INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR

2017/2018

TII

AMEAÇAS E VULNERABILIDADES À SEGURANÇA DA INFORMAÇÃO DOS SISTEMAS DE INFORMAÇÃO DA FORÇA AÉREA. POLÍTICA DE SEGURANÇA E PREVENÇÃO.

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Sara Alexandra Magalhães Pereira Coimbra

CAP/TINF

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

AMEAÇAS E VULNERABILIDADES À SEGURANÇA DA INFORMAÇÃO DOS SISTEMAS DE INFORMAÇÃO DA FORÇA AÉREA. POLÍTICA DE SEGURANÇA E PREVENÇÃO.

CAP/TINF Sara Alexandra Magalhães Pereira Coimbra

Trabalho de Investigação Individual do CPOS-FA

Pedrouços 2018

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

AMEAÇAS E VULNERABILIDADES À SEGURANÇA DA INFORMAÇÃO DOS SISTEMAS DE INFORMAÇÃO DA FORÇA AÉREA. POLÍTICA DE SEGURANÇA E PREVENÇÃO.

CAP/TINF Sara Alexandra Magalhães Pereira Coimbra

Trabalho de Investigação Individual do CPOS-FA

Orientador: TCOR/ADMAER
Pedro Dinis Capinha Maio

Pedrouços 2018

Declaração de compromisso Antiplágio

Eu, Sara Alexandra Magalhães Pereira Coimbra, declaro por minha honra que o documento intitulado Ameaças e vulnerabilidades à Segurança da Informação dos Sistemas de Informação da Força Aérea. Política de Segurança e Prevenção corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do Curso de Promoção a Oficial Superior 2017/2018 no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, 19 de junho de 2018

Agradecimentos

Apesar deste trabalho ser designado de Trabalho de Investigação Individual teve o contributo de várias pessoas que, direta ou indiretamente, contribuíram para a sua realização ao longo de todo o curso e, por isso, devem ser reconhecidas.

Desta forma agradeço, em primeiro lugar, ao meu orientador, TCor Pedro Maio, por toda a disponibilidade, acompanhamento e, principalmente, paciência ao longo deste percurso.

Aos entrevistados, BGen José Morgado, Cor Ana Telha, TCor José Mendes, TCor Veiga Lopes, e respetivos colaboradores, pelo tempo dispendido nas entrevistas, assim como a todos os que responderam ao questionário que foi disponibilizado, contribuindo para que o objetivo deste trabalho fosse alcançado.

Ao Ten Passeiro que, apesar de não ser citado diretamente ao longo do trabalho, muito me ajudou no esclarecimento de alguns conceitos mais técnicos.

Aos meus camaradas de curso, Força Aérea e Conjunto, por terem feito com que este caminho fosse mais fácil de percorrer.

À minha família que se viu muitas vezes privada da minha companhia, principalmente à minha mãe pelas muitas "quintas-feiras" e saborosas refeições.

Ao meu marido, por ter "aguentado as pontas" durante estes nove meses demonstrando ser um verdadeiro companheiro.

E, em último lugar mas não menos importante, à minha filhota linda, Matilde, que apesar de muito nova demostrou uma verdadeira compreensão pelas vezes em que eu não podia estar com ela. O seu sorriso e alegria foram muitas vezes a motivação para prosseguir e dar sempre o meu melhor.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

A Informação é um bem vital para qualquer organização e na Força Aérea não é exceção. Assim, é imperioso garantir a proteção dos sistemas de informação (SI) responsáveis pelo armazenamento, processamento e transmissão da informação dentro da organização de modo a respeitar os princípios de confidencialidade, integridade e disponibilidade, assegurando assim a Segurança da Informação.

Apesar de existirem várias ameaças, diretamente relacionadas com os níveis de proteção dos SI, o elemento mais vulnerável de um SI é o próprio utilizador.

A adoção de uma política de segurança e prevenção que inclua mecanismos e medidas de segurança pode contribuir para minimizar esta ameaça.

Neste âmbito, e de modo a compreender melhor esta temática, procedeu-se a um enquadramento teórico através de um levantamento bibliográfico e, posteriormente, foram realizadas entrevistas a algumas pessoas chave na organização e um questionário aos utilizadores dos SI desenvolvidos na Força Aérea.

Com esta investigação foi possível concluir que a prevenção é a base da Segurança da Informação. A adoção de medidas de segurança e prevenção por parte dos utilizadores dos SI, bem como o recurso a mecanismos de segurança, contribui efetivamente para a Segurança da Informação dos SI desenvolvidos internamente.

