão dos gestores sobre o negócio em relação à segurança. No QuestTec a maioria (95,8%) das respostas foi 'Rapidez na execução de tarefas' e 'Responsabilidade para decidir sobre a segurança'. Por seu lado, no QuestUF, verificou-se semelhantemente a opção pela 'Rapidez na execução de tarefas' e 'Responsabilidade para decidir sobre a segurança', 77,0% e 81,9% respetivamente. Tanto os técnicos quanto os utilizadores finais as encaram como características fundamentais para executarem os seus trabalhos com efetividade.

Relativamente à questão sobre é a importância que a segurança da informação tem no funcionamento da instituição e das suas atividades diárias no SI, verificou-se os seguintes resultados apresentados nos gráficos 1, 2 e 3.

.

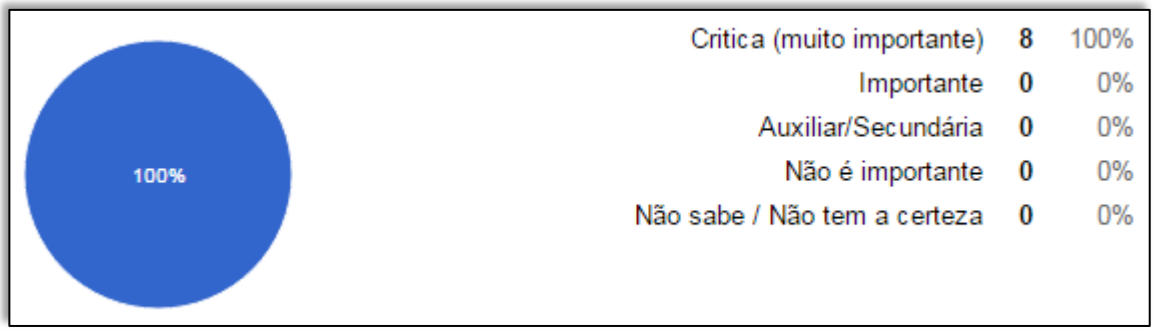


Gráfico 1- - Importância da segurança da informação na organização (QuestGes)

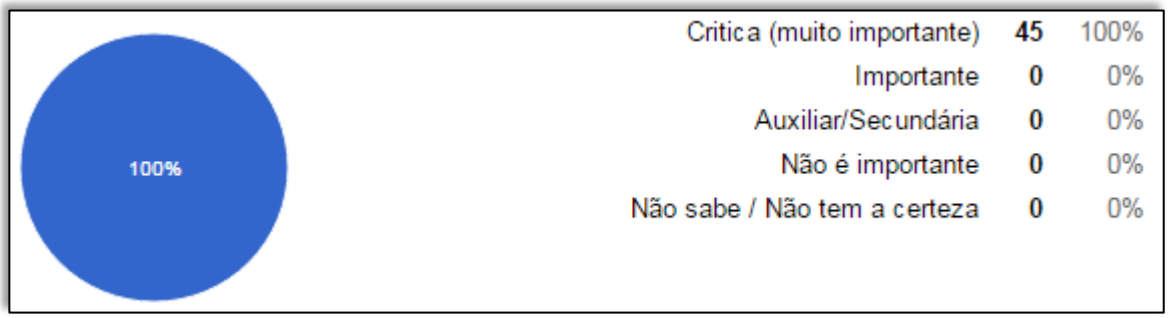


Gráfico 2-Importância da segurança da informação na organização (QuestTec)

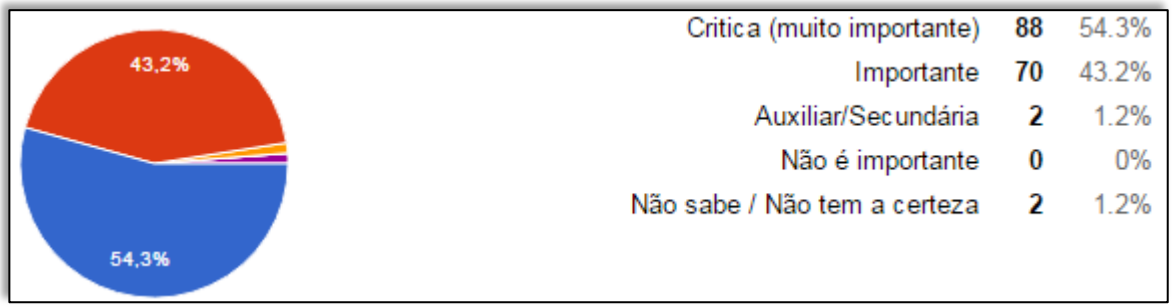


Gráfico 3- Importância da segurança da informação na organização (QuestUF)

5.4 Avaliar a satisfação da utilização do SI

No que respeita à avaliação da satisfação da utilização do SI por parte dos colaboradores da organização, constatou-se que há um grande grau de satisfação por parte

dos inquiridos com as políticas de segurança da informação. Os gráficos 4, 5 e 6 apresentam esses dados.

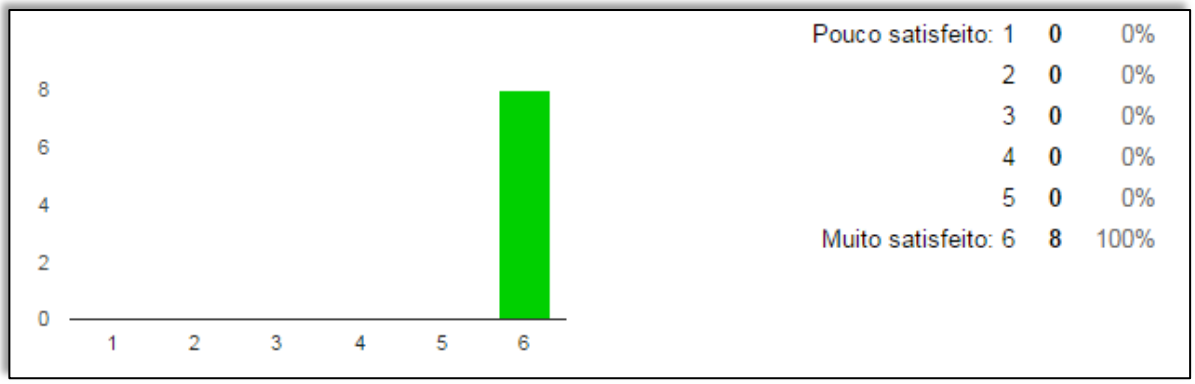


Gráfico 4- Grau de satisfação com as políticas de segurança da informação (QuestGes)

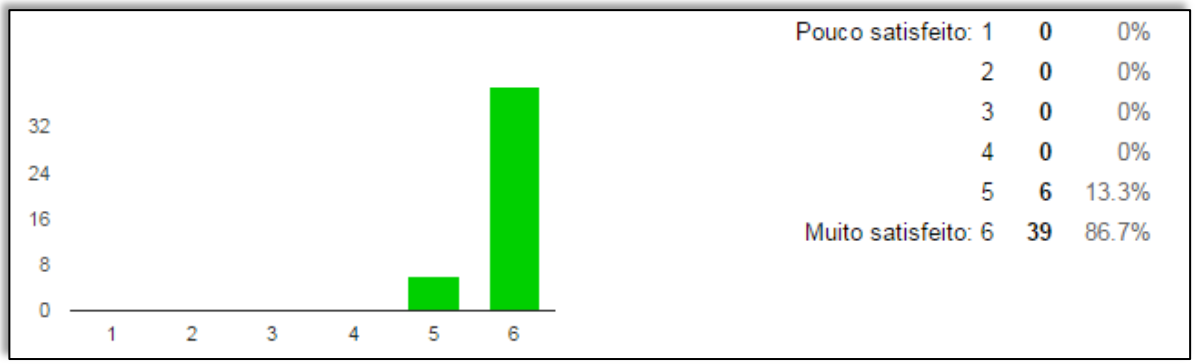


Gráfico 5- Grau de satisfação com as políticas de segurança da informação (QuestTec)

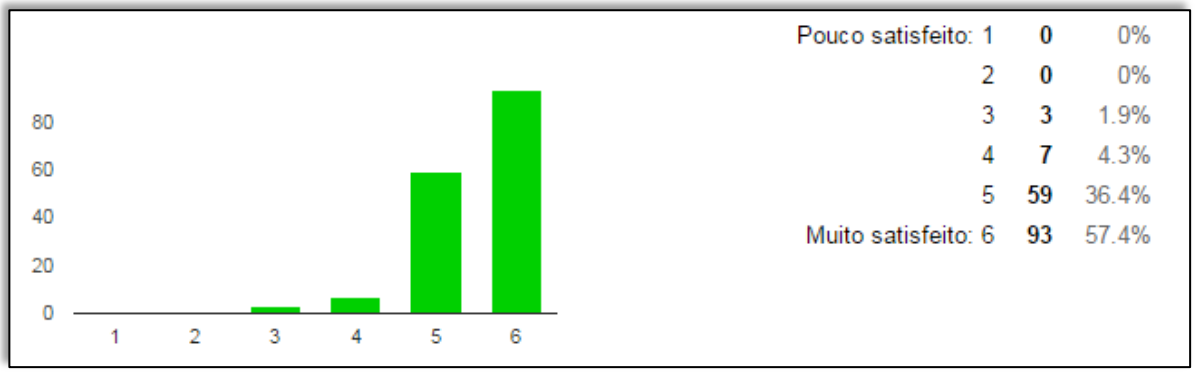


Gráfico 6- Grau de satisfação com as políticas de segurança da informação (QuestUF)

Relativamente aos fatores que levam o utilizador a ter confiança no SI, os inquiridos revelaram que trabalhar com o SI dá satisfação, destacaram o quão rápido é de se trabalhar

no sistema e a facilidade de utilização. A tabela 6 apresenta com maiores detalhes os resultados obtidos.

D7 – Quais são os fatores que levam o utilizador a ter confiança no SI? (Assinale todos os itens aplicáveis)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
O sistema é fácil de usar	8	100,0	43	95,6	153	94,4
É rápido de se trabalhar no sistema	8	100,0	44	97,8	139	85,8
Aumenta a produtividade do utilizador	8	100,0	41	91,1	143	88,3
Proporciona ao utilizador alcançar os objetivos estabelecidos	8	100,0	41	91,1	148	91,4
Trabalhar com o SI dá satisfação	8	100,0	45	100,0	137	84,6
Reduz os erros ao trabalhar no SI	8	100,0	37	82,2	147	90,7
Não Responderam	8	100,0	0	0,0	0	0,0
Total de Respostas	8	100,0	45		162	

Tabela 6-Questão sobre os fatores que levam o utilizador a ter confiança no SI

No que respeita ao grau de confiança que tem com o SI, verificou-se que a totalidade (100%) dos inquiridos do QuestGes respondeu o valor 6, ou seja, eles têm confiança total no SI. No QuestTec, verificou-se também um grau elevado de confiança no SI, onde 95,6% optou pelo grau 6 e 4,4% optou por 5. Já no respeitante aos inquiridos do QuestUF, a resposta maioritária (70,4%) também foi '6 - confiança', revelando que o SI tem credibilidade para os inquiridos.

5.5 Apreciação crítica do caso de estudo e recomendações

Através da análise e discussão, dos resultados obtidos verificou-se que os inquiridos conseguem utilizar o SI para a realização de tarefas com eficácia e eficiência, ou seja, com a precisão para atingir um objetivo específico e com a utilização dos recursos necessários para alcança-lo. Com esta constatação pode levar em consideração a conjuntura das vantagens de um SI que consistem na otimização do fluxo de informação, redução de

custos, ganho na produtividade, maior integridade e veracidade nas informações e maior segurança nas informações Laudon e Laudon (2007).

Verificou-se igualmente uma análise positiva por parte dos inquiridos em relação ao cometimento de erros com a utilização do SI, onde o utilizador consegue reconhecer, diagnosticar e recuperar dos erros, ou seja, o SI ajuda o utilizador em relação à prevenção de erros alertando-o quando está na eminência de cometer um erro grave (Hughes et al., 2014).

Através dos resultados obtidos das questões sobre a segurança de informação, verificou-se que está implementado um sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI, mas uma parte considerável dos utilizadores finais não tem noção da existência desse sistema. Contudo, identificaram-se igualmente diversos problemas de segurança associados aos comportamentos e práticas dos colaboradores (Erro humano e Procedimentos negligentes) que causaram violações à segurança do SI (como a perda ou roubo de dados). Isto é um ponto a melhorar, pois de acordo com Ng et al., (2009), pesquisas mostram que os utilizadores sentem-se incentivados a participar em programas de segurança quando têm a perceção: de que estão suscetíveis a ataques; dos benefícios advindos das ações de segurança; das facilidades de interação com os controlos de segurança; e a gravidade de cometer-se uma falha de segurança.

A análise dos resultados revelou, ainda, que mesmo depois da implementação do sistema de segurança os inquiridos apresentam um grau elevado de perceção da utilização do SI. A análise ao processo de implantação de um SGSI, tomando-se por base aos métodos qualitativos, poder-se-ia chegar a conclusões precipitadas, quanto ao sucesso ou fracasso desse projeto. Muitas vezes, prefere-se avaliar o impacto do sistema identificando-se os benefícios tangíveis e intangíveis alcançados a partir dele. Os benefícios tangíveis são aqueles que produzem vantagens económicas quantificáveis à organização (Kendall & Kendall 1991), por ex: a dinamização do processo, tais como melhorias no fluxo de trabalho e no fluxo de material, a pontualidade da informação, a redução no tempo de execução de uma tarefa e redução de procedimentos. Os benefícios intangíveis são difíceis de quantificar, tais como a melhoria no processo de tomada de decisão, a redução de erros, a melhoria dos serviços aos clientes, a imagem dos

organização etc. Constatou-se também que antes da implementação do sistema, a rapidez na execução de tarefas e a responsabilidade para decidir sobre a segurança eram aspetos positivos, por isso deduz-se que houve impactos nesses aspetos após a implementação do sistema.

Verificou-se também que os inquiridos têm a perceção que a segurança da informação tem uma grande importância no funcionamento da instituição e das suas atividades diárias no SI. Com base nessa ideia, Sharma et al. (2012), dizem que a confiabilidade das pessoas é um dos fatores determinantes no levantamento de riscos em segurança da informação. O que afigura-se como um impacto bastante significativo, tal como demonstrado em estudos anteriores (Fernandes & Souza), consolidando a ideia de que a confiança é um fator determinante na segurança da informação e em todos os momentos no contexto organizacional.

Aprendizagem revela ter impacto na Satisfação. Este fator é tido em conta pelas organizações, com especial atenção aos novos utilizadores (Nielsen, 2000). Pela pouca experiência de utilização do SI, os novos utilizadores não pretendem perder muito tempo a habituar-se a novas funcionalidades, pelo que é espectável que o SI proporcione o que um utilizador deseja com o mínimo esforço requerido (Lee & Kozar, 2012). O impacto positivo pode dever-se à formação proporcionada aos novos utilizadores, o que acelerou facilidade na compreensão e execução das tarefas, aumentado a satisfação destes. Evidenciando assim o conceito que Green e Pearson, (2010) apresentaram na sua pesquisa.

Observando os resultados obtidos, verifica-se que a Adaptação ao SI enquanto *software*, a terminologia usada e a Capacidade do sistema revelaram ter impacto direto na Satisfação. A análise revelou que os inquiridos confiam no SI, e os fatores que os levam a ter essa confiança são: trabalhar com o SI dá satisfação, a rapidez de se trabalhar no sistema e a facilidade de utilização. O grande impacto pode ser justificado pela qualidade e atualização da informação e o facto da facilidade de utilização não ter sido afetada após a implantação do SGSI.

Neste trabalho, a importância de um enquadramento teórico para a interpretação dos resultados decorrentes da análise de dados levou à escolha da teoria institucional como base para essa interpretação. Segundo Scott (2004), a teoria institucional cuida dos aspetos da estrutura social, considerando os processos pelos quais as estruturas (tais como,

esquemas, regras, normas e rotinas) se estabelecem como linhas orientadoras e confiáveis para o comportamento social e investigando a forma como estes elementos são criados, difundidos, adotados e adaptados ao longo do tempo e do espaço; e a forma como eles caem em declínio e desuso.

As recomendações para implementação de SGSI na generalidade das organizações dadas pela norma ISO/IEC 27001 (2013), considerando obviamente as especificidades apresentadas por cada uma delas compreende uma série de ações importantes e indispensáveis: a consciência da necessidade de segurança da informação; a atribuição de responsabilidades pela segurança da informação; incorporar o compromisso da gestão e os interesses de todas as partes interessadas; reforçar os valores da sociedade; avaliar os riscos que determinam os controlos adequados para atingir níveis aceitáveis de risco; prevenção ativa e deteção de incidentes de segurança da informação; e reavaliação contínua da segurança da informação.

De acordo com os resultados do caso de estudo, recomenda-se identificar e examinar as atividades de negócio da organização e a preponderância que a informação tem no mesmo, visando a mensuração do nível de Segurança da Informação necessário.

Propõe-se também zelo na elaboração das Políticas de Segurança da Informação, que caracterizam o conjunto de princípios, valores e propósitos da organização, traduzidos em regras específicas para proteger o SI.

Durante a implementação da Segurança da Informação na organização, deve-se realizar a atividade mais importante que é engajar as pessoas no projeto, comprometendo-as com a segurança, sensibilizando-as e realizando ações de formação.

De acordo com Santos (2006) as *interfaces* desenvolvidas sem o atendimento aos requisitos de usabilidade levam a uma performance deficiente e a uma redução da qualidade da interação do utilizador com um SI.

A usabilidade de um sistema é atingida quando recomendações de usabilidade são obedecidas desde o projeto inicial. Quando isso ocorre, o sistema apresenta atributos relacionados à usabilidade como a facilidade de aprendizagem, a eficiência de uso, a facilidade de memorização, a baixa taxa de erros e a satisfação subjetiva (Nielsen, 1993).

Recomenda-se às organizações a optarem por um SI que tenha um modelo híbrido de abordagem de segurança e usabilidade (Kainda et al., 2010). Entretanto, avaliações de usabilidade de SI seguros requerem engajamento da organização e procedimentos que se afastem do comum.

6 Conclusão e perspetivas de trabalho futuro

A proteção dos SI abrange o impedimento de serviço a utilizadores não autorizados, assim como contra a intrusão, e a modificação não autorizada de dados ou informações, armazenados, em processamento ou em trânsito, incluindo até a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das TICS, assim como as destinadas a prevenir, detetar, deter e documentar eventuais ameaça a seu desenvolvimento.

Por sua vez, a usabilidade é uma característica de um determinado produto ser fácil de usar, fácil e rápido de aprender, não provocar erros ou caso ocorram sejam facilmente resolvidos, solucionar as tarefas que ele se propõe a resolver com eficiência e eficácia e oferecer um alto grau de satisfação para os seus utilizadores (Nielsen, 1993).

Esta dissertação de mestrado teve como objetivo avaliar os impactos da implementação da Segurança da Informação na usabilidade do SI numa empresa angolana de telecomunicações. Neste âmbito, tendo-se considerado pertinente analisar os efeitos após implementação da Segurança da Informação, perceber as alterações positivas ou negativas na facilidade de utilização dos SI, realizou-se um enquadramento teórico sobre as várias temáticas associadas a este problema, e de modo a alcançar os objetivos da dissertação, foi necessário realizar um caso de estudo para analisar as políticas de segurança da informação implementadas e a utilização dos SI, através de inquéritos por questionário, dirigido aos colaboradores da organização.

De certa forma, pretende-se analisar se os utilizadores conseguem atingir os seus objetivos a nível de eficiência e de eficácia; avaliar a satisfação da utilização do SI; analisar a redução ou aumento de erros dos utilizadores com a utilização do SI; e perceber qual relação de confiança têm os utilizadores com o SI.

6.1 Conclusões

No que respeita ao estudo empírico concluiu-se que pensar em segurança e usabilidade separadamente é uma perspetiva que tende a ficar obsoleta. As pessoas nas organizações

querem realizar as suas tarefas quotidianas no SI de uma forma rápida, transparente e simples. Além da usabilidade, as pessoas exigem cada vez mais segurança.

Com base nesta perspetiva, surge o uso de novas abordagens de segurança da informação que ajuda no objetivo de desenvolvimento de SI que juntam segurança com usabilidade, como sugere Heckel (1991), um SI com boas interfaces com utilizadores, deve ser projetado a pensar mais em comunicação do que em computação.

Esta perspetiva veio ainda influenciar mudanças a nível de *design*, tentando equilibrar as necessidades técnicas dos utilizadores com e sem experiência na utilização de SI para alcançar objetivos específicos com eficácia, eficiência e satisfação num contexto específico.

Conclui-se também que as pessoas são a parte mais importante da segurança da informação, a maior causa dos problemas de segurança apontam frequentemente para resultados que indicam ser a negligência dos colaboradores, mais do que os ataques vindos do exterior (Reddick, 2010). A segurança da informação não é apenas uma questão de *hardware* e *software*, abrange também questões relacionadas com a gestão de pessoas, processos e tecnologia. A sua implementação deve ser um processo contínuo e da responsabilidade de toda a organização.

Tendo em conta aos resultados obtidos do estudo de caso, tentou-se encontrar alguma relação entre implementação da segurança da informação e repercussões na usabilidade dos SI, ou seja, procurou-se avaliar os impactos da implementação da segurança da informação na usabilidade dos SI, no processo normal de trabalho dos colaboradores da organização. Procura-se avaliar quê alterações resultaram dessa implementação, tanto a nível funcional, ou seja a eficácia na utilização do SI e como a nível da satisfação e da confiança dos utilizadores do SI.

Verificou-se que a responsabilidade sobre a segurança da informação antes da implementação do sistema não estava bem definida, neste sentido, a incumbência estava atribuída à três entidades da organização, que são: a gestão do topo, o chefe do departamento e o técnico da informática. Constatou-se ainda que a forma como era gerida a segurança da informação não dava grandes garantias de proteção e deixava muito a desejar, pois a segurança passava por arquivos trancados fisicamente, implementação de

políticas aleatórias e a simples utilização do conjunto utilizador-password. A planificação estratégica da segurança assume na organização uma importância determinante, na medida em que a dinâmica do processo construtivo exige uma antecipação considerável na previsão das medidas em conformidade com algum normativo.

Foi ainda possível constatar que antes da implementação do sistema, a rapidez na execução de tarefas e a responsabilidade para decidir sobre a segurança eram aspetos positivos, por isso deduz-se que houve impactos nesses aspetos após a implementação do sistema. O mesmo aplica-se a perda de confidencialidade, de integridade e de disponibilidade.

Finalmente, os objetivos específicos permitiram concluir que:

- Os utilizadores conseguem atingir os seus objetivos a nível de eficiência (esforço e recursos utilizados para alcançar um objetivo) e de eficácia (precisão com que os utilizadores atingem um objetivo específico) na utilização do SI.

- Há um grande grau de satisfação por parte dos inquiridos com a utilização do SI. Sendo que vários fatores contribuíram para essa situação: satisfação com o SI enquanto software, com a terminologia e informação do sistema, com a aprendizagem, com a capacidade do sistema.

- Após a implementação da segurança da informação houve uma redução de erros dos utilizadores com a utilização do SI, verificou-se isso porque as mensagens de erro são claras e ajudam o utilizador a corrigir ou ultrapassá-los.

- Os utilizadores têm grande confiança no SI. Essa relação tem lugar, porque de acordo com os utilizadores o sistema é fácil de usar, é rápido de se trabalhar, aumenta a produtividade do utilizador, proporciona ao utilizador alcançar os objetivos estabelecidos, trabalhar com o SI dá satisfação e reduz os erros ao trabalhar no SI.

6.2 Perspetivas de trabalho futuro

O âmbito desta dissertação concernente aos objetivos específicos foi analisar os impactos decorrentes da implementação da Segurança da Informação na usabilidade dos SI.

Relativamente a perspetivas de trabalho futuro, cogitam-se três cenários:

1º O interesse em realizar o estudo de caso em mais organizações com vários tipos de negócios;

2º Alargar âmbito dos objetivos específicos fazendo a análise dos impactos financeiros e do retorno de investimento sobre a segurança da informação.

Com a importância da informação nas organizações e a evolução dos SI, a gestão da segurança da informação vem se tornando uma área essencial para todos os tipos de organizações e é um fator crítico totalmente ligado ao cumprimento dos seus objetivos de negócio.

É certo que todas as ações realizadas nas organizações visam a obtenção de um retorno positivo. Esse retorno pode ser financeiro ou não. Um incidente relacionado à informação na organização poderá comprometer a qualidade dos seus serviços e gerar impactos financeiros, operacionais e de imagem.

A indisponibilidade de um SI, a perda de informações internas por falha técnica, uso inadequado do sistema ou catástrofe naturais, são situações de incidentes de segurança da informação que podem gerar perda de negócios (impacto financeiro), insatisfação dos clientes (impacto na imagem da empresa) ou atraso na execução dos processos de negócio (impacto operacional). Proceder à avaliação de tais impactos afigura-se de grande interesse.

3º Pretende-se também fazer uma revisão dos vários métodos de segurança da informação que são utilizados, avaliar as questões de usabilidade e organizá-las. A intenção é fazer uma chamada de atenção para a necessidade de análises sistemáticas de usabilidade e para o desenvolvimento de métricas de usabilidade para segurança da informação, estabelecendo quais métodos de segurança da informação são melhores de usar, para quais pessoas e para quais trabalhos, e melhorar a usabilidade de métodos de segurança existentes;

Os resultados da pesquisa sobre a usabilidade e métodos de segurança devem estar voltados para dois objetivos, a saber: 1) Aumento a disposição dos utilizadores para usar o método; e 2) Certificar-se de que os utilizadores que optam por usar o método de segurança podem fazê-lo com maior facilidade, menos tempo, menos erros, e maior satisfação do que seria possível de outra maneira.

Referencias Bibliográficas

Abreu, T., Mota, L., & Araújo, M. (2010). Métricas de Software - Como utilizá-las no gerenciamento de projetos de software. *Engenharia de Software Magazine*, 21:50-55.

Ainin, S., Bahri, S., & Ahmad, A. (2012). Evaluating portal performance - A study of the National Higher Education Fund (PTPTN) Corporation portal. *Telematics and Informatics*, 3:314-323.

Al-Debei, M., Jalal, D., & Al-Lozi, E. (2013). Measuring web portals success: a respecification and validation of the DeLone and McLean information systems success model. *International Journal of Business Information Systems*, 1:96-133.

Alaboodi, S. S., (2006). A New Approach for Assessing the Maturity of Information Security. *Information Systems Control Journal*, 3:36-46.

Albrechtsen, E. (2007). A Qualitative Study Of User´s View On Information Security. *Computers & Security*, 4: 276-289.

Albrechtsen, E., & Hovden, J., (2010). Improving Information Security Awareness and Behaviour Through Dialogue, Participation and Collective Reflection. *Computer & Security*, 29:432-445.

Alter, S. (1999). A general, yet useful theory of information systems. *Communications of the AIS*, 13:1-68.

Amaral, L. (1994). *PRAXIS - Um Referencial para o Planeamento de Sistemas de informação*. (Tese de Doutoramento) Braga: Universidade do Minho.

Anderson, E. & Choobineh, J., (2008). Enterprise information security strategies. *Computers & Security*, 1:22-29.

Anderson, J. M., (2003). Why We Need a New Definition of Information Security. *Computers & Security*, 308-313.

Anunciação, P., & Zorrinho, C. (2006). *Urbanismo Organizacional – Como gerir o choque tecnológico nas empresas.* Lisboa: Edições Sílabo.

AT. (2016). *Angola Telecom*. Disponível: em 18 de Outubro de 2016, em: http://www.angolatelecom.com/AngolaTelecom/PT

Au, N., Ngai, E., W., & Cheng, T. (2008). Extending the Understanding of End User Information Systems Satisfaction Formation: An Equitable Needs Fulfillment Model Approach. *MIS Quarterly*, 1:43-66.

Aytes, K., & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational and End User Computing*, 3:22-40.

Badre, A., (2002). *Shaping Web Usability: Interaction Design in Context*, Boston: Addison-Wesley Publishing.

Baecker, R. & Buxton, W. (1987). *Readings in Human-Computer Interaction.* Los Altos, CA: Morgan Kaufmann.

Bailey, J., & Pearson, S. (1983). Development of a Tool for Measuring e Analyzing Computer User Satisfaction. *Management Science*, 5:530-545.

Barbosa, S., & Silva, B. (2010). *Interação Humano-Computador.* Rio de Janeiro: Campus-Elsevier.

Baroudi, J., & Orlikowski, W. (1988). A Short Form Measure of User Information Satisfaction: A Psychometric Evaluation and Notes on Use. *Journal of Management Information Systems*, 4:44-59.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, 3:253-264.

Bretschneider, S., & D. Wittmer, D. (1993). Organizational Adoption of Microcomputer Technology: The Role of Sector. *Information Systems Research,* 1:88-108.

Brotby, W. (2009). *Information security management metrics: a definitive guide to effective security monitoring and measurement*. Saxony: Auerbach Publications.

Calder, A., Watkins, S., (2008). *IT Governance : A Manager's Guide to Data Security and ISO 27001/ ISO 27002*. 4. ed. Philadelphia: Kogan Page.

Carroll, J. (2009). Human Computer Interaction. In: Soegaard, M. & Friis, R. (Ed.). *The Encyclopedia of Human-Computer Interaction.* Aarhus: The Interaction Design Foundation.

Carroll, J. (2013). Human Computer Interaction. In: Soegaard, M. & Friis, R. (Ed.). *The Encyclopedia of Human-Computer Interaction.* 2nd ed. Aarhus, Denmark: the Interaction Design Foundation.

Cassarro, A. (2011). *Sistemas de informações para tomada de decisões*. 4 ed. São Paulo: Cengage Learning.

Castells, M. (2003). *A Galáxia da Internet: Reflexões sobre a Internet, os negócios e a sociedade*. Rio de Janeiro: Jorge Zahar Editor.

Chapin, D., & Akridge, S. (2005). How Can Security Be Measured? *Information System Control Journal*. Salem: ISACA, 2:43-47.

Chew, E., Swanson, M., Stine, K., & Bartol, N. (2008). Performance Measurement Guide for Information Security. *National Institute of Standards and Technology (NIST).* Technical Report Special Publication, 55:1-80.

Chin, D., Goff, S., Webster, T., Smith, T., & Goldberg, A. (1988). Sequence of the lon gene in Escherichia coli.A heat-shock gene which encodes the ATP-dependent protease. *J.Biol.Chem,* 263:11718-11728.

Chin, W., & Lee, W. (2002). Matthew K.O. A Proposed Model and Measurement Instrument for the Formation of IS Satisfaction: The Case of End-User Computing Satisfaction. *Association for Information System,* 553-563.

Clarke, R. & Knake, R. (2015). *Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito.* Rio de Janeiro: Brasport.

Cockton, G. (2012). Usability Evaluation. In Soegaard, M. & Friis, R. (Ed.), *Encyclopedia of Human-Computer Interaction.* Aarhus: The Interaction Design Foundation.

Corby, M. J., (2002). Security Is All About Business, Not Technology. *Information Systems Security*, 6:10-13.

Cybis, W. (2003). Engenharia de Usabilidade: uma abordagem ergonômica. *Laboratório de utilizabilidade de informática Universidade Federal de Santa Catarina.* Florianópolis, 13:1-10.

Davenport, T. & Prusak, L. (1998) *Conhecimento empresarial: como as organizações gerenciam o seu capital intelectual*. Rio de Janeiro: Campus.

Delone, W., & Mclean, E. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research*, 1:60-95.

Delone, W., & Mclean, E. (2003). The DeLone and McLean model of information system success: a ten year update. *Journal of Management Information Systems*, 4:9-30.

Denis, T., Trobec, R., Pavesic, N.& Tasic, J. F., (2007). Information Systems Security and Human Behavior. *Behaviour & Information Technology,* 2:113-118.

Dias, C. (2003). *Usabilidade na web: criando portais mais acessíveis*. Rio de Janeiro: Ata Books.

Dhillon, G., & Backhouse, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM*, 7:125-128

Doll, W.J. & Torkzadeh, G. (1988). The measurement of end-user computing satisfaction. *MIS Quarterly*, 2:259-274.

Drucker, P (1993). Sociedade Pós-Capitalista. Difusão Cultural. Lisboa.

Eloff, J. & Eloff, M. (2003). Information security management: a new paradigm. In*: Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology*. Pretoria: South African.

Eloff, M. & Von Solms, S. (2000). Information security management: a hierarchical framework for various approaches. *Computers & Security*, 3:243-256.

Fernandes, J., & Souza, R. (2016). Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais. *Brazilian Journal of Information Science*, 1:63-75

Ferreira, F. & Araújo, M. (2006). *Política de Segurança da Informação: Guia Prático para Implementação e Elaboração*. Rio de Janeiro: Editora Ciência Moderna Lda.

Flechais, I. (2005). *Designing secure and usable system*. (Tese de Doutoramento). University College London.

Fleming, S. (2007). Implicit Trust Can Lead To Data Loss. *Information Systems Security*, 16:109-113.

Fortin, M. (2009). *Fundamentos e etapas do processo de investigação*. Loures: Lusodidacta.

Freixo, M. (2010). *Metodologia Científica: Fundamentos Métodos e Técnicas.* 2ª edição. Lisboa: Instituto Piaget.

Friedman, C. & Wyatt, J. (2006). *Evaluation Methods in Biomedical Informatics*. 2ª ed. New York: Springer.

Gaivéo, J. (2008). *As Pessoas nos Sistemas de Gestão da Segurança da Informação*. (Tese de Doutoramento) Universidade Aberta, Lisboa.

Galitz, W. (2002) *The essential guide to user interface design: An introduction to GUI design principles and techniques.* 2ª. ed. New York: John Wiley & Sons.

Galliers, R., & Baets, W. (1997). *Information Technology and organizational Transformation: Innovation for the 21 st Century Organization*. John Wiley & Sons

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, 2:41-73.

Green, D., & Pearson, J. (2009). The Examination of Two Web Site Usability Instruments for The Use in B2c E-Commerce Organization. *Journal of Computer Information Systems*, 4:19-32.

Guo, K., Yuan, Y., Archer, N., & Connelly, C. (2011). Understanding Nonmalicious Security Violations in the Workplace. *Journal of Management Information Systems*, 2:203-236.

Heckel, P. (1991). *Software Amigável: Técnicas de Projeto para uma melhor Interface com o Usuário*. Rio de Janeiro: Editora Campus.

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems*, 4:373-385.

Hetzel, B. (1993*). Making Software Measurement Work: Building an Effective Measurement Program*. USA. John Wiley and Sons: LTD.

Holgate, J. A., Williams, S. P., & Hardy, C. A. (2012). Information Security Governance: Investigating Diversity in Critical Infrastructure Organizations. *Proceedings of Bled eConference.* Bled, Slovenia.

Hughes, J., Van Dam, A., Morgan, M., Sklar, D., Foley, J., Feiner, S., & Akeley, K. (2014). *Computer graphics, principles and practice* (3rd ed). New Jersey: Pearson Education, Inc.

ISO/IEC (2014). *ISO/IEC 27000 - Information security management systems - Overview and vocabulary*. International Standard Organization.

ISO/IEC (2013). *ISO/IEC 27001 - Information technology – Security techniques – Information Security Management Systems - Requirements*. International Standard Organization.

ISO/IEC (2010). *ISO/IEC 27003 - Information technology - Security techniques - Information security management system implementation guidance*. International Standard Organization.

ISO/IEC (2008). *ISO/IEC 27005 - Information technology - Security techniques - Information security risk management.* International Standard Organization.

ISO 9241-11 (1998). *International Standards. Ergonomic requirements for office work with visual display terminals (VDTs)* - Part 11 : Guidance on usability. First Edition.

Ives, B., Olson, M. and Baroudi, S. (1983). The measurement of user information satisfaction. *Communications of the ACM*, 10:785-793.

Jansen, W. (2009). *Directions in security metrics research. Technical report*. National Institute of Standards and Technology Interagency Report. NISTIR 7564.

Jones, S. (2014, 5 de Junho). Kremlin alleged to wage cyber warfare on Kiev. *Financial Times*, 5.

Jonhson, R. (2011). *Security Policies and Implementation Issues*. Sudbery: World Headquarters.

Kainda, R., Flechais, I., & Roscoe, A. (2010). Security and Usability: Analysis and Evaluation. In ARES (Eds.), *Fifth International Conference on Availability, Reliability and Security*, (pp. 275-282). Polónia: IEEE Computer Society.

Karjalainen, M. & Siponen, M. (2011). Toward a New Meta-Theory For Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems*, 8:518-555.

Kendall, K., & Kendall, J. (1991) *Análisis y diseño de sistemas*. México : Prentice-Hall, 1991.

Khauaja, D., & Campomar, M. (2007). O Sistema de Informações no Planejamento de Marketing: em busca de vantagem competitiva. *Revista de Gestão da Tecnologia e Sistemas de Informação***,** 1:23-46.

Kim, D., & Solomon, M. (2012). *Fundamentals of Information Systems Security*. Sudbury: World Headquarters.

Kovacich, G., & Halibozek, E. (2006). *Security Metrics Management: How to Manage the Costs of an Assets Protection Program.* Burlington, MA: Elsevier Butterworth-Heinemann.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, Vol. 27, 5-6:224-231.

Lececerof, A., & Paterno, F. (1998). Automatic support for usability evaluation *IEEE Transactions on Software Engineering*, 10:863-888.

Laudon, J., & Laudon, K. (2007). *Sistemas de informações gerenciais.* 7a edição. São Paulo: Pearson Prentice Hall.

Laudon, K. & Laudon, J. (2000). *Management Information Systems -Organization and Technology in the Networked Enterprise* 6th ed. New Jersey: Prentice - Hall, Inc.

Laudon, K. & Laudon, J. (2004). *Sistemas de Informação Gerenciais: Administrando a empresa digital.* São Paulo: Prentice Hall.

Laudon, K. & Laudon, J. (2012). *Management Information Systems: Managing the Digital Firm.* 12th Ed., Upper Saddle River - New Jersey: Pearson Education Inc.

Lee, Y., & Kozar, K. (2012). Understanding of Website Usability: Specifying and Measuring Constructs and Their Relationships. *Decision Support Systems,* 1:450-463.

Lopes, F., Morais, M., & Carvalho, A. (2005). *Desenvolvimento de Sistemas de Informação.* Lisboa: FCA - Editora de Informática.

Lopes, M. (2009). Redes, tecnologia e desenvolvimento territorial. *Congresso de Desenvolvimento Regional de Cabo Verde: Redes de Desenvolvimento Regional.* Cabo Verde.

Lowdermilk, T. (2013). *Design Centrado no Usuário: um guia para o desenvolvimento de aplicativos amigáveis*. São Paulo: Novatec.

Macedo, P., Zacarias, M., & Tribolet, J. (2005). Técnicas e métodos de investigação em Engenharia Organizacional: Projecto de Investigação em Modelação de Processos de Produção. *6ª Conferência da Associação Portuguesa de Sistemas de Informação.* Portugal.

Mamede, H. S. (2006). *Segurança Informática nas Organizações.* Lisboa: FCA - Editora de Informática.

Mandarini, M. (2004). *Segurança Corporativa Estratégica.* São Paulo: Manole.

Martins, J. (2003). *Gestão de Projetos de Segurança da Informação*. Rio de Janeiro: Brasport.

Mazzotti, A. (2006). Usos e Abusos dos Estudos de Caso. *Cadernos de pesquisa*, 129: 637-651.

Mcgarry, K. (1999). *O contexto dinâmico da informação*. Brasília: Briquet de Lemos.

Mello, L., Vasconcellos, L., Bragança, L., & Motta, O. (2010). Contribuição para Gestão de Ativos Intangíveis Organizacionais: Proposição de Um Modelo Baseado no Balenced Scorecard. *VI Congresso Nacional de Excelência em Gestão – CNEG*. Niterói - Brasil.

Meyer, J., Stanley, D., Herscovitch, L., & Topolnytsky, L. (2002). Affective, Continuance and Normative Commitment to the Organization: A Meta-analysis of Antecedents, Correlates, and Consequences. *Journal of Vocational Behavior*, 20-52.

Minayo, M. (2005). *Avaliação por triangulação de métodos: abordagem de programas sociais*. Rio de Janeiro: Fiocruz.

Moraes, A. (2013). Ergonomia, ergodesign e usabilidade: algumas histórias, precursores: divergências e convergências. *Ergodesign & HCI*, 1:1-9.

Moran, T. (1981). The Command Language Grammars: a represetantion for the user interface of interactive computer systems. *International Journal of ManMachine Studies*, 1:3-50.

Morville, P. (2014) *Intertwingled: Information Changes Everything*. Michingan: Semantic Studios.

Ng, B-Y., Kankanhalli, A., Xu, Y. (2009). Studying Users Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems*, 4:815-825.

Nielsen, J. (1993). *Usability Engineering*. San Francisco: Morgan Kaufmann – Academic Press.