Palavras-chave

Segurança da Informação, Prevenção, Sistema de Informação, Garantia da Informação, *Awareness*

Abstract

Information is a vital asset to any organization and in the Portuguese Air Force is no exception. Therefore, it is essential to ensure the protection of information systems (IS) responsible for the storage, processing and transmission of information within the organization in order to guarantee the principles of confidentiality, integrity and availability, ensuring the Information Security.

Even though there are several threats related to the IS protection levels, the weakest element is the user himself.

The adoption of a security and prevention policy that includes security mechanisms and measures can help minimize this threat.

Given the background, and in order to better understand this subject, a theoretical framework was conducted through a bibliographical survey followed by interviews to some key players in the organization and a questionnaire to users of the IS developed in the Air Force.

With this investigation it was possible to conclude that prevention is the basis of Information security. The adoption of prevention and security measures from IS users, as well as the use of security mechanisms, contributes effectively for the information security of the internally developed IS.

Keywords

Information Security, Prevention, Information Systems, Information Assurance, Awareness

Lista de abreviaturas, siglas e acrónimos

CEMFA – Chefe do Estado-Maior da Força Aérea

CNCS – Centro Nacional de Cibersegurança

DCSI – Direção de Comunicações e Sistemas de Informação

DIVCSI – Divisão de Comunicações e Sistemas de Informação

DoS – *Denial of Service*

FA – Força Aérea

H – Hipótese

IDS – *Intrusion Detection Systems*

IPS – *Intrusion Prevention Systems*

IUM – Instituto Universitário Militar

OE – Objetivo Específico

PD – Pergunta Derivada

PP – Pergunta de Partida

RFA – Regulamento da Força Aérea

RSI – Repartição de Sistemas de Informação

RTI – Repartição de Tecnologias de Informação

SI – Sistemas de Informação

SIC – Sistemas de Informação e Comunicações

TIC – Tecnologias da Informação e Comunicações

TII – Trabalho de Investigação Individual

USB – *Universal Serial Bus*

Introdução

"A segurança continua a ser uma prioridade
de todos os povos, de todas as nações!"
(Tomé, 2018)

Num mundo cada vez mais digital e eletrónico, "(…) as redes e os sistemas e serviços de informação desempenham um papel vital na sociedade (…)" (UE, 2016), sendo naturalmente exigido que a informação esteja sempre disponível de uma forma rápida, íntegra e confidencial e que existam sistemas e tecnologias de informação que garantam a proteção dos Sistemas de Informação (SI) "(…) contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, […] incluindo as medidas necessárias para detetar e contrariar tais ameaças" (APDSI, 2017).

Caraterísticas como a confidencialidade, a integridade e a disponibilidade da informação são consideradas como essenciais e a perda de uma delas representa uma ameaça à Segurança da Informação de um SI, sendo de extrema importância a existência de mecanismos e medidas que as assegurem.

As ameaças aos SI, e consequentemente à informação que estes sistemas são responsáveis por armazenar, tratar e/ou alterar, podem ter várias origens e, analogamente, vários níveis de proteção: Tecnológico, Humano e Organizacional (Rodrigues, 2016). Contudo, quando se pensa em Segurança da Informação, o fator humano surge "(...) como um dos principais elementos a considerar […] para manutenção da segurança do SI, independentemente da sofisticação e preço dos meios e dispositivos disponibilizados" (Carneiro, 2002, cit. por Gaivéo, 2008, p. 139).

Decorrente da orientação do Chefe do Estado-Maior da Força Aérea (CEMFA) sobre a importância da Informação como um recurso organizacional no apoio à missão e à tomada de decisão, devendo ser aplicadas um "(…) conjunto de medidas destinadas a obter um determinado nível de confiança e protecção nos Sistemas de Informação e Comunicações (SIC) e na informação por estes armazenada, processada ou transmitida" (CEMFA, 2008), justifica-se um trabalho de investigação individual (TII) que analise de que forma a existência de medidas de segurança e prevenção pode minimizar o risco de ameaças à Segurança da Informação dos SI desenvolvidos na Força Aérea (FA), com origem nos seus utilizadores, de modo a evitar futuras ocorrências que a possam comprometer.

Neste sentido, o âmbito deste TII é delimitado aos SI desenvolvidos na FA e seus utilizadores, ocorrendo em três domínios distintos: tempo (atualidade), espaço (FA) e conteúdo (Segurança da Informação na FA).

Esta investigação permitirá à Direção de Comunicações e Sistemas de Informação (DCSI) perceber de que forma os utilizadores dos SI desenvolvidos na FA estão consciencializados sobre a Segurança da Informação de modo a melhorar a atual Segurança da Informação na organização.