Nielsen, J. (1994). Heuristic Evaluation. In Mack, R. & Nielsen, J. (Eds.) *Usability Inspection Methods* New York: John Wiley & Sons. 2:25-62.

Nielsen, J. (2000). *Designing Web Usability*. Indianapolis: New Riders

Nielsen, J. &. (2006). *Prioritizing Web Usability*. Indiana: New Riders.

Nielsen, J., & Loranger, H. (2007). *Usabilidade na web* (1ª ed). São Paulo: Editora Campus.

Nielsen, J. (2012). Usability 101: Introduction to Usability. *Nielsen Norman Group.* Disponível em: 05 de Outubro de 2016, em: *https://www.nngroup.com/articles/usability-101-introduction-to-usability/*

Norman, D., & Draper, S. W. (Eds.). (1986). *User centred system design*. Hillsdale, New Jersey: Erlbaum.

Norman, D. (2013). *The design of everyday things.* New York: Basic Books.

Nuckles, B. (2014). Android vs. iOS vs. Windows Phone: Which is Best for Business? B*usiness News Daily*. Disponível em: 20 de dezembro de 2016 em: http://www.businessnewsdaily.com/5759-android-vs-ios-vs-windows-phone-small-business.html#sthash.RPpSktVX.dpuf

Payne, S. (2006). A Guide to Security Metrics. *SANS Institute, Inc*., 1:1-11.

Pearrow, M. (2007). *Web Usability HandBook*. Boston, Massachusetts: Charles River Media.

Pereira, S. & Paiva, P. (2011). A importância da Engenharia da Usabilidade para a Segurança de Sistemas Informatizados em Saúde. *Journal Health Informatics,* 3:123-129.

Petter, S., Delone, W. & Mclean, E. (2008). Measuring information systems success: models, dimensions, measures and interrelationships. *European Journal of Information Systems*, 17:236-263.

Pfleeger, C. & Pfleeger, S. (2003). *Security in Computing*. 3rd ed. New Jersey: Pearson Education, Inc.

Preece, J., Rogers, Y., & Sharp, H. (2005) *Design de interação: além da interação homem-computador*. Porto Alegre, RS: Bookman.

Pressman, R. (2006). Engenharia de Software. McGraw-Hill, 6ª edição.

Pressman, R. (2011). Engenharia de Software: Uma abordagem profissional. 7ª ed. Bookman.

Qi, J., Xu L., Shu, H., & Li, H. (2006). Knowledge management in OSS: an enterprise information system for the telecommunications industry. *Systems Research and Behavioral Science*, 2: 177- 190.

Ramos, Isabel. (2000). *Aplicações das Tecnologias de Informação que suportam as Dimensões Estrutural, Social, Política, Simbólica do Trabalho*. (Tese de Doutorado) em Tecnologias e Sistemas de Informação - Universidade do Minho, Guimarães.

Rascão, J. (2004). *Sistemas de Informação para as organizações: A informação chave para a Tomada de Decisão*. Lisboa: Edições Sílabo.

Ravden, S.; Johnson, G. (1989). *Evaluating usability of human-computer interfaces.* Chichester: Ellis Horwood.

Reddick, C. (2010). *Homeland Security Preparedness and Information Systems: Strategies for Managing Public Policy*. New York: IGI Global.

Rezende, D., & Abreu, A. (2000). *Tecnologia da informação aplicada a sistemas de informação empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas*. São Paulo: Atlas.

Rhee, H., Kim, C., & Ryu, Y. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 8:816-826.

Rogers, Y., Sharp, H., & Preece, J. (2013) *Design de interação: além da interação homem-computador*. Porto Alegre, RS: Bookman.

Rubin, J., & Chisnell, D. (2008). *Handbook of Usability Testing - How to Plan, Design, and Conduct Effective Tests*. 2nd Ed. New Jersey: Wiley Publishing, Inc.

Scott, W. (2004). Institutional theory. In George Ritzer (Eds), *Encyclopedia of Social Theory*, (pp. 408-414). Thousand Oaks: Sage.

Serrano, A., Caldeira, M., & Guerreiro, A. (2004). *Gestão de Sistemas e Tecnologias de Informação*. Lisboa: FCA.

Sharma, M., Bai, Y., Chung, S., Dai, L. (2012). Using Risk in Access Control for Cloud-Assisted eHealth. *International Conference on High Performance Computing and Communications,* Liverpool – England.

Sheldon, J. (2011). Deciphering Cyberpower Strategic Purpose in Peace and War. *Strategic Studies Quarterly*, 5:95-112.

Siponen, M., Mahmood, A. & Pahnila, S. (2009). Are Employees Putting Your Company at Risk by Not Following Information Security Policies? *Communications of the ACM*. Vol. 52, 12:145-147.

Siqueira, M. (2005). *Gestão estratégica da informação*. Rio de Janeiro: Brasport.

Spears, J., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly, Minneapolis*, 3:503-522.

Stafford, L., e Hillyer, J. (2012). Information and communication technologies in personal relationships. *Review of Communication*, 4:290-312.

Starec, C., Gomes, E., & Chaves, J. (2006). *Gestão Estratégica da Informação e Inteligência Competitiva*. São Paulo: Saraiva.

Swanson, M., Bartol, N., Sabato, J., Hash, J., & Graffo, L. (2003). Security Metrics Guide for Information Technology Systems U.S. Department of Commerce: *National Institute of Standards and Technology*, 1:1-28.

Te'eni, D., Carey, J., & Zhang, P. (2007). *Human Computer Interaction: Developing Effective Organizational Information Systems*. Hoboken: John Wiley & Sons.

Tillery, S. (2010). How Safe Is The Cloud? *Baseline Magazine*, 106:15-15.

Torkzadeh, G., & Doll, W. (1999). The development of a tool measuring the perceived impact of information technology on work. *Omega - the international journal of management science*, 327-339.

Verendel, V. (2009). Quantified security is a weak hypothesis. *Proceedings of the 2009 workshop on new security paradigms workshop - NSPW*, 37-50.

Ward, J., & Griffiths, P. (1996*) Strategic Planning for Information Systems*. Chichester: John Wiley & Sons.

Whitten, A. (2004). *Making Security Usable*. (Tese de Doutoramento). Carnegie Mellon University, Pittsburgh.

Wu, J., & Wang, Y. (2006). Measuring KMS success: a respecification of the DeLone and McLean´s model. *Information and Management*, 6:728-739.

Yee, K. (2004). Aligning Security and Usability. *IEEE Security & Privacy*, 5:48-55.

Yin, R. (1994). *Case Study Research: Design and Methods*. Volume 5. Califórnia: SAGE.

Yin, R. (2005). *Estudo de Caso. Planejamento e Métodos*. Porto Alegre: Bookman.

Yin, R. (2009). *Case Study Research: Design and Methods*. California: SAGE Publication, Inc.

Zancheta, F. A. (2004). *Usabilidade e a ciberfobia dos usuários de sistemas computacionais de chão de fábrica.* Tese (Tese de Mestrado em Engenharia da Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, São Paulo.

Zorrinho, C. (1991). *Gestão da Informação*. Lisboa: Editorial Presença.

Zorrinho, C. (1995). *Gestão da Informação: condição para vencer*. Lisboa: Instituto de Apoio às Pequenas e Médias Empresas (IAPMEI).

Zúquete, A. 2008 *Segurança em redes informáticas*. Lisboa: FCA - Editora de Informática.

ANEXOS

ANEXO A – Questionário Gestores

Este anexo contém o questionário elaborado para os gestores de topo, com a finalidade de obter informações sobre as alterações verificadas na organização com a implementação do SGSI, na perspetiva da gestão.

Fazem parte dos inquiridos o pessoal da Administração Geral, os Órgãos de Assessoria e Apoio (Gabinete do Conselho de Administração, Gabinete Jurídico, Gabinete de Relações Institucionais, Gabinete de Auditoria Interna, Gabinete de Comunicação e Imagem e Gabinete de Planeamento Controlo e Gestão.

Questionário (Gestores) - Impactos da implementação da Segurança da Informação na usabilidade dos SI

Este questionário encontra-se estruturado em 4 grupos de questões. O grupo A destina-se a caracterizar o(a) inquirido(a) e os grupos B, C e D representam os objetivos específicos da dissertação.

Todas as informações fornecidas para o questionário serão tratadas de forma confidencial. De forma a garantir a confidencialidade e o anonimato dos(as) inquiridos(as), agradeço que em nenhuma parte do questionário coloque qualquer nome ou número que o identifique.

Por favor, leia atentamente as instruções e as questões e assinale a resposta que melhor reflecte a sua opinião.
Agradecemos sua colaboração,
Atenciosamente,
Manuel Sequesseque - Mestrando em Sistemas de Informação Organizacionais
José Manuel Gaivéo - Orientador

Nota: Tempo estimado de resposta: 10 minutos

*Obrigatório

A - Identificação/Caracterização do(a) inquirido(a)

A1 - Sexo

- ◯ Feminino
- ◯ Masculino

A2 - Escalão etário

- ◯ Menos de 30 anos
- ◯ Entre 30 a 45 anos
- ◯ Mais de 45 anos

A3 - Habilitações literárias

- ◯ Secundário (Ensino médio)
- ◯ Licenciatura
- ◯ Mestrado/Doutoramento

A4 - Indique a área da estrutura orgânica de gestão onde presta serviço. *

- ◯ Administração
- ◯ Orgãos de Assessoria e Apoio
- ◯ Direção Executiva de Operações

A5 - Há quanto tempo exerce funções?

- ◯ Menos de 1 ano

7

- ◯ De 1 a 5 anos
- ◯ Mais de 5 anos

B - Realizar tarefas no Sistema de Informação (SI).

SI é o conjunto constituído por pessoas, procedimentos, dados/informação e componentes TIC (hardware, software e comunicações) que recolhe, processa, armazena, analisa e distribui informação de forma adequada em função dos objetivos da organização.

B1 - Recebeu formação na utilização do SI? *
Se respondeu NÃO, passe para a questão B4

- ◯ Sim
- ◯ Não

B2 - Com que frequência recebe formação necessária à utilização do SI?

- ◯ Uma única vez
- ◯ Sempre que existem mudanças no SI
- ◯ Trimestralmente
- ◯ Semestralmente
- ◯ Anualmente
- ◯ Outro: _____

B3 - Classifique o grau de relevância dessa(s) formação(ões).

	1	2	3	4	5	6	
Pouco relevante	◯	◯	◯	◯	◯	◯	Muito relevante

B4 - Existe algum(uns) documento(s) acerca da utilização do SI?
Se respondeu NÃO, passe para a questão B7

- ◯ Sim
- ◯ Não

B5 - Como tomou conhecimento desse(s) documento(s)?
(Assinale todos os itens aplicáveis)

- ☐ Consta no contrato de trabalho
- ☐ Documento entregue na Organização
- ☐ Informação dos serviços de informática
- ☐ Informação afixada na Organização
- ☐ Colega
- ☐ Outro: _____

B6 - Classifique o grau de utilidade desse(s) documento(s).

	1	2	3	4	5	6	
Pouco Útil	◯	◯	◯	◯	◯	◯	Muito Útil

B7 - Com que frequência acede ao SI?

- ○ Todos os dias
- ○ Quase todos os dias
- ○ Pelo menos uma vez por semana
- ○ Pelo menos uma vez a cada duas semanas
- ○ Pelo menos uma vez por mês
- ○ Outro:

B8 - Qual é o tempo médio diário de utilização do SI?

- ○ Até 1 hora
- ○ Entre 1 e 3 horas
- ○ Entre 3 e 5 horas
- ○ Mais de 5 horas

B9 - Como caracteriza a sua utilização ao SI? *

As tarefas que realiza quando utiliza o SI. (Assinale todos os itens aplicáveis)

- ☐ Administração
- ☐ Manutenção do sistema
- ☐ Monitorização do sistema
- ☐ Inserção, modificação ou eliminação de dados
- ☐ Consulta de dados (acesso só de leitura)
- ☐ Elaboração de relatórios
- ☐ Envio/receção de emails
- ☐ Análise estatística
- ☐ Pesquisa na Internet
- ☐ Impressão de documentos
- ☐ Outro:

B10 - Classifique o seu grau de facilidade em executar tarefas no SI.

Considere quão à vontade ou ágil é a realizar tarefas quando utiliza o SI.

	1	2	3	4	5	6	
Muito difícil	○	○	○	○	○	○	Muito fácil

B11 - Indique o seu grau de desempenho ao executar tarefas no SI.

Considere se consegue cumprir na íntegra as tarefas que realiza no SI.

	1	2	3	4	5	6	
Baixo desempenho	○	○	○	○	○	○	Elevado desempenho

B12 - Indique o quão rápido é executar tarefas no SI.

Classifique a velocidade de realizar tarefas no SI.

	1	2	3	4	5	6	
Muito lento	○	○	○	○	○	○	Muito rápido

B13 - Classifique o SI quanto a prevenção de erros.

O SI prevê as situações em que o utilizador está prestes a cometer erro?

	1	2	3	4	5	6	
Baixo desempenho	○	○	○	○	○	○	Elevado desempenho

B14 - O utilizador é avisado pelo SI se está a cometer um erro grave.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B15 - O SI ajuda o utilizador a reconhecer, diagnosticar e recuperar dos erros.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B16 - O utilizador é informado da necessidade de plug-ins e são fornecidas instruções de como os instalar.

Um plug-in é uma aplicação que, num programa informático, acresce uma funcionalidade adicional ou uma nova característica ao software. Em português, por conseguinte, pode designar-se plug-in como um complemento.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B17 - As imagens são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B18 - As aplicações são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B19 - Os elementos áudio são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B20 - Os elementos vídeo são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6

Discordo ○ ○ ○ ○ ○ ○ Concordo

C- Segurança da Informação no SI

Segurança da informação trata da preservação da confidencialidade, integridade e disponibilidade dos dados armazenados nos SI (ISO/IEC 27001:2013).
Por Sistema de Gestão de Políticas Segurança da Informação entende-se ao conjunto de processos e procedimentos, baseado em normas e na legislação, que uma organização implementa para prover segurança no uso de seus ativos tecnológicos.

C1 - Desde a sua entrada na Organização foi feita alguma implementação de um sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI?
Se respondeu NÃO ou NÃO SABE, passe para a questão C16

- ○ Sim
- ○ Não
- ○ Não sabe

C2 - Como tomou conhecimento da implementação do sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI?
(Assinale todos os itens aplicáveis)

- ☐ Consta no contrato de trabalho
- ☐ Documento entregue na Organização
- ☐ Informação dos serviços de informática
- ☐ Informação afixada na Organização
- ☐ Colega
- ☐ Outro: _____

C3 - Participou na implementação desse sistema de gestão de políticas (normas/regulamentos/regras/procedimentos)?
Se respondeu NÃO, passe para a questão C6

- ○ Sim
- ○ Não

C4 - Caracterize a sua participação na implementação do sistema.
(Assinale todos os itens aplicáveis)

- ☐ Instalação de Software
- ☐ Instalação de Hardware
- ☐ Elaboração das políticas
- ☐ Projeção do sistema
- ☐ Implementação do sistema
- ☐ Análise de documentos
- ☐ Levantamento de requisitos
- ☐ Preenchimento de questionários
- ☐ Resposta a entrevistas
- ☐ Outro: _____

C5 - Classifique o seu grau de participação na implementação do sistema.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C6 - Classifique a sua perceção acerca do funcionamento do SI depois da implementação do sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança.

	1	2	3	4	5	6	
Baixa	○	○	○	○	○	○	Elevada

C7 - Classifique o seu grau de satisfação com implementação do sistema.

	1	2	3	4	5	6	
Pouco satisfeito	○	○	○	○	○	○	Muito satisfeito

C8 - As políticas (normas/regulamentos/regras/procedimentos) de segurança do SI têm sido atualizadas?
Se respondeu NÃO ou NÃO SABE, passe para a questão C12

- ○ Sim
- ○ Não
- ○ Não sabe

C9 - Com que frequência as políticas (normas/regulamentos/regras/procedimentos) de segurança do SI têm sido atualizadas?

- ○ Mensalmente
- ○ Trimestralmente
- ○ Semestralmente
- ○ Anualmente
- ○ Outro: _____

C10 - Participou de alguma atualização dessas políticas?
Se respondeu NÃO passe para a questão C12

- ○ Sim
- ○ Não

C11- Caracterize a sua participação na atualização das políticas.
(Assinale todos os itens aplicáveis)

- ☐ Planeamento das políticas
- ☐ Implementação das políticas
- ☐ Análise de documentos
- ☐ Levantamento de requisitos
- ☐ Preenchimento de questionários
- ☐ Resposta a entrevistas
- ☐ Outro: _____

C12 - Como era gerida a segurança da informação antes do sistema?
(Assinale todos os itens aplicáveis)

- ☐ Arquivos trancados fisicamente
- ☐ Implementação das políticas
- ☐ Conjunto utilizador-password
- ☐ Outro:

C13 - Quem fazia a gestão da segurança da informação antes do sistema?
(Assinale todos os itens aplicáveis)

- ☐ A gestão do topo
- ☐ O diretor
- ☐ O chefe do departamento
- ☐ O próprio funcionário
- ☐ O técnico da informática
- ☐ Outro:

C14 - Quais os principais problemas identificados na segurança antes da implementação do sistema?
(Assinale todos os itens aplicáveis)

- ☐ Perda de Confidencialidade
- ☐ Perda de Integridade
- ☐ Perda de Disponibilidade
- ☐ Outro:

C15 - Quais os principais aspetos positivos identificados na segurança antes da implementação do sistema?
(Assinale todos os itens aplicáveis)

- ☐ Autonomia
- ☐ Não ingerência
- ☐ Rapidez na execução de tarefas
- ☐ Responsabilidade para decidir sobre a segurança
- ☐ Outro:

C16 - Na sua opinião, qual é a importância que a segurança da informação tem no funcionamento da instituição e das suas atividades diárias no SI?

- ○ Critica (muito importante)
- ○ Importante
- ○ Auxiliar/Secundária
- ○ Não é importante
- ○ Não sabe / Não tem a certeza

C17- Na sua opinião, quais os maiores impedimentos para a segurança da informação?
(Assinale todos os itens aplicáveis)

- ☐ Restrições orçamentais.
- ☐ Falta de compreensão das ameaças.

- [ ] Falta de processos e procedimentos formais de segurança.
- [ ] Falta de envolvimento dos órgãos de gestão.
- [ ] Falta de sensibilização para as ameaças.
- [ ] Falta de formação para a segurança do SI.
- [ ] Problemas de performance das ferramentas de segurança.
- [ ] Inaptidão para cumprir os regulamentos.
- [ ] Não sabe
- [ ] Outro:

C18 - Na sua opinião quais as razões que justificaram/justificariam a necessidade de implementação de sistema de segurança da informação?

(assinale todos os itens aplicáveis)

- [ ] Importância do SI para a Organização
- [ ] Necessidade constante de acesso à informação, sendo necessário garantir a sua disponibilidade
- [ ] Legislação
- [ ] Dependência que as aplicações e sistemas têm da segurança
- [ ] Necessidade de garantir que as informações não são indevidamente alteradas, danificadas ou eliminadas
- [ ] Aumento das ameaças
- [ ] Outro:

C19- Sem um sistema de segurança da informação a organização consegue saber o que deve ser protegido?

Se respondeu NÃO ou NÃO SABE, passe para a questão C21

- ◯ Sim
- ◯ Não
- ◯ Não sabe

C20- O que a segurança da informação deve proteger?

- ◯ Ativos da organização de forma geral (proteger Pessoas, Hardware, Software e Informação)
- ◯ Segurança da TIC (proteger, as aplicações, as base de dados e os sistemas operativos).
- ◯ A Segurança da Informação (proteger a informação crítica de negócio nos seus vários suportes.
- ◯ Outro:

C21- Sem um sistema de segurança da informação a organização consegue saber contra o que será necessário proteger?

Se respondeu NÃO ou NÃO SABE, passe para a questão C23

- ◯ Sim
- ◯ Não
- ◯ Não sabe

C22- Contra o que protege um sistema de segurança da informação? (Assinale todos os itens aplicáveis)

Ameaça – potencial causa de um incidente inesperado que pode resultar em danos para um sistema ou organização. Vulnerabilidade – fraqueza, de um activo ou controlo, que pode ser explorada por uma ameaça.

- [ ] Catástrofes naturais (Inundações, terramotos, sismos, etc.)