Para tal, o presente trabalho tem os seguintes objetivos:

- Objetivo geral: analisar de que modo se pode minimizar o risco de ameaça à Segurança da Informação dos SI desenvolvidos na FA, com origem nos seus utilizadores, através da adoção de medidas de segurança e prevenção.
- Objetivos específicos (OE): OE1 – Verificar a existência de mecanismos de segurança que assegurem os princípios da Segurança da Informação na FA. OE2 – Analisar a adoção de medidas de segurança por parte dos utilizadores dos SI desenvolvidos na FA; OE3 – Analisar o nível de consciencialização dos utilizadores dos SI desenvolvidos na FA, relativamente à Segurança da Informação.

Assim, formulou-se a seguinte pergunta de partida que serviu de fio condutor à investigação: De que forma a adoção de uma política de segurança e prevenção pode contribuir para a Segurança da Informação dos SI desenvolvidos na FA, de modo a minimizar o risco de uma ameaça com origem nos seus utilizadores?

Para obter a resposta à pergunta de partida, a base da investigação assenta numa variada bibliografia, nacional e estrangeira, que permite esclarecer alguns conceitos, tendo sido também efetuadas entrevistas semiestruturadas e um questionário a todos os militares e civis da FA.

O percurso metodológico seguido neste trabalho passa pelas fases exploratória, analítica e conclusiva (IESM, 2015), sendo que a investigação segue o método hipotético-dedutivo.

Este trabalho está organizado de acordo com o referido na NEP/ACA 018, ponto 3, de setembro de 2015, e dividido em três partes: introdução, corpo e conclusão (IESM, 2015).

A introdução, que diz respeito ao presente capítulo, onde é feito o enquadramento e justificação do tema, apresentados os objetivos e questão principal da investigação, bem como uma breve síntese da metodologia seguida.

O corpo do trabalho é composto por três capítulos. No primeiro capítulo efetua-se a revisão da literatura e estado da arte do objeto de estudo, através de um enquadramento teórico relacionado com a Segurança da Informação. Neste capítulo é igualmente feita referência à metodologia seguida e ao Modelo de Análise. Nos segundo e terceiro capítulos é feita a análise do estudo de caso deste trabalho, sendo o segundo dedicado aos mecanismos de segurança na FA e o terceiro, maioritariamente, à análise dos resultados obtidos no questionário sobre a Segurança da Informação e os utilizadores na FA.

Por fim, a conclusão do trabalho compreende um sumário dos aspetos mais relevantes identificados ao longo da investigação, avaliação dos resultados obtidos (em relação aos objetivos, pergunta de partida, derivadas e respetivas hipóteses), contributo do trabalho para o conhecimento, limitações que possam ter surgido e recomendações para trabalhos futuros.

1. Revisão da literatura e modelo de análise

"A Informação é um recurso organizacional de vital importância para a Força Aérea, no apoio à missão e à tomada de decisão (…)" (CEMFA, 2008), existindo atualmente cerca de 59 SI desenvolvidos internamente, que vão desde a componente pessoal à operacional, passando pela financeira, inspeção, logística e material, entre outros (CEMFA, 2015), englobando praticamente toda a informação existente na FA, com cerca de 7176 utilizadores registados, sendo 6595 efetivos[1] (Lopes, 2018).

1.1. Segurança da Informação

O objetivo da segurança dentro de uma organização é o de proteger os seus bens garantindo e assegurando a "(…) continuidade das suas actividades, reduzindo o efeito das possíveis ameaças através da minimização dos impactos decorrentes das quebras de segurança." (Garcia, 2002), e, num mundo cada vez mais digital e eletrónico, "(…) as redes e os sistemas e serviços de informação desempenham um papel vital na sociedade (…)" de modo que a "(…) sua fiabilidade e segurança são essenciais (…)" (UE, 2016). Deste modo, é naturalmente exigido que a informação esteja sempre disponível de uma forma rápida, íntegra e confidencial e que, consequentemente, existam mecanismos e medidas de segurança capazes de garantir estes três fatores, ou seja a Segurança da Informação.

De facto a importância da informação e da Segurança da Informação nos dias de hoje é indiscutível e considerada como um bem essencial para qualquer organização, " (…) em especial para a militar (…)", devendo ser "(…) mitigado o risco de recolha de informação através do ciberespaço por parte de um adversário (…)", que em qualquer lugar do mundo e a qualquer momento pode " (…) explorar as vulnerabilidades dos componentes principais dos seus Sistemas de Informação" (J. Martins et al., 2016, p. 143).