- [ ] Ataques externos (eliminação, roubo, utilização indevida, etc.)
- [ ] Ataques internos (eliminação, roubo, utilização indevida, etc.)
- [ ] Vulnerabilidades/falhas nas instalações.
- [ ] Vulnerabilidades/falhas na TIC.
- [ ] Vulnerabilidades/falhas inerentes aos erros humanos.
- [ ] Outro:

C23 - Já teve conhecimento de alguma(s) violação(ções) à segurança do SI da organização?
(por exemplo destruição/roubo de equipamentos, utilização não autorizada de ficheiros de outras pessoas, entradas em locais interdito). Se respondeu NÃO, passe para a questão C22

- ○ Sim
- ○ Não

C24 - Que atitude tomou quando presenciou essa(s) violação(ções)?
(Assinale todos os itens aplicáveis)

- [ ] Advertiu o(a) infrator(a)
- [ ] Comunicou à gestão
- [ ] Comunicou ao técnico de informática
- [ ] Propôs medidas de solução para o problema
- [ ] Comentou com os(as) seus(as) colegas
- [ ] Aplicou um processo disciplinar ao(à) infrator(a)
- [ ] Demitiu o(a) infrator(a)
- [ ] Nenhuma
- [ ] Outro:

C25- Quais considera terem sido as causas possíveis para as violações à segurança do SI?
(Assinale todos os itens aplicáveis)

- [ ] Ataque interno
- [ ] Ataque externo
- [ ] Vulnerabilidades conhecidas em produtos comerciais (ex.: Windows)
- [ ] Vulnerabilidades desconhecidas em produtos comerciais (ex.: Windows)
- [ ] Vírus e worms por email
- [ ] Aplicações ou serviços Web
- [ ] Engenharia social
- [ ] Erro humano
- [ ] Perda acidental de equipamentos
- [ ] Vírus ou outro código malicioso
- [ ] Abuso de privilégios pelos colaboradores de TI
- [ ] Procedimentos negligentes
- [ ] Não sabe a causa
- [ ] Não é aplicável
- [ ] Outro:

C26 - Existe um departamento, com responsabilidades definidas, para lidar estrategicamente com segurança da informação?

Se respondeu NÃO ou NÃO SABE, passe para a questão C28

- ○ Sim
- ○ Não
- ○ Não sabe

C27 - Qual é o departamento responsáveis pela estratégia da segurança da informação?
(Assinale todos os itens aplicáveis)

- ☐ A gestão de topo
- ☐ A direção
- ☐ O departamento de informática
- ☐ A chefia de cada departamento
- ☐ Não sabe
- ☐ Outro:

C28- Quais das seguintes tecnologias ou mecanismos estão implementadas no sistema da segurança?
(Assinale todos os itens aplicáveis)

- ☐ Antispyware
- ☐ Sistema de detenção de intrusão
- ☐ Controlo de acesso aos sistemas críticos da empresa;
- ☐ Análise da segurança das estações de trabalho, desktops e notebooks
- ☐ Análise da segurança física e lógica dos servidores de rede
- ☐ Análise da segurança contra contaminação por vírus
- ☐ Avaliação da configuração do firewall
- ☐ Criptografia de dados (e-mails e informações confidenciais)
- ☐ Análise da Política de Backup
- ☐ Análise da exigência de prevenção contra softwares não licenciados na empresa
- ☐ Plano de Contingência
- ☐ Análise da Política de Acesso dos funcionários à Internet
- ☐ Política de Instalação de Software nas estações e na rede;
- ☐ Processo de consciencialização de funcionários.

C29 - Classifique relativamente à segurança da informação do SI (6 para muito importante e 1 para pouco importante) os seguintes aspetos:

C29.1 - Classifique os Gestores.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C29.2 - Classifique os Utilizadores.

	1	2	3	4	5	6	

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.3 - Classifique os Técnicos de Informática.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.4 - Classifique os Computadores pessoais.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.5 - Classifique os Periféricos.

Por exemplo: Impressoras, Scanners, etc.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.6 - Classifique os Servidores.

Um servidor é um computador que faz parte de uma rede e que fornece serviços a outros computadores, que recebem o nome de clientes. Basicamente, é um computador mais potente do que um desktop comum. Ele foi desenvolvido especificamente para transmitir informações e fornecer produtos de software a outros computadores que estiverem conectados a ele por uma rede.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.7 - Classifique o(s) Software(s) aplicacional.

Por exemplo: Solução de CRM - Customer Relationship Management, SIG - Sistemas Integrado de Gestão e Solução de Gestão e ERP

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.8 - Classifique o(s) Sistema(s) Operativo(s).

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.9 - Classifique a(s) Base(s) de dados.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.10 - Classifique a Internet.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.11 - Classifique os Serviços na cloud.

Serviços na cloud refere-se à utilização da memória e da capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet, ou seja, é uma tecnologia que permite acesso remoto a programas (softwares), arquivos (documentos, músicas, jogos, fotos, vídeos) e serviços por meio da internet.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.12 - Classifique o Email.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.13 - Classifique a Rede interna.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C29.14 - Classifique o Sistema de telecomunicações.
(telefones, fax, etc.)

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

D- Avaliar a satisfação da utilização do SI

A norma ISO 9241-11 define usabilidade como a capacidade de um produto ser usado por utilizadores específicos para atingir objetivos específicos com eficácia, eficiência e satisfação num contexto específico de uso.
Considerando as práticas de segurança da informação, avalie o impacto delas na satisfação da utilização do SI.

D1- Indique o grau de satisfação com as políticas de segurança da informação. *

1 2 3 4 5 6

Pouco satisfeito ○ ○ ○ ○ ○ ○ Muito satisfeito

D2 - Satisfação com o SI enquanto software.

Reação ao software é a resposta do utilizador ao interagir com a interface do SI

D2.1 - Expetativa Visual.

Reação ao contacto visual com a interface

	1	2	3	4	5	6	
Horrível	○	○	○	○	○	○	Fantástico

D2.2 - Adaptação ao software.

Reação à habituação ao SI

	1	2	3	4	5	6	
Difícil	○	○	○	○	○	○	Fácil

D2.3 - Utilização do software.

Reação ao executar tarefas no SI

	1	2	3	4	5	6	
Frustrante	○	○	○	○	○	○	Satisfatório

D2.4 - Capacidade do software.

A capacidade de um software prover funcionalidades que satisfaçam o utilizador nas suas necessidades declaradas e implícitas, dentro de um determinado contexto de uso.

	1	2	3	4	5	6	
Capacidade inadequada	○	○	○	○	○	○	Capacidade adequada

D2.5 - Atratividade do software.

	1	2	3	4	5	6	
Aborrecido	○	○	○	○	○	○	Estimulante

D2.6 - Flexibilidade do software.

O princípio da flexibilidade diz respeito a como o software é capaz de se adequar às mudanças solicitadas na aplicação.

	1	2	3	4	5	6	
Rígido	○	○	○	○	○	○	Flexível

D3 - Satisfação com as Terminologia e informação do sistema.

Reação à terminologia é a resposta do utilizador ao conjunto de termos particulares ou a nomenclatura de cada um desses através de uma palavra ou vocábulo apresentados pelo SI

D3.1 - Como avalia os termos usados no sistema?

1	2	3	4	5	6

Inconsistentes ○ ○ ○ ○ ○ ○ Consistentes

D3.2 - A terminologia do SI está relacionada com a tarefa que o utilizador está a realizar?

1 2 3 4 5 6

Nunca ○ ○ ○ ○ ○ ○ Sempre

D3.3 - Como avalia o posicionamento de mensagens no ecrã?

1 2 3 4 5 6

Inconsistente ○ ○ ○ ○ ○ ○ Consistente

D3.4 - O SI mantém o utilizador informado sobre o que está a fazer?

1 2 3 4 5 6

Nunca ○ ○ ○ ○ ○ ○ Sempre

D3.5 - Como avalia as mensagens de erro?

1 2 3 4 5 6

Inúteis ○ ○ ○ ○ ○ ○ Úteis

D4 - Satisfação com a Aprendizagem.

Reação à aprendizagem é a resposta do utilizador à facilidade em aprender a utilizar o SI. O utilizador deve compreender com facilidade a interface, os diferentes percursos e o que pode fazer no sistema

D4.1- Como avalia a exploração de novos recursos do sistema por tentativas?

1 2 3 4 5 6

Difícil ○ ○ ○ ○ ○ ○ Fácil

D4.2 - Como avalia o processo de memorizar os termos e como utilizar os comandos?

1 2 3 4 5 6

Difícil ○ ○ ○ ○ ○ ○ Fácil

D4.3 - As tarefas podem ser realizadas de uma maneira direta?

Os resultados são previsíveis? É lógica a sequência de passos para realizar

1 2 3 4 5 6

Nunca ○ ○ ○ ○ ○ ○ Sempre

D4.4 - Como qualifica as mensagens de ajuda no ecrã?

	1	2	3	4	5	6	
Inúteis	○	○	○	○	○	○	Úteis

D5 - Satisfação com a Capacidade do sistema.

Reação à capacidade é a resposta do utilizador ao conjunto de recursos e características do SI para que se realizem tarefas com sucesso.

D5.1 - Como avalia a velocidade do sistema?

	1	2	3	4	5	6	
Demasiado lento	○	○	○	○	○	○	Suficientemente rápido

D5.2 - Como avalia a fiabilidade do sistema?

	1	2	3	4	5	6	
Não fiável	○	○	○	○	○	○	Fiável

D5.3- As necessidades dos utilizadores com ou sem experiência são tomadas em consideração?

	1	2	3	4	5	6	
Nunca	○	○	○	○	○	○	Sempre

D6 - Sobre os factores abaixo, qual é o nível de importância para avaliar satisfação do utilizador com o SI?

	Sem importância	Pouco importante	Importante	Muito importante
Reações ao Software	○	○	○	○
Terminologia e informação do sistema	○	○	○	○
Aprendizagem	○	○	○	○
Capacidades do sistema	○	○	○	○

D7 - Quais são os fatores que levam o utilizador a ter confiança no SI?

(Assinale todos os itens aplicáveis)

- ☐ O sistema é fácil de usar
- ☐ É rápido de se trabalhar no sistema
- ☐ Aumenta a produtividade do utilizador
- ☐ Proporciona ao utilizador alcançar os objetivos estabelecidos
- ☐ Trabalhar com o SI dá satisfação

☐ Reduz os erros ao trabalhar no SI

D8- Indique o grau de confiança que tem com o SI *
(assinale todos os itens aplicáveis)

	1	2	3	4	5	6	
Desconfiança	○	○	○	○	○	○	Confiança

Enviar

Nunca envie senhas pelo Formulários Google.

Powered by

Este conteúdo não foi criado nem aprovado pelo Google.
Denunciar abuso - Termos de Serviço - Termos Adicionais

ANEXO B – Questionário Técnico

O questionário apresentado neste anexo é o inquérito submetido aos técnicos, que tinha como objetivo obter informações sobre os procedimentos e mecanismos de proteção atualmente implementados comparados com o período antes da implementação, na perspetiva mais técnica.

Questionário (Técnicos) - Impactos da implementação da Segurança da Informação na usabilidade dos SI

Este questionário encontra-se estruturado em 4 grupos de questões. O grupo A destina-se a caracterizar o(a) inquirido(a) e os grupos B, C e D representam os objetivos específicos da dissertação.

Todas as informações fornecidas para o questionário serão tratadas de forma confidencial. De forma a garantir a confidencialidade e o anonimato dos(as) inquiridos(as), agradeço que em nenhuma parte do questionário coloque qualquer nome ou número que o identifique.

Por favor, leia atentamente as instruções e as questões e assinale a resposta que melhor reflecte a sua opinião.
Agradecemos sua colaboração,
Atenciosamente,
Manuel Sequesseque - Mestrando em Sistemas de Informação Organizacionais
José Manuel Gaivéo - Orientador

Nota: Tempo estimado de resposta: 10 minutos

*Obrigatório

A - Identificação/Caracterização do(a) inquirido(a)

A1 - Sexo

- ◯ Feminino
- ◯ Masculino

A2 - Escalão etário

- ◯ Menos de 25 anos
- ◯ Entre 25 a 40 anos
- ◯ Mais de 40 anos

A3 - Habilitações literárias

- ◯ Secundário (Ensino médio)
- ◯ Licenciatura
- ◯ Mestrado/Doutoramento

A4 - Indique o departamento dentro da DFTI onde presta serviço. *

- ◯ Departamento de Engenharia e Implementação de TI
- ◯ Departamento de Serviços Profissionais de TI
- ◯ Departamento de Serviços de TI e Arquitetura de Sistemas

A5 - Há quanto tempo exerce funções?

- ◯ Menos de 1 ano

- ◯ De 1 a 5 anos
- ◯ Mais de 5 anos

A6 - Quais as responsabilidades ou funções de administração ou de suporte desempenha? *
(Assinale todos os itens aplicáveis)

- ☐ Sistema de Gestão de Políticas Segurança da Informação
- ☐ Sistema de gestão de base de dados
- ☐ Desenvolvimento da área de Informática da empresa
- ☐ Desenvolvimento de planos de ação na área das TI e das comunicações
- ☐ Gestão de fornecedores e de contratos de TI e de comunicações
- ☐ Administração dos recursos informáticos da empresa
- ☐ Manutenção da rede local da empresa
- ☐ Manutenção dos servidores da empresa
- ☐ Manutenção de computadores pessoais fixos, portáteis, tablets e smartphones
- ☐ Suporte a aplicações de gestão e de escritório
- ☐ Gestão de contas, domínios e alojamentos web
- ☐ Gestão de plataformas web
- ☐ Suporte a utilizadores
- ☐ Formação a utilizadores
- ☐ Outro: ____

B - Realizar tarefas no Sistema de Informação (SI).

SI é o conjunto constituído por pessoas, procedimentos, dados/informação e componentes TIC (hardware, software e comunicações) que recolhe, processa, armazena, analisa e distribui informação de forma adequada em função dos objetivos da organização.

B1 - Recebeu formação na utilização do SI? *
Se respondeu NÃO, passe para a questão B4

- ◯ Sim
- ◯ Não

B2 - Com que frequência recebe formação necessária à utilização do SI?

- ◯ Uma única vez
- ◯ Sempre que existem mudanças no SI
- ◯ Trimestralmente
- ◯ Semestralmente
- ◯ Anualmente
- ◯ Outro: ____

B3 - Classifique o grau de relevância dessa(s) formação(ões).

	1	2	3	4	5	6	
Pouco relevante	◯	◯	◯	◯	◯	◯	Muito relevante

B4 - Existe algum(uns) documento(s) acerca da utilização do SI?
Se respondeu NÃO, passe para a questão B7

- ◯ Sim
- ◯ Não

B5 - Como tomou conhecimento desse(s) documento(s)?
(Assinale todos os itens aplicáveis)

- ☐ Consta no contrato de trabalho
- ☐ Documento entregue na Organização
- ☐ Informação dos serviços de informática
- ☐ Informação afixada na Organização
- ☐ Chefe de departamento
- ☐ Colega de departamento
- ☐ Outro:

B6 - Classifique o grau de utilidade desse(s) documento(s).

	1	2	3	4	5	6	
Pouco Útil	◯	◯	◯	◯	◯	◯	Muito Útil

B7 - Com que frequência acede ao SI?

- ◯ Todos os dias
- ◯ Quase todos os dias
- ◯ Pelo menos uma vez por semana
- ◯ Pelo menos uma vez a cada duas semanas
- ◯ Pelo menos uma vez por mês
- ◯ Outro:

B8 - Qual é o tempo médio diário de utilização do SI?

- ◯ Até 1 hora
- ◯ Entre 1 e 3 horas
- ◯ Entre 3 e 5 horas
- ◯ Mais de 5 horas

B9 - Como caracteriza a sua utilização ao SI? *
As tarefas que realiza quando utiliza o SI. (Assinale todos os itens aplicáveis)

- ☐ Administração
- ☐ Manutenção do sistema
- ☐ Monitorização do sistema
- ☐ Inserção, modificação ou eliminação de dados
- ☐ Consulta de dados (acesso só de leitura)
- ☐ Elaboração de relatórios
- ☐ Envio/receção de emails
- ☐ Análise estatística
- ☐ Pesquisa na Internet

☐ Impressão de documentos

☐ Outro:

B10 - Classifique o seu grau de facilidade em executar tarefas no SI.

Considere quão à vontade ou ágil é a realizar tarefas quando utiliza o SI.

	1	2	3	4	5	6	
Muito difícil	○	○	○	○	○	○	Muito fácil

B11 - Indique o seu grau de desempenho ao executar tarefas no SI.

Considere se consegue cumprir na íntegra as tarefas que realiza no SI.

	1	2	3	4	5	6	
Baixo desempenho	○	○	○	○	○	○	Elevado desempenho

B12 - Indique o quão rápido é executar tarefas no SI.

Classifique a velocidade de realizar tarefas no SI.

	1	2	3	4	5	6	
Muito lento	○	○	○	○	○	○	Muito rápido

B13 - Classifique o SI quanto a prevenção de erros.

O SI prevê as situações em que o utilizador está prestes a cometer erro?

	1	2	3	4	5	6	
Baixo desempenho	○	○	○	○	○	○	Elevado desempenho

B14 - O utilizador é avisado pelo SI se está a cometer um erro grave.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B15 - O SI ajuda o utilizador a reconhecer, diagnosticar e recuperar dos erros.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B16 - O utilizador é informado da necessidade de plug-ins e são fornecidas instruções de como os instalar.

Um plug-in é uma aplicação que, num programa informático, acresce uma funcionalidade adicional ou uma nova característica ao software. Em português, por conseguinte, pode designar-se plug-in como um complemento.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B17 - As imagens são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B18 - As aplicações são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B19 - Os elementos áudio são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B20 - Os elementos vídeo são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

C- Segurança da Informação no SI

Segurança da informação trata da preservação da confidencialidade, integridade e disponibilidade dos dados armazenados nos SI (ISO/IEC 27001:2013).
Por Sistema de Gestão de Políticas Segurança da Informação entende-se ao conjunto de processos e procedimentos, baseado em normas e na legislação, que uma organização implementa para prover segurança no uso de seus ativos tecnológicos.

C1 - Desde a sua entrada na Organização foi feita alguma implementação de um sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI?

Se respondeu NÃO ou NÃO SABE, passe para a questão C16

- ○ Sim
- ○ Não
- ○ Não sabe

C2 - Como tomou conhecimento da implementação do sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI?

(Assinale todos os itens aplicáveis)

- ☐ Consta no contrato de trabalho
- ☐ Documento entregue na Organização
- ☐ Informação dos serviços de informática
- ☐ Informação afixada na Organização
- ☐ Chefe de departamento
- ☐ Colega de departamento

☐ Outro:

C3 - Participou na implementação desse sistema de gestão de políticas (normas/regulamentos/regras/procedimentos)?

Se respondeu NÃO, passe para a questão C6

○ Sim
○ Não

C4 - Caracterize a sua participação na implementação do sistema.

(Assinale todos os itens aplicáveis)

☐ Instalação de Software
☐ Instalação de Hardware
☐ Elaboração das políticas
☐ Projeção do sistema
☐ Implementação do sistema
☐ Análise de documentos
☐ Levantamento de requisitos
☐ Preenchimento de questionários
☐ Resposta a entrevistas
☐ Outro:

C5 - Classifique o seu grau de participação na implementação do sistema.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C6 - Classifique a sua perceção acerca do funcionamento do SI depois da implementação do sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança.

	1	2	3	4	5	6	
Baixa	○	○	○	○	○	○	Elevada

C7 - Classifique o seu grau de satisfação com implementação do sistema.

	1	2	3	4	5	6	
Pouco satisfeito	○	○	○	○	○	○	Muito satisfeito

C8 - As políticas (normas/regulamentos/regras/procedimentos) de segurança do SI têm sido atualizadas?

Se respondeu NÃO ou NÃO SABE, passe para a questão C12

○ Sim
○ Não
○ Não sabe

C9 - Com que frequência as políticas (normas/regulamentos/regras/procedimentos) de segurança do SI têm sido atualizadas?

- ◯ Mensalmente
- ◯ Trimestralmente
- ◯ Semestralmente
- ◯ Anualmente
- ◯ Outro: _____

C10 - Participou de alguma atualização dessas políticas?

Se respondeu NÃO passe para a questão C12

- ◯ Sim
- ◯ Não

C11- Caracterize a sua participação na atualização das políticas.

(Assinale todos os itens aplicáveis)

- ☐ Planeamento das políticas
- ☐ Implementação das políticas
- ☐ Análise de documentos
- ☐ Levantamento de requisitos
- ☐ Preenchimento de questionários
- ☐ Resposta a entrevistas
- ☐ Outro: _____

C12 - Como era gerida a segurança da informação antes do sistema?

(Assinale todos os itens aplicáveis)

- ☐ Arquivos trancados fisicamente
- ☐ Implementação de políticas aleatórias
- ☐ Conjunto utilizador-password
- ☐ Outro: _____

C13 - Quem fazia a gestão da segurança da informação antes do sistema?