O Centro Nacional de Cibersegurança (CNCS) define Segurança da Informação como "(…) um processo organizado e estruturado que permite preservar a confidencialidade, integridade e a disponibilidade da informação" (CNCS, 2017).

1.1.1. Princípios da Segurança da Informação

Para Mamede (2006, p. 9), a segurança em sistemas informáticos e, analogamente, a segurança dos sistemas de informação, engloba três aspetos essenciais: a confidencialidade, a integridade e a disponibilidade.

[1] A 4 de janeiro de 2018.

Estes três aspetos formam a conhecida tríade da Segurança da Informação, CIA[2] (INFOSEC, s.d.) e são reconhecidos como os Princípios da Segurança da Informação:

- Confidencialidade**,** "é assegurar que a informação é acessível somente por pessoas devidamente autorizadas. O acesso à informação é restrito a utilizadores legítimos." (CNCS, 2017a).
- Integridade, "é garantir a veracidade e complementaridade da informação, bem como os seus métodos de processamento. O conteúdo da informação não pode ser modificado de forma inesperada." (CNCS, 2017a).
- Disponibilidade, "é assegurar o acesso à informação e bens associados por quem devidamente autorizado. A informação deve estar acessível sempre que necessário." (CNCS, 2017a).

A Segurança da Informação, também designada como *Information Security*, resulta assim da aplicação de um conjunto de medidas de segurança com o objetivo de garantir a proteção da informação contra a perda de um dos seus três princípios, assim como dos próprios sistemas que processam, armazenam e transmitem essa informação (CEMFA, 2011a), prevenindo possíveis ameaças à mesma.

1.1.2. Ameaça e Vulnerabilidade - O elemento humano

A vulnerabilidade é a "(…) fraqueza de um sistema informático, revelada por um exame à sua segurança (por exemplo, devido a falhas na análise, conceção, implementação ou operação), que se traduz por uma incapacidade de fazer frente às ameaças informáticas que pesam sobre ele." (CNCS, 2017b), sendo uma ameaça a "(…) causa potencial de incidente indesejável que pode resultar em danos para uma organização ou qualquer dos sistemas por ela utilizados. Estas ameaças podem ser acidentais ou deliberadas (com dolo) e caracterizam-se por elementos ameaçadores, alvos potenciais e métodos de ataque." (CNCS, 2017b).

Assim, e de acordo com o tema deste trabalho, entende-se por ameaça o potencial comprometimento da Segurança da Informação, seja ele acidental ou deliberado, e por vulnerabilidade a existência de uma fraqueza ou a falta de controlo do SI que poderá permitir

[2] Esta sigla corresponde, em inglês, a cada um dos Princípios da Segurança da Informação: Confidencialidade (*Confidentiality*), Integridade (*Integrity*) e Disponibilidade (*Availability*).

ou facilitar a atuação de ameaça (CEMFA, 2008). Uma ameaça pode explorar acidental ou propositadamente uma determinada vulnerabilidade e pode ter origem interna ou externa, estando diretamente relacionada com a perda de um dos seus princípios.

Existe perda de confidencialidade quando há uma quebra de sigilo de uma determinada informação, por exemplo a divulgação de senhas de acesso a um SI, permitindo que fiquem expostas informações restritas.

Um utilizador deixar o computador desbloqueado é uma ameaça à Segurança da Informação porque permite que determinada informação fique exposta e sujeita a alterações por uma pessoa não autorizada, havendo a perda da integridade dessa informação.

Quando a informação deixa de estar acessível por quem dela necessita existe perda de disponibilidade. É o caso de um ataque à prestação de serviços (DoS – *Denial of Service*) em que uma máquina pode ficar numa situação de impossibilidade de prestar um determinado serviço (Zúquete, 2013, p 20).

De modo a garantir a Segurança da Informação ou, pelo menos, minimizar o risco de perda destes princípios, devem-se "(…) identificar os elementos mais fracos do sistema que se pretende seguro e desenhar soluções adequadas (…)" (Mamede, 2006, p.3).

Apesar de ainda existir uma certa tendência para se considerarem as ameaças a nível tecnológico através da implementação de medidas de proteção assentes, por exemplo, em *antivírus*[3] e *firewall*[4], "o elemento humano é, por definição, o elemento mais fraco de um sistema de informação" (Rodrigues, 2016), ficando assim identificado o tal elemento mais fraco de um sistema que Mamede (2006) considerava ser fundamental definir.

Esta ideia é reforçada por Garcia (2002) que escreve que muitas vezes se julga que "(…) as ameaças à segurança vêm principalmente do exterior (…)" porém, "(…) os maiores perigos e os que provocam danos superiores aos sistemas são aqueles que surgem no interior da organização, por pessoas internas, por causa da má formação ou mesmo por descuido ou desconhecimento".

[3] Vírus – "Classe de software malicioso que tem a capacidade de se auto-replicar e "infetar" partes do sistema operativo ou de outros programas, com o intuito de causar a perda ou alteração da informação." (CNCS, 2017b). Por oposição, antivírus é a ferramenta que impedirá que um SI seja "afetado" por um vírus informático.

[4] *Firewall* – "(…) sistema informático concebido para proteger uma rede de computadores do acesso externo de utilizadores não autorizados." (CNCS, 2017b).

1.1.3. Política de segurança e prevenção

Uma política de segurança diz respeito ao conjunto de normas, indicações ou instruções a seguir, com o objetivo de prevenir a ocorrência de incidentes (ameaças) relacionados com a Segurança da Informação (Arthur, 2009), sendo a prevenção, a "(…) capacidade de proteger a informação e os sistemas que a processam da perda da Confidencialidade, Integridade e Disponibilidade." (CEMFA, 2011a).

Na FA, o Regulamento da Força Aérea (RFA) 390-3, Política de Segurança da Informação e dos Sistemas de Informação e Comunicações na Força Aérea, "(…) destina-se a estabelecer a Política de Segurança, assim como os requisitos considerados mínimos […] para a protecção da informação classificada (…)" (CEMFA, 2008), todavia os SI desenvolvidos na FA não têm qualquer acreditação de segurança (Lopes, 2018). No entanto, o RFA 390-6, Política de Ciberdefesa da Força Aérea, refere que os princípios contidos neste regulamento "(…) aplicam-se a todos os sistemas de informação e comunicações da Força Aérea e à informação neles contida (…)" devendo ser implementadas as necessárias medidas de segurança que assegurem a "(…) proteção da informação armazenada, processada e transmitida por esses sistemas (…)" (CEMFA, 2011).

Desta forma, as políticas de segurança referem-se, essencialmente, aos requisitos que devem ser cumpridos de modo a garantir a Segurança da Informação, enquanto que os mecanismos de segurança dizem respeito à "(…) tecnologia que permite pôr em prática as políticas de segurança" (Zúquete, 2013, p. 10).

1.1.4. Mecanismos de Segurança

Segundo Zúquete (2013, p. 15), os mecanismos de segurança, ao contrário das políticas de segurança que se baseiam em regras limitadas e atividades estáveis ao longo do tempo, poderão estar constantemente em evolução derivado do surgimento de novos mecanismos de segurança mais modernos e mais seguros que os anteriores, ou mesmo para colmatar novas vulnerabilidades descobertas, sendo quase impossível apresentar uma lista atualizada com todos os mecanismos de segurança.

No entanto, é possível identificar alguns mecanismos de segurança, ou ferramentas, considerados como essenciais para a manutenção da Segurança da Informação (Zúquete, 2013, pp. 16-18; Júnior, 2005):

- Mecanismos de filtragem, servem para identificar atividades não autorizadas e evitar a sua realização (ex. existência de programas antivírus);

- Mecanismos de confinamento, criando barreiras de segurança (ex. *firewall*);
- Mecanismos de controlo de acesso, permitem verificar se um utilizador pode ou não realizar uma determinada ação sobre um determinado objeto (ex. autenticação através do binómio utilizador + senha, para aceder a um computador);
- Mecanismos de inspeção, com o objetivo de detetar alguma atividade não esperada, ilegal ou ilícita (ex. sistemas de deteção de intrusões – IDS (*Intrusion Detection Systems*));
- Algoritmos criptográficos que permitem garantir a confidencialidade;
- Utilização de código *Checksum* de modo a verificar a integridade dos dados;
- *Backups* que, no caso de ataques à prestação de serviços (DoS), garantem que a informação foi guardada assegurando o princípio da disponibilidade.

1.1.5. Medidas de Segurança e Prevenção

Para Mamede (2006, p.3), o termo segurança está relacionado com ameaças, sua prevenção e minimização, sendo essencial que exista numa organização capacidade para se tomarem medidas preventivas capazes de evitar ocorrências indesejadas, maliciosas ou imprevistas ou, caso não seja possível, minimizar essas mesmas ocorrências, sendo primordial a "(…) a prevenção e detecção de acções não autorizadas por utilizadores de sistemas de computadores" (Mamede, 2006, p.10).