(Assinale todos os itens aplicáveis)

- ☐ A gestão do topo
- ☐ O diretor
- ☐ O chefe do departamento
- ☐ O próprio funcionário
- ☐ O técnico da informática
- ☐ Outro: _____

C14 - Quais os principais problemas identificados na segurança antes da implementação do sistema?

(Assinale todos os itens aplicáveis)

- ☐ Perda de Confidencialidade
- ☐ Perda de Integridade
- ☐ Perda de Disponibilidade

☐ Outro:

C15 - Quais os principais aspetos positivos identificados na segurança antes da implementação do sistema?

(Assinale todos os itens aplicáveis)

☐ Autonomia

☐ Não ingerência

☐ Rapidez na execução de tarefas

☐ Responsabilidade para decidir sobre a segurança

☐ Outro:

C16 - Na sua opinião, qual é a importância que a segurança da informação tem no funcionamento da instituição e das suas atividades diárias no SI?

○ Critica (muito importante)

○ Importante

○ Auxiliar/Secundária

○ Não é importante

○ Não sabe / Não tem a certeza

C17- Na sua opinião, quais os maiores impedimentos para a segurança da informação?

(Assinale todos os itens aplicáveis)

☐ Restrições orçamentais.

☐ Falta de compreensão das ameaças.

☐ Falta de processos e procedimentos formais de segurança.

☐ Falta de envolvimento dos órgãos de gestão.

☐ Falta de sensibilização para as ameaças.

☐ Falta de formação para a segurança do SI.

☐ Problemas de performance das ferramentas de segurança.

☐ Inaptidão para cumprir os regulamentos.

☐ Não sabe

☐ Outro:

C18 - Na sua opinião quais as razões que justificaram/justificariam a necessidade de implementação de sistema de segurança da informação?

(assinale todos os itens aplicáveis)

☐ Importância do SI para a Organização

☐ Necessidade constante de acesso à informação, sendo necessário garantir a sua disponibilidade

☐ Legislação

☐ Dependência que as aplicações e sistemas têm da segurança.

☐ Necessidade de garantir que as informações não são indevidamente alteradas, danificadas ou eliminadas

☐ Aumento das ameaças

☐ Outro:

C19 - Já teve conhecimento de alguma(s) violação(ções) à segurança do SI da organização?

(por exemplo destruição/roubo de equipamentos, utilização não autorizada de ficheiros de outras pessoas, entradas em locais interdito). Se respondeu NÃO, passe para a questão C22

- ◯ Sim
- ◯ Não

C20 - Que atitude tomou quando presenciou essa(s) violação(ções)?
(Assinale todos os itens aplicáveis)

- ☐ Advertiu o(a) infrator(a)
- ☐ Comunicou à gestão
- ☐ Comunicou ao técnico de informática
- ☐ Propôs medidas de solução para o problema
- ☐ Comentou com os(as) seus(as) colegas
- ☐ Nenhuma
- ☐ Outro:

C21- Quais considera terem sido as causas possíveis para as violações à segurança do SI?
(Assinale todos os itens aplicáveis)

- ☐ Ataque interno
- ☐ Ataque externo
- ☐ Vulnerabilidades conhecidas em produtos comerciais (ex.: Windows)
- ☐ Vulnerabilidades desconhecidas em produtos comerciais (ex.: Windows)
- ☐ Vírus e worms por email
- ☐ Aplicações ou serviços Web
- ☐ Engenharia social
- ☐ Erro humano
- ☐ Perda acidental de equipamentos
- ☐ Vírus ou outro código malicioso
- ☐ Abuso de privilégios pelos colaboradores de TI
- ☐ Procedimentos negligentes
- ☐ Não sabe a causa
- ☐ Não é aplicável
- ☐ Outro:

C22 - Existe um departamento, com responsabilidades definidas, para lidar estrategicamente com segurança da informação?
Se respondeu NÃO ou NÃO SABE, passe para a questão C24

- ◯ Sim
- ◯ Não
- ◯ Não sabe

C23 - Qual é o departamento responsáveis pela estratégia da segurança da informação?
(Assinale todos os itens aplicáveis)

- ☐ A gestão de topo
- ☐ A direção
- ☐ O departamento de informática
- ☐ A chefia de cada departamento

- [ ] Não sabe
- [ ] Outro:

C24- Quais das seguintes tecnologias estão implementadas no sistema da segurança? (Assinale todos os itens aplicáveis)

- [ ] Antispyware
- [ ] Sistema de detenção de intrusão
- [ ] Controlo de acesso aos sistemas críticos da empresa;
- [ ] Análise da segurança das estações de trabalho, desktops e notebooks
- [ ] Análise da segurança física e lógica dos servidores de rede
- [ ] Análise da segurança contra contaminação por vírus
- [ ] Avaliação da configuração do firewall
- [ ] Criptografia de dados (e-mails e informações confidenciais)
- [ ] Análise da Política de Backup
- [ ] Análise da exigência de prevenção contra softwares não licenciados na empresa
- [ ] Plano de Contingência
- [ ] Análise da Política de Acesso dos funcionários à Internet
- [ ] Política de Instalação de Software nas estações e na rede;
- [ ] Processo de consciencialização de funcionários.

C25 - Classifique relativamente à segurança da informação do SI (6 para muito importante e 1 para pouco importante) os seguintes aspetos:

C25.1 - Classifique os Gestores.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.2 - Classifique os Utilizadores.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.3 - Classifique os Técnicos de Informática.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.4 - Classifique os Computadores pessoais.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.5 - Classifique os Periféricos.

Por exemplo: Impressoras, Scanners, etc.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.6 - Classifique os Servidores.

Um servidor é um computador que faz parte de uma rede e que fornece serviços a outros computadores, que recebem o nome de clientes. Basicamente, é um computador mais potente do que um desktop comum. Ele foi desenvolvido especificamente para transmitir informações e fornecer produtos de software a outros computadores que estiverem conectados a ele por uma rede.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.7 - Classifique o(s) Software(s) aplicacional.

Por exemplo: Solução de CRM - Customer Relationship Management, SIG - Sistemas Integrado de Gestão e Solução de Gestão e ERP

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.8 - Classifique o(s) Sistema(s) Operativo(s).

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.9 - Classifique a(s) Base(s) de dados.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.10 - Classifique a Internet.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.11 - Classifique os Serviços na cloud.

Serviços na cloud refere-se à utilização da memória e da capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet, ou seja, é uma tecnologia que permite acesso remoto a programas (softwares), arquivos (documentos, músicas, jogos, fotos, vídeos) e serviços por meio da internet.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.12 - Classifique o Email.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.13 - Classifique a Rede interna.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C25.14 - Classifique o Sistema de telecomunicações.
(telefones, fax, etc.)

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

D- Avaliar a satisfação da utilização do SI

A norma ISO 9241-11 define usabilidade como a capacidade de um produto ser usado por utilizadores específicos para atingir objetivos específicos com eficácia, eficiência e satisfação num contexto específico de uso.
Considerando as práticas de segurança da informação, avalie o impacto delas na satisfação da utilização do SI.

D1- Indique o grau de satisfação com as políticas de segurança da informação. *

	1	2	3	4	5	6	
Pouco satisfeito	○	○	○	○	○	○	Muito satisfeito

D2 - Satisfação com o SI enquanto software.

Reação ao software é a resposta do utilizador ao interagir com a interface do SI

D2.1 - Expetativa Visual.
Reação ao contacto visual com a interface

	1	2	3	4	5	6	
Horrível	○	○	○	○	○	○	Fantástico

D2.2 - Adaptação ao software.
Reação à habituação ao SI

	1	2	3	4	5	6	
Difícil	○	○	○	○	○	○	Fácil

D2.3 - Utilização do software.

Reação ao executar tarefas no SI

	1	2	3	4	5	6	
Frustrante	○	○	○	○	○	○	Satisfatório

D2.4 - Capacidade do software.

A capacidade de um software prover funcionalidades que satisfaçam o utilizador nas suas necessidades declaradas e implícitas, dentro de um determinado contexto de uso.

	1	2	3	4	5	6	
Capacidade inadequada	○	○	○	○	○	○	Capacidade adequada

D2.5 - Atratividade do software.

	1	2	3	4	5	6	
Aborrecido	○	○	○	○	○	○	Estimulante

D2.6 - Flexibilidade do software.

O princípio da flexibilidade diz respeito a como o software é capaz de se adequar às mudanças solicitadas na aplicação.

	1	2	3	4	5	6	
Rígido	○	○	○	○	○	○	Flexível

D3 - Satisfação com as Terminologia e informação do sistema.

Reação à terminologia é a resposta do utilizador ao conjunto de termos particulares ou a nomenclatura de cada um desses através de uma palavra ou vocábulo apresentados pelo SI

D3.1 - Como avalia os termos usados no sistema?

	1	2	3	4	5	6	
Inconsistentes	○	○	○	○	○	○	Consistentes

D3.2 - A terminologia do SI está relacionada com a tarefa que o utilizador está a realizar?

	1	2	3	4	5	6	
Nunca	○	○	○	○	○	○	Sempre

D3.3 - Como avalia o posicionamento de mensagens no ecrã?

	1	2	3	4	5	6	

Inconsistente ○ ○ ○ ○ ○ ○ Consistente

D3.4 - O SI mantém o utilizador informado sobre o que está a fazer?

1 2 3 4 5 6

Nunca ○ ○ ○ ○ ○ ○ Sempre

D3.5 - Como avalia as mensagens de erro?

1 2 3 4 5 6

Inúteis ○ ○ ○ ○ ○ ○ Úteis

D4 - Satisfação com a Aprendizagem.

Reação à aprendizagem é a resposta do utilizador à facilidade em aprender a utilizar o SI. O utilizador deve compreender com facilidade a interface, os diferentes percursos e o que pode fazer no sistema

D4.1- Como avalia a exploração de novos recursos do sistema por tentativas?

1 2 3 4 5 6

Difícil ○ ○ ○ ○ ○ ○ Fácil

D4.2 - Como avalia o processo de memorizar os termos e como utilizar os comandos?

1 2 3 4 5 6

Difícil ○ ○ ○ ○ ○ ○ Fácil

D4.3 - As tarefas podem ser realizadas de uma maneira direta?

Os resultados são previsíveis? É lógica a sequência de passos para realizar

1 2 3 4 5 6

Nunca ○ ○ ○ ○ ○ ○ Sempre

D4.4 - Como qualifica as mensagens de ajuda no ecrã?

1 2 3 4 5 6

Inúteis ○ ○ ○ ○ ○ ○ Úteis

D5 - Satisfação com a Capacidade do sistema.

Reação à capacidade é a resposta do utilizador ao conjunto de recursos e características do SI para que se realizem tarefas com sucesso.

D5.1 - Como avalia a velocidade do sistema?

	1	2	3	4	5	6	
Demasiado lento	○	○	○	○	○	○	Suficientemente rápido

D5.2 - Como avalia a fiabilidade do sistema?

	1	2	3	4	5	6	
Não fiável	○	○	○	○	○	○	Fiável

D5.3- As necessidades dos utilizadores com ou sem experiência são tomadas em consideração?

	1	2	3	4	5	6	
Nunca	○	○	○	○	○	○	Sempre

D6 - Sobre os factores abaixo, qual é o nível de importância para avaliar satisfação do utilizador com o SI?

	Sem importância	Pouco importante	Importante	Muito importante
Reações ao Software	○	○	○	○
Terminologia e informação do sistema	○	○	○	○
Aprendizagem	○	○	○	○
Capacidades do sistema	○	○	○	○

D7 - Quais são os fatores que levam o utilizador a ter confiança no SI?
(Assinale todos os itens aplicáveis)

- ☐ O sistema é fácil de usar
- ☐ É rápido de se trabalhar no sistema
- ☐ Aumenta a produtividade do utilizador
- ☐ Proporciona ao utilizador alcançar os objetivos estabelecidos
- ☐ Trabalhar com o SI dá satisfação
- ☐ Reduz os erros ao trabalhar no SI

D8- Indique o grau de confiança que tem com o SI *

	1	2	3	4	5	6	
Desconfiança	○	○	○	○	○	○	Confiança

Enviar

Nunca envie senhas pelo Formulários Google.

ANEXO C – Questionário Utilizador Final

O questionário que se encontra neste anexo apresenta questões mais gerais dirigidas aos utilizadores finais, descurando-se dos aspetos técnicos e da gestão do negócio, tinham o objetivo de obter a informações sobre os impactos causados na utilização do SI pelos procedimentos e mecanismos de proteção atualmente implementados comparados com o período antes da implementação.

Questionário (Utilizadores Finais) - Impactos da implementação da Segurança da Informação na usabilidade dos SI

Este questionário encontra-se estruturado em 4 grupos de questões. O grupo A destina-se a caracterizar o(a) inquirido(a) e os grupos B, C e D representam os objetivos específicos da dissertação.

Todas as informações fornecidas para o questionário serão tratadas de forma confidencial. De forma a garantir a confidencialidade e o anonimato dos(as) inquiridos(as), agradeço que em nenhuma parte do questionário coloque qualquer nome ou número que o identifique.

Por favor, leia atentamente as instruções e as questões e assinale a resposta que melhor reflecte a sua opinião.
Agradecemos sua colaboração,
Atenciosamente,
Manuel Sequesseque - Mestrando em Sistemas de Informação Organizacionais
José Manuel Gaivéo - Orientador

Nota: Tempo estimado de resposta: 10 minutos

*Obrigatório

A - Identificação/Caracterização do(a) inquirido(a)

A1 - Sexo

- ◯ Feminino
- ◯ Masculino

A2 - Escalão etário

- ◯ Menos de 25 anos
- ◯ Entre 25 a 40 anos
- ◯ Mais de 40 anos

A3 - Habilitações literárias

- ◯ Secundário (Ensino médio)
- ◯ Lincenciatura
- ◯ Mestrado/Doutoramento

A4 - Indique o departamento onde presta serviço *

- ◯ Direção de Apoio, Logística e Segurança
- ◯ Direção Comercial e Marketing
- ◯ Direção de Estudos Planeamento e Engenharia
- ◯ Direção de Finanças e Contabilidade
- ◯ Direção de Operação e Manutenção
- ◯ Direção de Recursos Humanos

- ◯ Unidade de Negócios de Cartões Pré-Pago
- ◯ Unidade de Negócios e Serviços Via Operadora
- ◯ Unidade de Negócios Mercados e Serviços Internacionais
- ◯ Unidade de Negócios e Serviços Empresariais

A5 - Há quanto tempo exerce funções? *

- ◯ Menos de 1 ano
- ◯ De 1 a 5 anos
- ◯ Mais de 5 anos

B - Realizar tarefas no Sistema de Informação (SI).

SI é o conjunto constituído por pessoas, procedimentos, dados/informação e componentes TIC (hardware, software e comunicações) que recolhe, processa, armazena, analisa e distribui informação de forma adequada em função dos objetivos da organização.

B1 - Recebeu formação na utilização do SI? *

Se respondeu NÃO, passe para a questão B4

- ◯ Sim
- ◯ Não

B2 - Com que frequência recebe formação necessária à utilização do SI?

- ◯ Uma única vez
- ◯ Sempre que existem mudanças no SI
- ◯ Trimestralmente
- ◯ Semestralmente
- ◯ Anualmente
- ◯ Outro: _____

B3 - Classifique o grau de relevância dessa(s) formação(ões). (6 para elevado e 1 para baixo)

	1	2	3	4	5	6	
Pouco relevante	◯	◯	◯	◯	◯	◯	Muito relevante

B4 - Existe algum(uns) documento(s) acerca da utilização do SI? *

Se respondeu NÃO ou Não sabe, passe para a questão B7

- ◯ Sim
- ◯ Não
- ◯ Não sabe

B5 - Como tomou conhecimento desse(s) documento(s)?

(Assinale todos os itens aplicáveis)

- ☐ Consta no contrato de trabalho
- ☐ Documento entregue na Organização
- ☐ Informação dos serviços de informática
- ☐ Informação afixada na Organização

- [ ] Chefe de departamento
- [ ] Colega de departamento
- [ ] Outro:

B6 - Classifique o grau de utilidade desse(s) documento(s).

	1	2	3	4	5	6	
Pouco Útil	○	○	○	○	○	○	Muito Útil

B7 - Com que frequência acede ao SI? *

- ○ Todos os dias
- ○ Quase todos os dias
- ○ Pelo menos uma vez por semana
- ○ Pelo menos uma vez a cada duas semanas
- ○ Pelo menos uma vez por mês
- ○ Outro:

B8 - Qual é o tempo médio diário de utilização do SI *

- ○ Até 1 hora
- ○ Entre 1 e 3 horas
- ○ Entre 3 e 5 horas
- ○ Mais de 5 horas

B9 - Como caracteriza a sua utilização ao SI?

As tarefas que realiza quando utiliza o SI. (Assinale todos os itens aplicáveis)

- [ ] Administração
- [ ] Manutenção do sistema
- [ ] Monitorização do sistema
- [ ] Inserção, modificação ou eliminação de dados
- [ ] Consulta de dados (acesso só de leitura)
- [ ] Elaboração de relatórios
- [ ] Envio/receção de emails
- [ ] Análise estatística
- [ ] Pesquisa na Internet
- [ ] Impressão de documentos
- [ ] Outro:

B10 - Classifique o seu grau de facilidade em executar tarefas no SI.

Considere quão à vontade ou ágil é a realizar tarefas quando utiliza o SI.

	1	2	3	4	5	6	
Muito difícil	○	○	○	○	○	○	Muito fácil

B11 - Indique o seu grau de desempenho ao executar tarefas no SI.

Considere se consegue cumprir na íntegra as tarefas que realiza no SI.

	1	2	3	4	5	6	
Baixo desempenho	○	○	○	○	○	○	Elevado desempenho

B12 - Indique o quão rápido é executar tarefas no SI.

Classifique a velocidade de realizar tarefas no SI.

	1	2	3	4	5	6	
Muito lento	○	○	○	○	○	○	Muito rápido

B13 - Classifique o SI quanto a prevenção de erros

O SI prevê as situações em que o utilizador está prestes a cometer erro?

	1	2	3	4	5	6	
Baixo desempenho	○	○	○	○	○	○	Elevado desempenho

B14 - O utilizador é avisado pelo SI se está a cometer um erro grave.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B15 - O SI ajuda o utilizador a reconhecer, diagnosticar e recuperar dos erros.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B16 - O utilizador é informado da necessidade de plug-ins e são fornecidas instruções de como os instalar

Um plug-in é uma aplicação que, num programa informático, acresce uma funcionalidade adicional ou uma nova característica ao software. Em português, por conseguinte, pode designar-se plug-in como um complemento.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B17 - As imagens são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B18 - As aplicações são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B19 - Os elementos áudio são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

B20 - Os elementos vídeo são de boa qualidade e demoram pouco tempo a carregar.

	1	2	3	4	5	6	
Discordo	○	○	○	○	○	○	Concordo

C- Segurança da Informação no SI

Segurança da informação trata da preservação da confidencialidade, integridade e disponibilidade dos dados armazenados nos SI (ISO/IEC 27001:2013).
Por Sistema de Gestão de Políticas Segurança da Informação entende-se ao conjunto de processos e procedimentos, baseado em normas e na legislação, que uma organização implementa para prover segurança no uso de seus ativos tecnológicos.

C1 - Desde a sua entrada na Organização foi feita alguma implementação de um sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI? *

Se respondeu NÃO ou NÃO SABE, passe para a questão C14

- ○ Sim
- ○ Não
- ○ Não sabe

C2 - Como tomou conhecimento da implementação do sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI?

(Assinale todos os itens aplicáveis)

- ☐ Consta no contrato de trabalho
- ☐ Documento entregue na Organização
- ☐ Informação dos serviços de informática
- ☐ Informação afixada na Organização
- ☐ Chefe de departamento
- ☐ Colega de departamento
- ☐ Outro: _____

C3 - Participou na implementação desse sistema de gestão de políticas (normas/regulamentos/regras/procedimentos)?

Se respondeu NÃO, passe para a questão C6

- ○ Sim
- ○ Não

C4 - Caracterize a sua participação na implementação do sistema.

(Assinale todos os itens aplicáveis)

- ☐ Instalação de Software

- [ ] Instalação de Hardware
- [ ] Elaboração das políticas
- [ ] Projeção do sistema
- [ ] Implementação do sistema
- [ ] Análise de documentos
- [ ] Levantamento de requisitos
- [ ] Preenchimento de questionários
- [ ] Resposta a entrevistas
- [ ] Outro:

C5 - Classifique o seu grau de participação na implementação do sistema.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C6 - Classifique a sua perceção acerca do funcionamento do SI depois da implementação do sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança.