Desta forma, além dos mecanismos de segurança já referidos, numa organização os utilizadores devem adotar as seguintes medidas de segurança e prevenção, entre outras, no seu posto de trabalho (Pimenta e Quaresma, 2016; Rhee, Kim e Ryu, 2009):

- Efetuar as atualizações de segurança recomendadas;
- Realizar cópias de segurança com regularidade;
- Não partilhar a informação do computador com outras pessoas;
- Ser cuidadoso na utilização de equipamentos de armazenamento externos;
- Bloquear o computador quando se ausentar;
- Utilizar senhas robustas e diferentes em cada aplicação;
- Não compartilhar ou divulgar as suas senhas com outras pessoas;
- Ser responsável e cuidadoso na utilização da Internet e do correio eletrónico;
- Informar no caso de incidentes estranhos.

Estes autores consideram essencial que os utilizadores estejam cientes de quais as medidas de segurança a adotar como contributo para a Segurança da Informação dos SI.

O descuido ou desconhecimento por parte dos utilizadores de SI, em relação às medidas a adotar para garantir a Segurança da Informação, poderão refletir-se como um risco, ou seja, como uma maior "probabilidade do grau de exposição a uma ameaça à informação e/ou aos sistemas de uma organização" (CEMFA, 2011).

Pimenta e Quaresma (2016) acrescentam ainda que além da "(…) criação e divulgação de um conjunto de boas práticas e comportamentos que sejam percebidos e adotados por todos os elementos da organização (…)", as organizações devem motivar os utilizadores a aplicá-las, através de ações de sensibilização que lhes mostrem como eles poderão provocar "(…) vulnerabilidades e, consequentemente, ataques aos SI da organização (…)".

1.1.6. *Awareness*

Os recursos humanos desempenham um papel fundamental pois são eles que formulam e executam as políticas de segurança numa organização. Por isso, é essencial a formação e o treino apropriados destes elementos para poderem prevenir, detetar e agir, de forma adequada, perante uma ameaça à Segurança da Informação que poderá resultar na perda de um dos seus princípios, confidencialidade, integridade ou disponibilidade.

O conceito *Awareness* está relacionado com a consciência que um utilizador de um SI deve ter sobre o papel que desempenha na Segurança da Informação dos SI, ou seja, estar ciente e atento a tudo o que pode implicar uma ameaça, incluindo ele próprio, prevendo futuras quebras à mesma. Esta ameaça pode ser minimizada com a adoção de medidas de segurança preventivas por parte dos utilizadores.

De facto, o conhecimento por parte dos utilizadores de quais as medidas de segurança que devem adotar, pode "(…) contribuir fortemente para uma tomada de consciência e sensibilização global para as questões da segurança." (Mamede, 2006, p.23), minimizando o risco de uma ameaça à Segurança da Informação dos SI por parte dos seus utilizadores.

A FA já está ciente e compartilha da importância da Segurança da Informação e do papel vital que os utilizadores têm para garantir a mesma, referindo que a "(…) formação adequada em Segurança da Informação, para todos os responsáveis pelo estudo, implementação e operação dos SIC, bem como dos utilizadores finais, é um aspecto fundamental na protecção dos mesmos, devendo constituir um requisito essencial (…)" (CEMFA, 2008).

1.2. Metodologia seguida

A escolha de uma metodologia adequada é um passo importante e que deve ser tomado antes de se iniciar a investigação, sendo essencial analisar a "forma como o investigador se posiciona face ao seu objeto de investigação (…)" (Slife e Williams, 1995; Marsh e Furlong, 2002, cit. por Santos, et al., 2016, p. 15), uma vez que a sua perspetiva pode influenciar o desenrolar da investigação.

Para tal, houve necessidade de efetuar um posicionamento filosófico concluindo-se que se pretende uma investigação objetiva de modo a compreender vários conceitos associados à Segurança da Informação e à forma como os utilizadores de SI podem significar uma ameaça.

No que toca à epistemologia, entende-se que o positivismo é a visão mais adequada para validar esta investigação, já que esta "teoria permite gerar hipóteses, que podem ser testadas (…)" possibilitando, ou não, confirmá-las "(…) através da recolha empírica de factos que servem de base (…)" (Santos, et al., 2016, p. 19) à sua análise.

Seguindo o estipulado na NEP/ACA-010, ponto 5, de 15 de setembro de 2015 (IESM, 2015), o percurso metodológico seguido neste trabalho passa por três fases:

(i) A fase exploratória, de extrema importância para o percurso deste trabalho de investigação uma vez que "(…) condicionará o valor e a credibilidade da informação e do conhecimento produzido neste processo (…)" (Santos, et al., 2016, p. 43), permitiu a delimitação do tema no tempo, espaço e conteúdo, sendo que no tempo considerou-se a atualidade, o espaço a FA e o conteúdo restrito à Segurança da Informação dos SI desenvolvidos na FA.