	1	2	3	4	5	6	
Baixa	○	○	○	○	○	○	Elevada

C7 - Classifique o seu grau de satisfação com implementação do sistema.

	1	2	3	4	5	6	
Pouco satisfeito	○	○	○	○	○	○	Muito satisfeito

C8 - As políticas (normas/regulamentos/regras/procedimentos) de segurança do SI têm sido atualizadas?

Se respondeu NÃO ou NÃO SABE, passe para a questão C12

- ○ Sim
- ○ Não
- ○ Não sabe

C9 - Com que frequência as políticas (normas/regulamentos/regras/procedimentos) de segurança do SI têm sido atualizadas?

- ○ Mensalmente
- ○ Trimestralmente
- ○ Semestralmente
- ○ Anualmente
- ○ Outro:

C10 - Participou de alguma atualização dessas políticas?

Se respondeu NÃO passe para a questão C12

- ○ Sim
- ○ Não

C11- Caracterize a sua participação na atualização das políticas.
(Assinale todos os itens aplicáveis)

- ☐ Planeamento das políticas
- ☐ Implementação das políticas
- ☐ Análise de documentos
- ☐ Levantamento de requisitos
- ☐ Preenchimento de questionários
- ☐ Resposta a entrevistas
- ☐ Outro:

C12 - Como era gerida a segurança da informação antes do sistema?
(Assinale todos os itens aplicáveis)

- ☐ Arquivos trancados fisicamente
- ☐ Implementação de políticas aleatórias
- ☐ Conjunto utilizador-password
- ☐ Outro:

C13 - Quais os principais aspetos positivos identificados na segurança antes da implementação do sistema?
(Assinale todos os itens aplicáveis)

- ☐ Autonomia
- ☐ Não ingerência
- ☐ Rapidez na execução de tarefas
- ☐ Responsabilidade para decidir sobre a segurança
- ☐ Outro:

C14 - Na sua opinião, qual é a importância que a segurança da informação tem no funcionamento da instituição e das suas atividades diárias no SI? *

- ○ Critica (muito importante)
- ○ Importante
- ○ Auxiliar/Secundária
- ○ Não é importante
- ○ Não sabe / Não tem a certeza

C15 - Na sua opinião quais as razões que justificaram/justificariam a necessidade de implementação de sistema de segurança da informação? *
(Assinale todos os itens aplicáveis)

- ☐ Importância do SI para a Organização
- ☐ Necessidade constante de acesso à informação, sendo necessário garantir a sua disponibilidade
- ☐ Legislação
- ☐ Dependência que as aplicações e sistemas têm da segurança
- ☐ Necessidade de garantir que as informações não são indevidamente alteradas, danificadas ou eliminadas
- ☐ Aumento das ameaças
- ☐ Outro:

C16 - Já teve conhecimento de alguma(s) violação(ções) à segurança do SI da organização?
(por exemplo destruição/roubo de equipamentos, utilização não autorizada de ficheiros de outras pessoas, entradas em locais interdito) Se respondeu NÃO, passe para a questão C19

- ◯ Sim
- ◯ Não

C17 - Que atitude tomou quando presenciou essa(s) violação(ções)?
(Assinale todos os itens aplicáveis)

- ☐ Advertiu o(a) infrator(a)
- ☐ Comunicou à gestão
- ☐ Comunicou ao técnico de informática
- ☐ Propôs medidas de solução para o problema
- ☐ Comentou com os(as) seus(as) colegas
- ☐ Nenhuma
- ☐ Outro:

C18 - Quais considera terem sido as causas possíveis para a(s) violação(ões) à segurança do SI?
(Assinale todos os itens aplicáveis)

- ☐ Ataque externo
- ☐ Erro humano
- ☐ Ataque interno
- ☐ Perda acidental de equipamentos
- ☐ Vírus ou outro código malicioso
- ☐ Abuso de privilégios pelos colaboradores de TI
- ☐ Procedimentos negligentes
- ☐ Não sabe a causa
- ☐ Não é aplicável
- ☐ Outro:

C19 - Existe um departamento, com responsabilidades definidas, para lidar estrategicamente com segurança da informação?
Se respondeu NÃO ou NÃO SABE, passe para a questão C21

- ◯ Sim
- ◯ Não
- ◯ Não sabe

C20 - Qual é o departamento responsável pela estratégia da segurança da informação?
(Assinale todos os itens aplicáveis)

- ☐ A gestão de topo
- ☐ A direção
- ☐ O departamento de informática
- ☐ A chefia de cada departamento
- ☐ Não sabe
- ☐ Outro:

C21 - Classifique relativamente à segurança da informação do SI (6 para muito importante e 1 para pouco importante) os seguintes aspetos:

C21.1 - Classifique os Utilizadores.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C21.2 - Classifique os Técnicos de Informática.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C21.3 - Classifique os Computadores pessoais.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C21.4 - Classifique os Periféricos.

Por exemplo: Impressoras, Scanners, etc.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C21.5 - Classifique os Servidores.

Um servidor é um computador que faz parte de uma rede e que fornece serviços a outros computadores, que recebem o nome de clientes. Basicamente, é um computador mais potente do que um desktop comum. Ele foi desenvolvido especificamente para transmitir informações e fornecer produtos de software a outros computadores que estiverem conectados a ele por uma rede.

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C21.6 - Classifique o(s) Software(s) aplicacional.

Por exemplo: Solução de CRM - Customer Relationship Management, SIG - Sistemas Integrado de Gestão e Solução de Gestão e ERP

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C21.7 - Classifique o(s) Sistema(s) Operativo(s)

1 2 3 4 5 6

Pouco importante ○ ○ ○ ○ ○ ○ Muito importante

C21.8 - Classifique a(s) Base(s) de dados

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C21.9 - Classifique a Internet

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C21.10 - Classifique os Serviços na cloud

Serviços na cloud refere-se à utilização da memória e da capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet, ou seja, é uma tecnologia que permite acesso remoto a programas (softwares), arquivos (documentos, músicas, jogos, fotos, vídeos) e serviços por meio da internet.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C21.11 - Classifique o Email.

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C21.12 - Classifique a Rede interna

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

C21.13 - Classifique o Sistema de telecomunicações
(telefones, fax, etc.)

	1	2	3	4	5	6	
Pouco importante	○	○	○	○	○	○	Muito importante

D- Avaliar a satisfação da utilização do SI

A norma ISO 9241-11 define usabilidade como a capacidade de um produto ser usado por utilizadores específicos para atingir objetivos específicos com eficácia, eficiência e satisfação num contexto específico de uso.
Considerando as práticas de segurança da informação, avalie o impacto delas na satisfação da utilização do SI.

D1- Indique o grau de satisfação com as políticas de segurança da informação. *

1 2 3 4 5 6

Pouco satisfeito ○ ○ ○ ○ ○ ○ Muito satisfeito

D2 - Satisfação com o SI enquanto software.

Reação ao software é a resposta do utilizador ao interagir com a interface do SI

D2.1 - Expetativa Visual

Reação ao contacto visual com a interface

1 2 3 4 5 6

Horrível ○ ○ ○ ○ ○ ○ Fantástico

D2.2 - Adaptação ao software

Reação à habituação ao SI

1 2 3 4 5 6

Difícil ○ ○ ○ ○ ○ ○ Fácil

D2.3 - Utilização do software

Reação ao executar tarefas no SI

1 2 3 4 5 6

Frustrante ○ ○ ○ ○ ○ ○ Satisfatório

D2.4 - Capacidade do software

A capacidade de um software prover funcionalidades que satisfaçam o utilizador nas suas necessidades declaradas e implícitas, dentro de um determinado contexto de uso.

1 2 3 4 5 6

Capacidade inadequada ○ ○ ○ ○ ○ ○ Capacidade adequada

D2.5 - Atratividade do software

1 2 3 4 5 6

Aborrecido ○ ○ ○ ○ ○ ○ Estimulante

D2.6 - Flexibilidade do software

O princípio da flexibilidade diz respeito a como o software é capaz de se adequar às mudanças solicitadas na aplicação.

1 2 3 4 5 6

Rígido ○ ○ ○ ○ ○ ○ Flexível

D3 - Satisfação com as Terminologia e informação do sistema.

Reação à terminologia é a resposta do utilizador ao conjunto de termos particulares ou a nomenclatura de cada um desses através de uma palavra ou vocábulo apresentados pelo SI

D3.1 - Como avalia os termos usados no sistema?

	1	2	3	4	5	6	
Inconsistentes	○	○	○	○	○	○	Consistentes

D3.2 - A terminologia do SI está relacionada com a tarefa que o utilizador está a realizar?

	1	2	3	4	5	6	
Nunca	○	○	○	○	○	○	Sempre

D3.3 - Como avalia o posicionamento de mensagens no ecrã?

	1	2	3	4	5	6	
Inconsistente	○	○	○	○	○	○	Consistente

D3.4 - O SI mantém o utilizador informado sobre o que está a fazer?

	1	2	3	4	5	6	
Nunca	○	○	○	○	○	○	Sempre

D3.5 - Como avalia as mensagens de erro? *

	1	2	3	4	5	6	
Inúteis	○	○	○	○	○	○	Úteis

D4 - Satisfação com a Aprendizagem.

Reação à aprendizagem é a resposta do utilizador à facilidade em aprender a utilizar o SI. O utilizador deve compreender com facilidade a interface, os diferentes percursos e o que pode fazer no sistema

D4.1- Como avalia a exploração de novos recursos do sistema por tentativas?

	1	2	3	4	5	6	
Difícil	○	○	○	○	○	○	Fácil

D4.2 - Como avalia o processo de memorizar os termos e como utilizar os comandos?

	1	2	3	4	5	6	

Difícil ○ ○ ○ ○ ○ ○ Fácil

D4.3 - As tarefas podem ser realizadas de uma maneira direta?
Os resultados são previsíveis? É lógica a sequência de passos para realizar uma tarefa?

1 2 3 4 5 6

Nunca ○ ○ ○ ○ ○ ○ Sempre

D4.4 - Como qualifica as mensagens de ajuda no ecrã?

1 2 3 4 5 6

Inúteis ○ ○ ○ ○ ○ ○ Úteis

D5 - Satisfação com a Capacidade do sistema.

Reação à capacidade é a resposta do utilizador ao conjunto de recursos e características do SI para que se realizem tarefas com sucesso.

D5.1 - Como avalia a velocidade do sistema?

1 2 3 4 5 6

Demasiado lento ○ ○ ○ ○ ○ ○ Suficientemente rápido

D5.2 - Como avalia a fiabilidade do sistema?

1 2 3 4 5 6

Não fiável ○ ○ ○ ○ ○ ○ Fiável

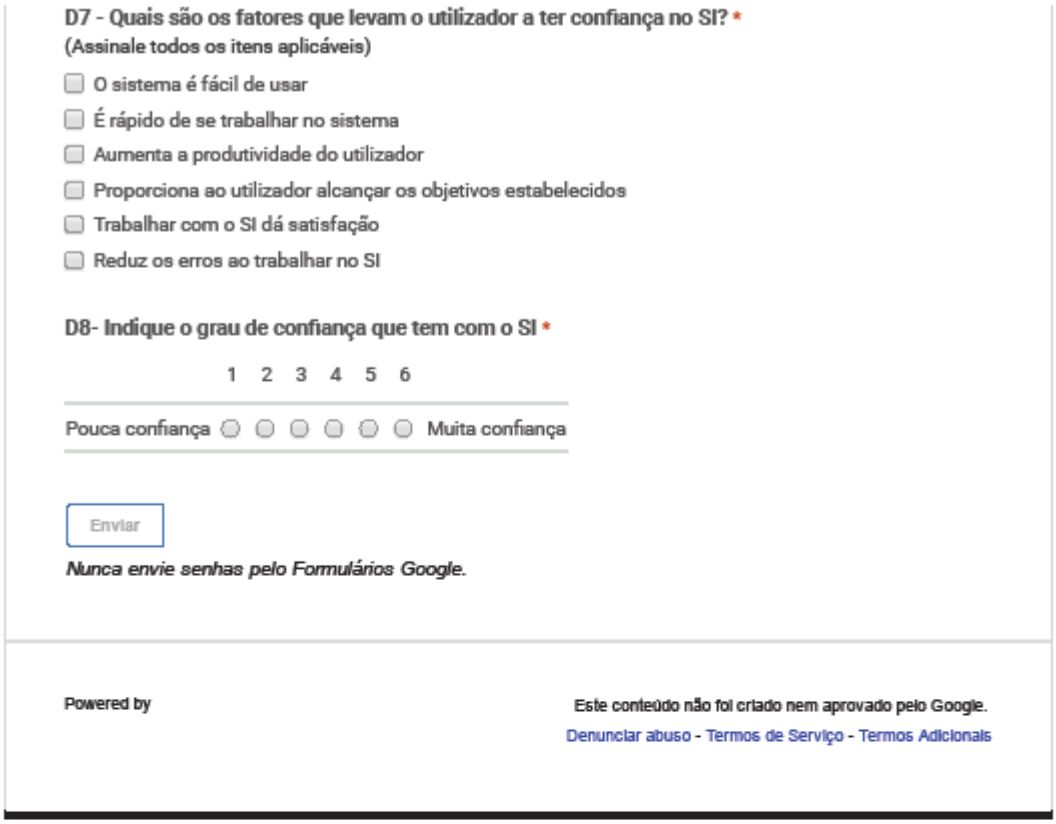
D5.3- As necessidades dos utilizadores com ou sem experiência são tomadas em consideração?

1 2 3 4 5 6

Nunca ○ ○ ○ ○ ○ ○ Sempre

D6 - Sobre os factores abaixo, qual é o nível de importância para avaliar satisfação do utilizador com o SI?

	Sem importância	Pouco importante	Importante	Muito importante
Reações ao Software	○	○	○	○
Terminologia e informação do sistema	○	○	○	○
Aprendizagem	○	○	○	○
Capacidades do sistema	○	○	○	○



D7 - Quais são os fatores que levam o utilizador a ter confiança no SI? *
(Assinale todos os itens aplicáveis)

- [ ] O sistema é fácil de usar
- [ ] É rápido de se trabalhar no sistema
- [ ] Aumenta a produtividade do utilizador
- [ ] Proporciona ao utilizador alcançar os objetivos estabelecidos
- [ ] Trabalhar com o SI dá satisfação
- [ ] Reduz os erros ao trabalhar no SI

D8- Indique o grau de confiança que tem com o SI *

	1	2	3	4	5	6	
Pouca confiança	○	○	○	○	○	○	Muita confiança

Enviar

Nunca envie senhas pelo Formulários Google.

Powered by

Este conteúdo não foi criado nem aprovado pelo Google.
Denunciar abuso - Termos de Serviço - Termos Adicionais

ANEXO D – Resultados dos Questionários

Os resultados aqui apresentados correspondem às respostas dos três tipos questionários apresentados nos anexos A, B e C, cujos resultados são apresentados no capítulo 5.

Resultados dos Questionários

A - Identificação/Caracterização do(a) inquirido(a)

A1 – Sexo						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Feminino	4	50,0	8	17,8	46	28,4
Masculino	4	50,0	37	82,2	116	71,6
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

A2 – Escalão etário		
	Gestores	
	Nº	%
Menos de 30 anos	0	0,0
Entre 30 a 45 anos	2	25,0
Mais de 45 anos	6	75,0
Não Responderam	0	0,0
Total de Respostas	8	

A2 – Escalão etário				
	Técnicos		Utilizadores finais	
	Nº	%	Nº	%
Menos de 25 anos	8	17,8	40	24,7
Entre 25 a 40 anos	27	60,0	86	53,1
Mais de 40 anos	10	22,2	36	22,2
Não Responderam	0	0,0	0	0,0
Total de Respostas	45		162	

A3 – Habilitações literárias		
	Gestores	
	Nº	%
Licenciatura		
Mestrado	4	50,0
Doutoramento	4	50,0
Não Responderam	0	0,0
Total de Respostas	8	

A3 – Habilitações literárias				
	Técnicos		Utilizadores finais	
	Nº	%	Nº	%
Secundário (Ensino médio)	0	0,0	9	5,5
Licenciatura	29	64,5	128	79,0
Mestrado/Doutoramento	15	33,3	22	13,6
Não Responderam	1	2,2	3	1,9
Total de Respostas	45		162	

A4 – Indique a área da estrutura orgânica de gestão onde presta serviço.		
	Gestores	
	Nº	%
Administração	1	12,5
Orgãos de Assessoria e Apoio	5	62,5
Direção Executiva de Operações	2	25,0
Não Responderam	0	0,0
Total de Respostas	8	

A4 – Indique o departamento dentro da DFTI onde presta serviço.		
	Técnicos	
	Nº	%
Departamento de Engenharia e Implementação de TI	19	42,2
Departamento de Serviços Profissionais de TI	11	24,4
Departamento de Serviços de TI e Arquitetura de Sistemas	15	33,3
Não Responderam	0	0,0
Total de Respostas	45	

A4 – Indique o departamento onde presta serviço.		
	Utilizadores finais	
	Nº	%
Direção de Apoio, Logística e Segurança	9	5,5
Direção Comercial e Marketing	14	8,6
Direção de Estudos Planeamento e Engenharia	41	25,3
Direção de Finanças e Contabilidade	10	6,2
Direção de Operação e Manutenção	49	30,2
Direção de Recursos Humanos	10	6,2
Unidade de Negócios de Cartões Pré-Pago	5	3,1
Unidade de Negócios e Serviços Via Operadora	10	6,2
Unidade de Negócios Mercados e Serviços Internacionais	3	1,9
Unidade de Negócios e Serviços Empresariais	11	6,8
Não Responderam	0	0,0
Total de Respostas	162	

A5 – Há quanto tempo exerce funções?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Menos de 1 ano	0	0,0	5	11,9	30	18.5
De 1 a 5 anos	1	12,5	16	38,1	74	45,7
Mais de 5 anos	7	87,5	21	50,0	58	35,8
Não Responderam	0	0,0	3	0,0	0	0,0
Total de Respostas	8		45		162	

A6 – Quais as responsabilidade ou funções de administração ou de suporte desempenha? (Assinale todos os itens aplicáveis)		
	Técnicos	
	Nº	%
Sistema de Gestão de Políticas Segurança da Informação	7	15,6
Sistema de gestão de base de dados	7	15,6
Desenvolvimento da área de Informática da empresa	4	8,9
Desenvolvimento de planos de ação na área das TI e das comunicações	7	15,6
Gestão de fornecedores e de contratos de TI e de comunicações	7	15,6
Administração dos recursos informáticos da empresa	2	4,4
Manutenção da rede local da empresa	8	17,8
Manutenção dos servidores da empresa	6	13,3
Manutenção de computadores pessoais fixos, portáteis, tablets e smartphones	3	6,7
Suporte a aplicações de gestão e de escritório	6	13,3
Gestão de contas, domínios e alojamentos web	5	11,1
Gestão de plataformas web	3	6,7
Suporte a utilizadores	12	26,7
Formação a utilizadores	6	13,3
Outras	27	60,0
Não Responderam	0	0,0
Total de Respostas	45	

B - Realizar tarefas no Sistema de Informação (SI).

B1 – Recebeu formação na utilização do SI?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Não	0	0,0	0	0,0	8	4,9
Sim	8	100	45	100	154	95,1
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B2 – Com que frequência recebe formação necessária à utilização do SI?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Uma única vez	0	0,0	0	0,0	84	51,9
Sempre que existem mudanças no SI	8	100	30	66,7	61	37,7
Trimestralmente	0	0,0	0	0,0	2	1,2
Semestralmente	0	0,0	0	0,0	1	0,6
Anualmente	0	0,0	0	0,0	0	0,0
Outra	0	0,0	15	33,3	6	3,7
Não Responderam	0	0,0	0	0,0	8	4,9
Total de Respostas	8		45		162	

B3 – Classifique o grau de relevância dessa(s) formação(ões). (1 pouco relevante e 6 muito relevante)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	1	0,6
3	0	0,0	0	0,0	0	0,0
4	0	0,0	0	0,0	6	3,7
5	0	0,0	0	0,0	15	9,2
6	8	100,0	45	100,0	131	80.9
Não Responderam	0	0,0	0	0,0	9	5,6
Total de Respostas	8		45		162	

B4 – Existe algum(uns) documento(s) acerca da utilização do SI?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Não	0	0,0	0	0,0	44	27,2
Não sabe	0	0,0	0	0,0	4	2,5
Sim	8	100,0	45	100,0	114	70,4
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B5 – Como tomou conhecimento desse(s) documento(s)?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Consta no contrato de trabalho	0	0,0	1	2,2	1	0,9
Documento entregue na Organização		0,0	40	88,9	86	74,8
Informação dos serviços de informática	2	25,0	15	33,3	108	93,9
Informação afixada na Organização	7	87,5	0	0,0	2	1,7
Colega	0	0,0	0	0,0	4	3,5
Outro	0	0,0	0	0,0	0	0,0
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B6 – Classifique o grau de utilidade desse(s) documento(s). (1 para pouco útil e 6 para muito útil)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	1	0,6
3	0	0,0	0	0,0	0	0,0
4	0	0,0	0	0,0	2	1,3
5	0	0,0	0	0,0	6	3,7
6	8	0,0	42	93,3	153	94,4
Não Responderam	0	0,0	3	6,7	0	0,0
Total de Respostas	8		45		162	

B7 – Com que frequência acede ao SI?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Todos os dias	6	75,0	45	100,0	69	42,6
Quase todos os dias	2	25,0	0	0,0	84	51,9
Pelo menos uma vez por semana	0	0,0	0	0,0	4	2,5
Pelo menos uma vez a cada duas semanas	0	0,0	0	0,0	4	2,5
Pelo menos uma vez por mês	0	0,0	0	0,0	0	0,0
Todos os dias	0	0,0	0	0,0	1	0,6
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B8 – Com que frequência acede ao SI?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Até 1 hora	0	0,0	0	0,0	7	4,3
Entre 1 e 3 horas	0	0,0	0	0,0	25	15,4
Entre 3 e 5 horas	0	0,0	0	0,0	72	44,4
Mais de 5 horas	8	100,0	45	100,0	58	35,8
Não Responderam	0	0,0	0		0	0,0
Total de Respostas	8		45		162	

B9 – Como caracteriza a sua utilização ao SI?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Administração	8	100,0	40	88,9	12	7,4
Manutenção do sistema	0	0,0	35	77,8	5	3,1
Monitorização do sistema	8	100,0	43	95,6	44	27,2
Inserção, modificação ou eliminação de dados	8	100,0	45	100,0	133	82,1
Consulta de dados (acesso só de leitura)	8	100,0	44	97,8	144	88,9
Elaboração de relatórios	8	100,0	45	100,0	147	90,7
Envio/receção de emails	8	100,0	44	97,8	154	95,1
Análise estatística	8	100,0	38	84,4	122	75,3
Pesquisa na Internet	7	87,5	36	80,0	142	87,7
Impressão de documentos	8	100,0	44	97,8	148	91,4
Outra:	0	0,0	0	0,0	0	0,0
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B10 – Classifique o seu grau de facilidade em executar tarefas no SI. (1 para muito difícil e 6 para muito fácil)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	25	15,4
2	0	0,0	0	0,0	2	1,2
3	0	0,0	0	0,0	8	4,9
4	0	0,0	0	0,0	3	1,9
5	0	0,0	0	0,0	12	7,4
6	8	100,0	45	100,0	112	69,1
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B11 – Indique o seu grau de desempenho ao executar tarefas no SI. (1 para baixo e 6 para elevado)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	2	1,2
4	0	0,0	0	0,0	6	3,7
5	0	0,0	0	0,0	43	26,5
6	8	100,0	45	100,0	111	68,5
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B12 – Indique o quão rápido é executar tarefas no SI. (1 para muito lento e 6 para muito rápido)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	1	0,6
4	0	0,0	0	0,0	14	8,6
5	0	0,0	0	0,0	35	21,6
6	8	100,0	45	100,0	112	69,1
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B13 – Classifique o SI quanto a prevenção de erros. (1 para baixo desempenho e 6 para elevado desempenho)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	4	2,5
4	0	0,0	0	0,0	12	7,4
5	0	0,0	0	0,0	54	33,3
6	8	100,0	45	100,0	91	56,2
Não Responderam	0	0,0	0	0,0	1	0,6
Total de Respostas	8		45		162	

B14 – O utilizador é avisado pelo SI se está a cometer um erro grave. (1 para discordo e 6 para concordo)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	1	0,6
3	0	0,0	0	0,0	3	1,9
4	0	0,0	0	0,0	8	4,9
5	0	0,0	1	2,2	46	28,4
6	8	100,0	44	97,8	104	64,2
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B15 – O SI ajuda o utilizador a reconhecer, diagnosticar e recuperar dos erros. (1 para discordo e 6 para concordo)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	1	0,6
3	0	0,0	0	0,0	3	1,9
4	0	0,0	0	0,0	7	4,3
5	0	0,0	0	0,0	49	30,2
6	8	100,0	45	100,0	102	63,0
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B16 – O utilizador é informado da necessidade de plug-ins e são fornecidas instruções de como os instalar. (1 para discordo e 6 para concordo)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	2	1,2
3	0	0,0	0	0,0	3	1,9
4	0	0,0	0	0,0	21	13,0
5	1	12,5	0	0,0	38	23,5
6	7	87,5	45	100,0	98	60,5
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B17 – As imagens são de boa qualidade e demoram pouco tempo a carregar. (1 para discordo e 6 para concordo)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	1	0,6
3	0	0,0	0	0,0	2	1,2
4	0	0,0	0	0,0	12	7,4
5	0	0,0	0	0,0	44	27,2
6	8	100,0	45	100,0	102	63,0
Não Responderam	0	0,0	0	0,0	1	0,6
Total de Respostas	8		45		162	

B18 – As aplicações são de boa qualidade e demoram pouco tempo a carregar. (1 para discordo e 6 para concordo)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	2	1,2
4	0	0,0	0	0,0	8	4,9
5	0	0,0	0	0,0	36	22,2
6	8	100,0	45	100,0	116	71,6
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B19 – Os elementos áudio são de boa qualidade e demoram pouco tempo a carregar. (1 para discordo e 6 para concordo)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	2	1,2
4	0	0,0	0	0,0	9	5,6
5	0	0,0	0	0,0	49	30,4
6	8	100,0	45	100,0	101	62,7
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

B20 – Os elementos vídeo são de boa qualidade e demoram pouco tempo a carregar. (1 para discordo e 6 para concordo)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	1	0,6
3	0	0,0	0	0,0	5	3,1
4	0	0,0	0	0,0	9	5,6
5	0	0,0	0	0,0	52	32,1
6	8	100,0	45	100,0	95	58,6
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

C- Segurança da Informação no SI

C1 - Desde a sua entrada na Organização foi feita alguma implementação de um sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Não	1	12,5	19	42,2	37	22,8
Não sabe	0	0,0	2	4,4	64	39,5
Sim	7	87,5	24	53,3	61	37,7
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

C2 – Como tomou conhecimento da implementação do sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI? (Assinale todos os itens aplicáveis)		
	Gestores	
	Nº	%
Consta no contrato de trabalho	0	0,0
Documento entregue na Organização	0	0,0
Informação dos serviços de informática	5	71,4
Informação afixada na Organização	7	100,0
Colega	0	0,0
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	7	

C2 – Como tomou conhecimento da implementação do sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança do SI? (Assinale todos os itens aplicáveis)				
	Técnicos		Utilizadores finais	
	Nº	%	Nº	%
Consta no contrato de trabalho	2	8,3	1	1,6
Documento entregue na Organização	22	91,7	40	65,6
Informação dos serviços de informática	5	20,8	60	98,3
Informação afixada na Organização	1	4,2	2	3,2
Chefe de departamento	0	0,0	5	8,2
Colega	0	0,0	2	3,2
Outro	0	0,0	0	0,0
Não Responderam	0	0,0	0	0,0
Total de Respostas	24		61	

C3 - Participou na implementação desse sistema de gestão de políticas (normas/regulamentos/regras/procedimentos)?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Não	0	0,0	1	4,2	25	40,9
Sim	7	100,0	23	95,8	36	59,1
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	7		24		61	

C4 – Caracterize a sua participação na implementação do sistema. (Assinale todos os itens aplicáveis)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Instalação de Software	0	0,0	3	13,0	0	0,0
Instalação de Hardware	0	0,0	0	0,0	0	0,0
Elaboração das políticas	0	0,0	7	30,4	1	2,8
Projeção do sistema	0	0,0	2	8,7	0	0,0
Implementação do sistema	0	0,0	4	17,4	0	0,0
Análise de documentos	1	14,3	12	52,2	1	2,8
Levantamento de requisitos	0	0,0	15	65,2	8	22,2
Preenchimento de questionários	2	28,6	11	47,8	34	94,4
Resposta a entrevistas	6	85,7	7	30,4	34	94,4
Outro:	0	0,0	0	0,0	0	0,0
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	7		23		36	

C5 – Classifique o seu grau de participação na implementação do sistema. (1 para pouco importante e 6 para muito importante)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	0	0,0
4	0	0,0	1	4,3	7	19,4
5	0	0,0	5	21,7	11	30,5
6	7	100,0	17	73,9	17	47,2
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	7		23		36	

C6 – Classifique a sua perceção acerca do funcionamento do SI depois da implementação do sistema de gestão de políticas (normas/regulamentos/regras/procedimentos) de segurança. (1 para baixa e 6 para elevada)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	0	0,0
4	0	0,0	0	0,0	2	3,3
5	0	0,0	0	0,0	12	19,6
6	7	100,0	24	100,0	46	75,4
Não Responderam	0	0,0		0,0	1	1,6
Total de Respostas	7		24		61	

C7 – Classifique o seu grau de satisfação com implementação do sistema. (1 para pouco satisfeito e 6 para muito satisfeito)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	0	0,0
4	0	0,0	0	0,0	1	1,6
5	0	0,0	3	12,5	23	37,7
6	7	100,0	21	87,5	37	60,7
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	7		24		61	

C8 - As políticas (normas/regulamentos/regras/procedimentos) de segurança do SI têm sido atualizadas?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Não	0	0,0	0	0,0	0	0
Não sabe	0	0,0	0	0,0	7	11,5
Sim	7	100,0	24	100,0	54	88,5
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	7		24		61	

C9 – Com que frequência as políticas (normas/regulamentos/regras/procedimentos) de segurança do SI têm sido atualizadas?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Mensalmente	0	0,0	0	0,0	2	3,9
Trimestralmente	0	0,0	0	0,0	1	1,7
Semestralmente	0	0,0	0	0,0	0	0,0
Anualmente	0	0,0	0	0,0	0	0,0
Outro	7	100,0	24	100,0	51	94,4
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	7		24		54	

C10 - Participou de alguma atualização dessas políticas?						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Não	0	0,0	0	0,0	18	33,3
Sim	7	100,0	24	100,0	36	66,7
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	7		24		54	

C11 – Caracterize a sua participação na atualização das políticas. (Assinale todos os itens aplicáveis)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Planeamento das políticas	2	28,6	9	37,5	0	0,0
Implementação das políticas	0	0,0	8	33,3	0	0,0
Análise de documentos	1	14,3	9	37,5	1	2,7
Levantamento de requisitos	0	0,0	12	50,0	1	2,7
Preenchimento de questionários	1	14,3	10	41,7	32	88,9
Resposta a entrevistas	5	71,4	10	41,7	32	88,9
Outro	0	0,0	0	0,0	0	0,0
Não Responderam	0	0,0	0	4,1	0	0,0
Total de Respostas	7		24		36	

C12 – Como era gerida a segurança da informação antes do sistema? (Assinale todos os itens aplicáveis)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
Arquivos trancados fisicamente	7	100,0	22	91,6	21	34,4
Implementação de políticas aleatórias	6	85,7	11	45,8	33	54,1
Conjunto utilizador-password	7	100,0	23	95,8	59	96,7
Outro	0	0,0	12	50,0	0	0,0
Não Responderam	0	0,0	1	4,1	0	0,0
Total de Respostas	7		24		61	

C13 – Quem fazia a gestão da segurança da informação antes do sistema? (Assinale todos os itens aplicáveis)				
	Gestores		Técnicos	
	Nº	%	Nº	%
A gestão do topo	7	100,0	23	95,8
O diretor	0	0,0	0	0,0
O chefe do departamento	2	28,6	18	75,0
O próprio funcionário	0	0,0	0	0,0
O técnico da informática	7	100,0	19	79,1
Outro	0	0,0	0	0,0
Não Responderam	0	0,0	1	4,1
Total de Respostas	7		24	

C13 – Quais os principais aspetos positivos identificados na segurança antes da implementação do sistema? (Assinale todos os itens aplicáveis)		
	Utilizadores finais	
	Nº	%
Autonomia	22	36,1
Não ingerência	6	9,8
Rapidez na execução de tarefas	47	77,0
Responsabilidade para decidir sobre a segurança	50	81,9
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	61	

C14 – Quais os principais problemas identificados na segurança antes da implementação do sistema? (Assinale todos os itens aplicáveis)				
	Gestores		Técnicos	
	Nº	%	Nº	%
Perda de Confidencialidade	7	100,0	23	95,8
Perda de Integridade	7	100,0	23	95,8
Perda de Disponibilidade	7	100,0	23	95,8
Outro	0	0,0	0	0,0
Não Responderam	0	0,0	1	4,1
Total de Respostas	7		24	

C14 – Na sua opinião, qual é a importância que a segurança da informação tem no funcionamento da instituição e das suas atividades diárias no SI?		
	Utilizadores finais	
	Nº	%
Critica (muito importante)	88	54,3
Importante	70	43,2
Auxiliar/Secundária	2	1,2
Não é importante	0	0
Não sabe / Não tem a certeza	2	1,2
Não Responderam	0	0,0
Total de Respostas	162	

C15 – Quais os principais problemas identificados na segurança antes da implementação do sistema? (Assinale todos os itens aplicáveis)				
	Gestores		Técnicos	
	Nº	%	Nº	%
Autonomia	0	0,0	4	16,6
Não ingerência	0	0,0	2	8,3
Rapidez na execução de tarefas	2	28,6	23	95,8
Responsabilidade para decidir sobre a segurança	0	0,0	23	95,8
Outro	5	71,4	0	0,0
Não Responderam	0	0,0	1	4,1
Total de Respostas	7		24	

C15 – Na sua opinião quais as razões que justificaram/justificariam a necessidade de implementação de sistema de segurança da informação? (Assinale todos os itens aplicáveis)		
	Utilizadores finais	
	Nº	%
Importância do SI para a Organização	97	59,9
Necessidade constante de acesso à informação, sendo necessário garantir a sua disponibilidade	84	51,9
Legislação	19	11,7
Dependência que as aplicações e sistemas têm da segurança.	13	8,0
Necessidade de garantir que as informações não são indevidamente alteradas, danificadas ou eliminadas	129	79,6
Aumento das ameaças	135	83,3
Outra	55	34,0
Não Responderam	0	0,0
Total de Respostas	162	

C16 – Na sua opinião, qual é a importância que a segurança da informação tem no funcionamento da instituição e das suas atividades diárias no SI?				
	Gestores		Técnicos	
	Nº	%	Nº	%
Critica (muito importante)	8	100,0	45	100,0
Importante	0	0,0	0	0,0
Auxiliar/Secundária	0	0,0	0	0,0
Não é importante	0	0,0	0	0,0
Não sabe / Não tem a certeza	0	0,0	0	0,0
Não Responderam	0	0,0	0	0,0
Total de Respostas	8		45	

C16 – Já teve conhecimento de alguma(s) violação(ções) à segurança do SI da organização?		
	Utilizadores finais	
	Nº	%
Não	102	63,0
Sim	60	37,0
Não Responderam	0	0,0
Total de Respostas	162	

C17 – Na sua opinião, quais os maiores impedimentos para a segurança da informação? (Assinale todos os itens aplicáveis)				
	Gestores		Técnicos	
	Nº	%	Nº	%
Restrições orçamentais.	8	100,0	45	100,0
Falta de compreensão das ameaças.	8	100,0	41	91,1
Falta de processos e procedimentos formais de segurança.	8	100,0	17	37,8
Falta de envolvimento dos órgãos de gestão.	8	100,0	42	93,3
Falta de sensibilização para as ameaças.	8	100,0	27	60,0
Falta de formação para a segurança do SI.	8	100,0	28	62,2
Problemas de performance das ferramentas de segurança.	8	100,0	17	37,8
Inaptidão para cumprir os regulamentos.	8	100,0	39	86,7
Não sabe	0	0,0	0	0,0
Outro	0	0,0	3	6,7
Não Responderam	0	0,0	0	0,0
Total de Respostas	8		45	

C17 – Que atitude tomou quando presenciou essa(s) violação(ções)? (Assinale todos os itens aplicáveis)		
	Utilizadores finais	
	Nº	%
Advertiu o(a) infrator(a)	24	38,1
Comunicou à gestão	10	15,9
Comunicou ao técnico de informática	32	50,8
Propôs medidas de solução para o problema	6	9,5
Comentou com os(as) seus(as) colegas	17	27,0
Nenhuma	18	28,6
Outro	1	1,6
Não Responderam	0	0,0
Total de Respostas	60	

C18 – Na sua opinião quais as razões que justificaram/justificariam a necessidade de implementação de sistema de segurança da informação? (Assinale todos os itens aplicáveis)				
	Gestores		Técnicos	
	Nº	%	Nº	%
Importância do SI para a Organização	8	100,0	45	100,0
Necessidade constante de acesso à informação, sendo necessário garantir a sua disponibilidade	8	100,0	38	84,4
Legislação	8	100,0	20	44,4
Dependência que as aplicações e sistemas têm da segurança.	8	100,0	32	71,1
Necessidade de garantir que as informações não são indevidamente alteradas, danificadas ou eliminadas	8	100,0	41	91,1
Aumento das ameaças	8	100,0	45	100,0
Outro	0	0,0	0	0,0
Não Responderam	0	0,0	0	0,0
Total de Respostas	8		45	

C18 – Quais considera terem sido as causas possíveis para a(s) violação(ões) à segurança do SI? (Assinale todos os itens aplicáveis)		
	Utilizadores finais	
	Nº	%
Ataque externo	3	4,7
Erro humano	34	53,1
Ataque interno	1	1,6
Perda acidental de equipamentos	18	28,1
Vírus ou outro código malicioso	7	10,9
Abuso de privilégios pelos colaboradores de TI	8	12,5
Procedimentos negligentes	44	68,8
Não sabe a causa	11	17,2
Não é aplicável	0	0,0
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	60	

C19 – Sem um sistema de segurança da informação a organização consegue saber o que deve ser protegido?		
	Gestores	
	Nº	%
Não	2	25,0
Não sabe	0	0,0
Sim	6	75,0
Não Responderam	0	0,0
Total de Respostas	8	

C19 – Já teve conhecimento de alguma(s) violação(ções) à segurança do SI da organização?		
	Técnicos	
	Nº	%
Não	12	26,7
Sim	33	73,3
Não Responderam	0	0,0
Total de Respostas	45	

C19 – Existe um departamento, com responsabilidades definidas, para lidar estrategicamente com segurança da informação?		
	Utilizadores finais	
	Nº	%
Não	1	0,6
Não sabe	11	6,7
Sim	148	91,3
Não Responderam	2	1,2
Total de Respostas	162	

C20 – O que a segurança da informação deve proteger?		
	Gestores	
	Nº	%
Ativos da organização de forma geral (proteger Pessoas, Hardware, Software e Informação)	8	100,0
Segurança da TIC (proteger, as aplicações, as base de dados e os sistemas operativos).	0	0,0
A Segurança da Informação (proteger a informação crítica de negócio nos seus vários suportes.	0	0,0
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	8	

C20 – Que atitude tomou quando presenciou essa(s) violação(ções)? (Assinale todos os itens aplicáveis)		
	Técnicos	
	Nº	%
Advertiu o(a) infrator(a)	12	36,4
Comunicou à gestão	20	60,6
Comunicou ao técnico de informática	6	18,2
Propôs medidas de solução para o problema	21	63,6
Comentou com os(as) seus(as) colegas	7	21,2
Nenhuma	3	9,1
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	33	

C20 – Qual é o departamento responsável pela estratégia da segurança da informação? (Assinale todos os itens aplicáveis)		
	Utilizadores finais	
	Nº	%
A gestão de topo	116	78,3
A direção	0	0,0
O departamento de informática	148	100,0
A chefia de cada departamento	1	0,6
Não sabe	2	1,3
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	148	

C21 – Sem um sistema de segurança da informação a organização consegue saber contra o que será necessário proteger?		
	Gestores	
	Nº	%
Não	2	25,0
Não sabe	0	0,0
Sim	6	75,0
Não Responderam	0	0,0
Total de Respostas	8	

C21 – Quais considera terem sido as causas possíveis para as violações à segurança do SI? (Assinale todos os itens aplicáveis)		
	Técnicos	
	Nº	%
Ataque interno	6	18,2
Ataque externo	11	33,3
Vulnerabilidades conhecidas em produtos comerciais (ex.: Windows)	4	12,1
Vulnerabilidades desconhecidas em produtos comerciais (ex.: Windows)	8	24,2
Vírus e worms por email	15	45,5
Aplicações ou serviços Web	10	30,3
Engenharia social	1	3,0
Erro humano	31	93,9
Perda acidental de equipamentos	16	48,5
Vírus ou outro código malicioso	19	57,6
Abuso de privilégios pelos colaboradores de TI	11	33,3
Procedimentos negligentes	30	90,9
Não sabe a causa	0	0,0
Não é aplicável	0	0,0
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	33	