Relativamente às "formas de raciocínio que podem ser adotadas durante a investigação" (Freixo, 2011, cit. por Santos, et al., 2016, p. 20), entende-se que nesta investigação está em causa o raciocínio hipotético-dedutivo, uma vez que "(…) só a partir de uma teoria é possível formular as questões que pretendemos estudar, as quais, por sua vez, irão determinar o tipo de dados a observar." (Popper, 2006, cit. por Santos, et al., 2016, p.22). Assim foram formuladas, como guia da investigação, as questões (pergunta principal e derivadas) e respetivas teorias (hipóteses).

De acordo com o posicionamento filosófico e o tipo de raciocínio escolhido, considera-se que para a realização deste TII seguir-se-á uma estratégia de investigação qualitativa pois pretende-se compreender que medidas de segurança e prevenção podem contribuir para a Segurança da Informação dos SI desenvolvidos na FA, pela interpretação de dados

recolhidos através de entrevistas semiestruturadas, de literatura existente, e da "(…) exploração do comportamento, das perspetivas e das experiências dos indivíduos estudados, alcançar uma interpretação da realidade social" (Vilelas, 2009, p. 105, cit. por Santos, et al., 2016, p. 29). Para se compreender de que modo o comportamento dos utilizadores dos SI desenvolvidos na FA pode contribuir para a Segurança da Informação na FA, recorrer-se-á a uma estratégia quantitativa, com "(…) recolha de dados observáveis e quantificáveis (…)" (Santos, et al., 2016, p. 27), através da realização de um questionário aos utilizadores dos SI da FA.

Apesar de se utilizarem diferentes estratégias para a recolha e interpretação dos dados a investigar no presente trabalho, reforça-se que a estratégia seguida neste trabalho é qualitativa uma vez que, independentemente do método de recolha, a "(…) interpretação dos fenómenos sociais e a atribuição dos respectivos significados é feita a partir de padrões encontrados nos dados" (Vilelas, 2009, p. 105, cit. por Santos, et al., 2016, p. 29).

Quanto ao desenho de pesquisa utilizado neste TII, enquadra-se num estudo de caso, nomeadamente na análise da adoção de medidas de segurança e prevenção de modo a minimizar o risco de uma ameaça à Segurança da Informação dos SI desenvolvidos na FA, com origem nos seus utilizadores.

Após identificado o problema surge a pergunta de partida que serviu de fio condutor à investigação: De que forma a adoção de uma política de segurança e prevenção pode contribuir para a Segurança da Informação dos SI desenvolvidos na FA, de modo a minimizar o risco de uma ameaça com origem nos seus utilizadores?

(ii) A fase analítica onde é feita a recolha, análise e apresentação dos dados obtidos através de entrevistas semiestruturadas, da análise documental e de um questionário realizado aos utilizadores dos SI desenvolvidos na FA composto por várias questões relacionadas sobre a Segurança da Informação.

(iii) Finalmente, na fase conclusiva, a avaliação e discussão sobre os resultados obtidos na fase anterior.

1.2.1. Modelo de Análise

A construção de um modelo de análise coeso assenta num conjunto de hipóteses, coerentes e interligadas entre si, permitindo estabelecer relações entre os conceitos apresentados no quadro teórico de modo a fundamentar a investigação (Pardal e Correia, 1995, cit. por Santos, et al., 2016, p. 43).

Após a fase exploratória optou-se pela análise de variados documentos que permitiram a construção do modelo de análise desta investigação, constituído pela pergunta de partida (PP), perguntas derivadas (PD) e respetivas hipóteses (H), e conceitos utilizados para a realização do presente estudo. A Tabela n.º 1 diz respeito ao modelo de análise com os referidos fatores. O modelo de análise completo encontra-se no Apêndice A.

Tabela 1 – Modelo de Análise

Pergunta de partida (PP)	Perguntas derivadas (PD)	Hipóteses (H)	Conceitos
PP: De que forma a adoção de uma política de segurança e prevenção pode contribuir para a Segurança da Informação dos SI desenvolvidos na FA, de modo a minimizar o risco de uma ameaça com origem nos seus utilizadores?	**PD1:** De que maneira o recurso a mecanismos de segurança contribui para a Segurança da Informação na FA?	**H1:** O recurso a mecanismos de segurança contribui, como medida de segurança e prevenção, para a Garantia da Informação dos SI desenvolvidos na FA	Prevenção Garantia da Informação
			Mecanismos de Segurança
	PD2: Em que medida os utilizadores dos SI desenvolvidos na FA podem contribuir para a Segurança da Informação na FA?	**H2:** A adoção de medidas de segurança e prevenção por parte dos utilizadores dos SI desenvolvidos na FA, contribui para a Segurança da Informação na FA.	Medidas de Segurança e Prevenção
		H3: A consciencialização (Awareness) dos utilizadores dos SI desenvolvidos na FA, relativamente ao comportamento a adotar, contribui como medida de segurança e prevenção para a Segurança da Informação na FA.	Awareness

Fonte: (Autora, 2018)

De modo a validar as hipóteses e respetivas PD recorreu-se aos principais meios de recolha de informação: a entrevista, a observação e o questionário (Freixo, 2011, cit. por Santos, et al., 2016, p. 74), complementando-os com a análise documental.