C21 – Classifique relativamente à segurança da informação do SI (6 para muito importante e 1 para pouco importante) os seguintes aspetos:

C21.1 – Classifique os Utilizadores. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	0	0,0
3	2	1,2
4	6	3,7
5	28	17,3
6	126	77,8
Não Responderam	0	0,0
Total de Respostas	162	

C21.2 – Classifique os Técnicos de Informática. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	1	0,6
3	1	0,6
4	5	3,1
5	15	9,3
6	140	86,4
Não Responderam	0	0,0
Total de Respostas	162	

C21.3 – Classifique os Computadores Pessoais. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	0	0,0
3	4	2,5
4	9	5,6
5	28	17,2
6	120	74,1
Não Responderam	1	0,6
Total de Respostas	162	

C21.4 – Classifique os Periféricos. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	1	0,6
2	1	0,6
3	2	1,2
4	11	6,8
5	46	28,4
6	101	62,3
Não Responderam	0	0,0
Total de Respostas	162	

C21.5 – Classifique os Servidores. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	1	0,6
3	2	1,2
4	5	3,1
5	20	12,3
6	134	82,7
Não Responderam	0	0,0
Total de Respostas	162	

C21.6 – Classifique o(s) Software(s) aplicacional. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	7	4,3
5	23	14,2
6	132	81,5
Não Responderam	0	0,0
Total de Respostas	162	

C21.7 – Classifique o(s) Sistema(s) Operativo(s). (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	6	3,7
5	16	9,9
6	140	86,4
Não Responderam	0	0,0
Total de Respostas	162	

C21.8 – Classifique a(s) Base(s) de dados. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	3	1,9
5	14	8,6
6	145	89,5
Não Responderam	0	0,0
Total de Respostas	162	

C21.9 – Classifique a Internet. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	0	0,0
3	2	1,2
4	4	2,5
5	34	21,0
6	122	75,3
Não Responderam	0	0,0
Total de Respostas	162	

C21.10 – Classifique os Serviços na cloud. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	2	1,2
3	2	1,2
4	10	6,2
5	32	19,8
6	114	70,4
Não Responderam	2	1,2
Total de Respostas	162	

C21.11 – Classifique o Email. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	0	0,0
3	3	1,8
4	11	6,8
5	67	41,4
6	80	49,4
Não Responderam	1	0,6
Total de Respostas	162	

C21.12 – Classifique a Rede interna. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	5	3,1
5	38	23,5
6	119	73,5
Não Responderam	0	0,0
Total de Respostas	162	

C21.13 – Classifique o Sistema de telecomunicações. (6 para muito importante e 1 para pouco importante)		
	Utilizadores finais	
	Nº	%
1	0	0,0
2	0	0,0
3	1	0,6
4	44	27,2
5	48	29,6
6	69	42,6
Não Responderam	0	0,0
Total de Respostas	162	

C22 – Contra o que protege um sistema de segurança da informação? (Assinale todos os itens aplicáveis)		
	Gestores	
	Nº	%
Catástrofes naturais (Inundações, terramotos, sismos, etc.)	8	100,0
Ataques externos (eliminação, roubo, utilização indevida, etc.)	8	100,0
Ataques internos (eliminação, roubo, utilização indevida, etc.)	8	100,0
Vulnerabilidades/falhas nas instalações.	8	100,0
Vulnerabilidades/falhas na TIC.	8	100,0
Vulnerabilidades/falhas inerentes aos erros humanos.	8	100,0
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	8	

C22 – Existe um departamento, com responsabilidades definidas, para lidar estrategicamente com segurança da informação?		
	Técnicos	
	Nº	%
Não	0	0,0
Não sabes	0	0,0
Sim	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C23 – Já teve conhecimento de alguma(s) violação(ções) à segurança do SI da organização?		
	Gestores	
	Nº	%
Não	0	0,0
Sim	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C23 – Qual é o departamento responsáveis pela estratégia da segurança da informação? (Assinale todos os itens aplicáveis)		
	Técnicos	
	Nº	%
A gestão de topo	41	91,1
A direção	0	0,0
O departamento de informática	45	100,0
A chefia de cada departamento	0	0,0
Não sabe	0	0,0
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	45	

C24 – Que atitude tomou quando presenciou essa(s) violação(ções)? (Assinale todos os itens aplicáveis)		
	Gestores	
	Nº	%
Advertiu o(a) infrator(a)	1	12,5
Comunicou à gestão	0	0,0
Comunicou ao técnico de informática	0	0,0
Propôs medidas de solução para o problema	8	100,0
Comentou com os(as) seus(as) colegas	6	75,0
Aplicou um processo disciplinar ao(à) infrator(a)	0	0,0
Demitiu o(a) infrator(a)	0	0,0
Nenhuma	0	0,0
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	8	

C24 – Quais das seguintes tecnologias ou mecanismos estão implementadas no sistema de segurança? (Assinale todos os itens aplicáveis)		
	Técnicos	
	Nº	%
Antispyware	43	95,6
Sistema de detenção de intrusão	45	100,0
Controlo de acesso aos sistemas críticos da empresa;	42	93,3
Análise da segurança das estações de trabalho, desktops e notebooks	42	93,3
Análise da segurança física e lógica dos servidores de rede	42	93,3
Análise da segurança contra contaminação por vírus	44	
Avaliação da configuração do firewall	42	93,3
Criptografia de dados (e-mails e informações confidenciais)	44	97,8
Análise da Política de Backup	43	95,6
Análise da exigência de prevenção contra softwares não licenciados na empresa	43	95,6
Plano de Contingência	43	95,6
Análise da Política de Acesso dos funcionários à Internet	43	95,6
Política de Instalação de Software nas estações e na rede;	44	97,8
Processo de consciencialização de funcionários.	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25 – Quais considera terem sido as causas possíveis para as violações à segurança do SI? (Assinale todos os itens aplicáveis)		
	Gestores	
	Nº	%
Ataque interno	0	0,0
Ataque externo	1	12,5
Vulnerabilidades conhecidas em produtos comerciais (ex.: Windows)	1	12,5
Vulnerabilidades desconhecidas em produtos comerciais (ex.: Windows)	2	25,0
Vírus e worms por email	1	12,5
Aplicações ou serviços Web	1	12,5
Engenharia social	1	12,5
Erro humano	7	87,5
Perda acidental de equipamentos	2	25,0
Vírus ou outro código malicioso	2	25,0
Abuso de privilégios pelos colaboradores de TI	1	12,5
Procedimentos negligentes	8	100,0
Não sabe a causa	0	0,0
Não é aplicável	0	0,0
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	8	

C25 – Classifique relativamente à segurança da informação do SI (6 para muito importante e 1 para pouco importante) os seguintes aspetos:

C25.1 – Classifique os Gestores. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.2 – Classifique os Utilizadores. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.3 – Classifique os Técnicos de Informática. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.4 – Classifique os Computadores Pessoais. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.5 – Classifique os Periféricos. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.6 – Classifique os Servidores. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.7 – Classifique o(s) Software(s) aplicacional. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.8 – Classifique o(s) Sistema(s) Operativo(s). (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.9 – Classifique a(s) Base(s) de dados. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.10 – Classifique a Internet. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.11 – Classifique os Serviços na cloud. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.12 – Classifique o Email. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	1	2,2
6	45	97,8
Não Responderam	0	0,0
Total de Respostas	45	

C25.13 – Classifique a Rede interna. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	45	100,0
Não Responderam	0	0,0
Total de Respostas	45	

C25.14 – Classifique o Sistema de telecomunicações. (6 para muito importante e 1 para pouco importante)		
	Técnicos	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	7	15,6
6	38	84,4
Não Responderam	0	0,0
Total de Respostas	45	

C26 – Existe um departamento, com responsabilidades definidas, para lidar estrategicamente com segurança da informação?		
	Gestores	
	Nº	%
Não	0	0,0
Não sabe	0	0,0
Sim	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C27 – Qual é o departamento responsáveis pela estratégia da segurança da informação? (Assinale todos os itens aplicáveis)		
	Gestores	
	Nº	%
A gestão de topo	8	100,0
A direção	0	0,0
O departamento de informática	8	100,0
A chefia de cada departamento	0	0,0
Não sabe	0	0,0
Outro	0	0,0
Não Responderam	0	0,0
Total de Respostas	8	

C28 – Quais das seguintes tecnologias ou mecanismos estão implementadas no sistema de segurança? (Assinale todos os itens aplicáveis)		
	Gestores	
	Nº	%
Antispyware	8	100,0
Sistema de detenção de intrusão	8	100,0
Controlo de acesso aos sistemas críticos da empresa;	8	100,0
Análise da segurança das estações de trabalho, desktops e notebooks	8	100,0
Análise da segurança física e lógica dos servidores de rede	8	100,0
Análise da segurança contra contaminação por vírus	8	100,0
Avaliação da configuração do firewall	8	100,0
Criptografia de dados (e-mails e informações confidenciais)	8	100,0
Análise da Política de Backup	8	100,0
Análise da exigência de prevenção contra softwares não licenciados na empresa	8	100,0
Plano de Contingência	8	100,0
Análise da Política de Acesso dos funcionários à Internet	8	100,0
Política de Instalação de Software nas estações e na rede;	8	100,0
Processo de consciencialização de funcionários.	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	100,0

C29 – Classifique relativamente à segurança da informação do SI (6 para muito importante e 1 para pouco importante) os seguintes aspetos:

C29.1 – Classifique os Gestores. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.2 – Classifique os Utilizadores. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.3 – Classifique os Técnicos de Informática. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.4 – Classifique os Computadores Pessoais. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.5 – Classifique os Periféricos. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.6 – Classifique os Servidores. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.7 – Classifique o(s) Software(s) aplicacional. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.8 – Classifique o(s) Sistema(s) Operativo(s). (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.9 – Classifique a(s) Base(s) de dados. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.10 – Classifique a Internet. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.11 – Classifique os Serviços na cloud. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.12 – Classifique o Email. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	1	12,5
6	7	87,5
Não Responderam	0	0,0
Total de Respostas	8	

C29.13 – Classifique a Rede interna. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	0	0,0
6	8	100,0
Não Responderam	0	0,0
Total de Respostas	8	

C29.14 – Classifique o Sistema de telecomunicações. (6 para muito importante e 1 para pouco importante)		
	Gestores	
	Nº	%
1	0	0,0
2	0	0,0
3	0	0,0
4	0	0,0
5	1	12,5
6	7	87,5
Não Responderam	0	0,0
Total de Respostas	8	

D- Avaliar a satisfação da utilização do SI

D1 – Indique o grau de satisfação com as políticas de segurança da informação. (6 para muito satisfeito e 1 para pouco satisfeito)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	3	1,9
4	0	0,0	0	0,0	7	4,3
5	0	0,0	6	13,3	59	36,4
6	8	100,0	39	86,7	93	57,4
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

D2 - Satisfação com o SI enquanto software.

D2.1 – Expetativa Visual. (6 para fantástico e 1 para horrível)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	5	3,1
4	0	0,0	0	0,0	22	13,6
5	1	12,5	13	28,9	79	48,8
6	7	87,5	32	71,1	56	34,6
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

D2.2 – Adaptação ao software. (6 para fácil e 1 para difícil)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	1	0,6
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	2	1,2
4	0	0,0	0	0,0	10	6,2
5	0	0,0	3	6,7	18	11,1
6	8	100,0	42	93,3	131	80,9
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

D2.3 – Utilização do software. (6 para satisfatório e 1 para frustante)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	5	3,1
4	0	0,0	0	0,0	4	2,5
5	0	0,0	3	6,7	40	24,7
6	8	100,0	42	93,3	112	69,1
Não Responderam	0	0,0	0	0,0	1	0,6
Total de Respostas	8		45		162	

D2.4 – Capacidade do software. (6 para capacidade adequada e 1 para capacidade inadequada)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	4	2,5
4	0	0,0	0	0,0	4	2,5
5	0	0,0	8	17,8	60	37,0
6	8	100,0	37	82,2	92	56,8
Não Responderam	0	0,0	0	0,0	2	1,2
Total de Respostas	8		45		162	

D2.5 – Atratividade do software. (6 para estimulante e 1 para aborrecido)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	5	3,1
4	0	0,0	0	0,0	13	8,0
5	1	12,5	8	17,8	62	38,3
6	7	87,5	37	82,2	82	50,6
Não Responderam	0	0,0	0	0,0	0	0
Total de Respostas	8		45		162	

D2.6 – Flexibilidade do software. (6 para flexível e 1 para rígido)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	3	1,9
4	0	0,0	0	0,0	6	3,7
5	0	0,0	4	8,9	43	26,5
6	8	100,0	41	91,1	110	67,9
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

D3 - Satisfação com as Terminologia e informação do sistema.

D3.1 – Como avalia os termos usados no sistema? (6 para consistentes e 1 para inconsistentes)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	5	3,1
4	0	0,0	0	0,0	4	2,5
5	0	0,0	2	4,4	18	11,1
6	8	100,0	43	95,6	134	82,7
Não Responderam	0	0,0	0	0,0	1	0,6
Total de Respostas	8		45		162	

D3.2 – A terminologia do SI está relacionada com a tarefa que o utilizador está a realizar? (6 para sempre e 1 para nunca)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	5	3,1
4	0	0,0	0	0,0	7	4,3
5	0	0,0	2	4,4	26	16,1
6	8	100,0	43	95,6	123	75,9
Não Responderam	0	0,0	0	0,0	1	0,6
Total de Respostas	8		45		162	

D3.3 – Como avalia o posicionamento de mensagens no ecrã? (6 para consistentes e 1 para inconsistentes)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	1	0,6
3	0	0,0	0	0,0	5	3,1
4	0	0,0	0	0,0	7	4,3
5	0	0,0	1	2,2	18	11,1
6	8	100,0	44	97,8	130	80,2
Não Responderam	0	0,0	0	0,0	1	0,6
Total de Respostas	8		45		162	

D3.4 – O SI mantém o utilizador informado sobre o que está a fazer? (6 para sempre e 1 para nunca)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	3	1,9
4	0	0,0	0	0,0	4	2,5
5	0	0,0	2	4,4	31	19,1
6	8	100,0	43	95,6	122	75,3
Não Responderam	0	0,0	0	0,0	2	1,2
Total de Respostas	8		45		162	

D3.5 – Como avalia as mensagens de erro? (6 para úteis e 1 para inúteis)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	2	1,2
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	2	1,2
4	0	0,0	0	0,0	3	1,9
5	0	0,0	1	2,2	6	3,7
6	8	100,0	44	97,8	149	92,0
Não Responderam	0	0,0	0	0,0	2	1,2
Total de Respostas	8		45		162	

D4 - Satisfação com a Aprendizagem.

D4.1 – Como avalia a exploração de novos recursos do sistema por tentativas? (6 para fácil e 1 para difícil)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	3	1,9
2	0	0,0	0	0,0	16	9,9
3	0	0,0	0	0,0	10	6,2
4	0	0,0	0	0,0	22	13,6
5	0	0,0	17	37,8	33	20,4
6	8	100,0	28	62,2	78	48,1
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

D4.2 – Como avalia o processo de memorizar os termos e como utilizar os comandos? (6 para fácil e 1 para difícil)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	4	2,5
2	0	0,0	0	0,0	17	10,5
3	0	0,0	0	0,0	8	4,9
4	0	0,0	0	0,0	13	8,0
5	0	0,0	17	37,8	43	26,5
6	8	100,0	28	62,2	77	47,5
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

D4.3 – As tarefas podem ser realizadas de uma maneira direta? (6 para sempre e 1 para nunca)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	7	4,3
4	0	0,0	0	0,0	13	8,0
5	0	0,0	7	15,6	72	44,4
6	8	100,0	38	84,4	70	43,2
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

D4.4 – Como qualifica as mensagens de ajuda no ecrã? (6 para úteis e 1 para inúteis)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	3	1,9
4	0	0,0	0	0,0	2	1,2
5	0	0,0	2	4,4	12	7,4
6	8	100,0	43	95,6	144	88,9
Não Responderam	0	0,0	0	0,0	1	0,6
Total de Respostas	8		45		162	

D5 - Satisfação com a Capacidade do sistema.

D5.1 – Como avalia a velocidade do sistema? (6 para Demasiado lento e 1 para suficientemente rápido)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	1	0,6
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	1	0,6
4	0	0,0	0	0,0	7	4,3
5	0	0,0	1	8,9	66	40,7
6	8	100,0	41	91,1	87	53,7
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

D5.2 – Como avalia a fiabilidade do sistema? (6 para fiável e 1 para não fiável)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	1	0,6
4	0	0,0	0	0,0	8	4,9
5	0	0,0	2	4,4	41	25,3
6	8	100,0	43	95,6	112	69,1
Não Responderam	0	0,0	0	0,0	0	0,0
Total de Respostas	8		45		162	

D5.3 – As necessidades dos utilizadores com ou sem experiência são tomadas em consideração? (6 para sempre e 1 para nunca)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	1	0,6
3	0	0,0	0	0,0	2	1,2
4	0	0,0	0	0,0	12	7,4
5	0	0,0	3	6,7	51	31,5
6	8	100,0	42	93,3	95	58,6
Não Responderam	0	0,0	0	0,0	1	0,6
Total de Respostas	8		45		162	

D6 – Sobre os factores abaixo, qual é o nível de importância para avaliar satisfação do utilizador com o SI?										
Gestores										
	Sem importância		Pouco importante		Importante		Muito importante		Total	
	Nº	%	Nº	%	Nº	%	Nº	%	Nº	%
Reações ao Software	0	0,0	0	0,0	0	0,0	8	100	8	
Terminologia e informação do sistema	0	0,0	0	0,0	0	0,0	8	100	8	
Aprendizagem	0	0,0	0	0,0	0	0,0	8	100	8	
Capacidades do sistema	0	0,0	0	0,0	0	0,0	8	100	8	

D6 – Sobre os factores abaixo, qual é o nível de importância para avaliar satisfação do utilizador com o SI?										
Técnicos										
	Sem importância		Pouco importante		Importante		Muito importante		Total	
	Nº	%	Nº	%	Nº	%	Nº	%	Nº	%
Reações ao Software	0	0,0	0	0,0	2	4,4	43	95,6	45	
Terminologia e informação do sistema	0	0,0	0	0,0	1	2,2	44	97,8	45	
Aprendizagem	0	0,0	0	0,0	0	0,0	45	100	45	
Capacidades do sistema	0	0,0	0	0,0	0	0,0	45	100	45	

D6 – Sobre os factores abaixo, qual é o nível de importância para avaliar satisfação do utilizador com o SI?										
Utilizadores finais										
	Sem importância		Pouco importante		Importante		Muito importante		Total	
	Nº	%	Nº	%	Nº	%	Nº	%	Nº	%
Reações ao Software	0	0,0	6	3,7	49	30,2	107	66,0	162	
Terminologia e informação do sistema	0	0,0	0	0,0	45	27,8	117	72,2	162	
Aprendizagem	0	0,0	1	0,6	12	7,4	149	92,0	162	
Capacidades do sistema	0	0,0	0	1,2	13	8,0	147	90,7	162	

D7 – Quais são os fatores que levam o utilizador a ter confiança no SI? (Assinale todos os itens aplicáveis)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
O sistema é fácil de usar	8	100,0	43	95,6	153	94,4
É rápido de se trabalhar no sistema	8	100,0	44	97,8	139	85,8
Aumenta a produtividade do utilizador	8	100,0	41	91,1	143	88,3
Proporciona ao utilizador alcançar os objetivos estabelecidos	8	100,0	41	91,1	148	91,4
Trabalhar com o SI dá satisfação	8	100,0	45	100,0	137	84,6
Reduz os erros ao trabalhar no SI	8	100,0	37	82,2	147	90,7
Não Responderam	8	100,0	0	0,0	0	0,0
Total de Respostas	8	100,0	45		162	

D8 – Indique o grau de confiança que tem com o SI. (6 para confiança e 1 para desconfiança)						
	Gestores		Técnicos		Utilizadores finais	
	Nº	%	Nº	%	Nº	%
1	0	0,0	0	0,0	0	0,0
2	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	2	1,2
4	0	0,0	0	0,0	8	4,9
5	0	0,0	2	4,4	38	23,5
6	8	100,0	43	95,6	114	70,4
Não Responderam	0	0,0	0	0,0	1	0,6
Total de Respostas	8		45		162	