O questionário foi realizado a todos os militares e civis utilizadores de SI desenvolvidos na FA, enquanto que as entrevistas, de carácter semiestruturado, foram realizadas às seguintes entidades:

- Diretor da DCSI;
- Chefe da Divisão de Comunicações e Sistemas de Informação (DIVCSI);
- Chefe da Repartição de Tecnologias de Informação (RTI);
- Chefe da Repartição de Sistemas de Informação (RSI).

Os conceitos utilizados ao longo do trabalho são os seguintes:

- **Prevenção** – proteger a informação e os sistemas que a processam da perda de um dos Princípios da Segurança da Informação: Confidencialidade, Integridade e Disponibilidade (CEMFA, 2011a);
- **Garantia da Informação** – aplicação de um conjunto de medidas de segurança de modo a salvaguardar os Princípios da Segurança da Informação (CEMFA, 2011a);
- **Mecanismos de Segurança** – tecnologia que permite colocar em prática os requisitos que devem ser cumpridos de modo a garantir a Segurança da Informação (Zúquete, 2010, p. 10);
- **Medidas de Segurança e Prevenção** – medidas preventivas capazes de evitar, ou pelo menos minimizar, ocorrências indesejadas, maliciosas ou imprevistas que comprometam a Segurança da Informação (Mamede, 2006, p.3);
- ***Awareness*** – estímulo ou motivação por parte de um utilizador de SI sobre o seu papel para a Segurança da Informação na FA, assim como o conhecimento de quais as medidas de segurança e prevenção a adotar (Peltier, 2005, cit. por Francisco, 2016).

2. O recurso a mecanismos de segurança na FA

A fase exploratória deste TII permitiu identificar alguns dos mecanismos de segurança que devem ser utilizados de modo a assegurar a Segurança da Informação dos SI desenvolvidos na FA.

Partindo desta linha foram realizadas algumas entrevistas para, em paralelo com uma análise documental, investigar de que maneira o recurso a mecanismos de segurança pode contribuir, como medida de segurança e prevenção, para a Garantia da Informação dos SI desenvolvidos na FA.

O primeiro passo foi tentar perceber de que forma a FA, através dos órgãos considerados competentes, encara a Segurança da Informação dentro da organização.

O RFA 390-6 menciona que uma eficiente estratégia de prevenção deve conter vários mecanismos de defesa, também referenciados como conceito de "Defesa em Profundidade", que abrangem as várias componentes da segurança, que vão desde a Segurança Física à Segurança da Informação propriamente dita (CEMFA, 2011a). Este conceito refere a prevenção como um dos pilares da Ciberdefesa[5] e a política de segurança como uma das bases onde esta deve assentar (CEMFA, 2011a), de modo a assegurar a Garantia da Informação. O diretor da DCSI cita igualmente este regulamento quando refere que a FA "(…) tem como objetivo […] cumprir o princípio de defesa em profundidade […] através da implementação/edificação de diversas barreiras de segurança informática para proteção dos SI" (Morgado, 2018).

A prevenção e a segurança da informação dos SI é considerada, então, uma prioridade para a FA devendo ser tomadas as medidas necessárias para garantir os Princípios da Segurança da Informação.

A existência de *software* antivírus atualizado, sistemas de Deteção/Prevenção de Intrusão (IDS/IPS), dispositivos que protejam as nossas fronteiras (*Firewall*, *Proxy Servers*, *Mail Guard*) e *Workstation Access Control* (WAC) para controlar as portas USB[6] e proteger os dados que os dispositivos USB armazenam, são algumas das (…) medidas fundamentais para garantir […] a Segurança e a Superioridade da Informação" referidas por Telha (2018). Estas medidas enquadram-se nos indicadores respeitantes à H1 de existência de antivírus,

[5] Adoção de um conjunto de medidas de segurança destinadas a proteger os sistemas contra um ataque físico ou não, como o objetivo de provocar danos nestes sistemas (CEMFA, 2011a).

[6] USB é a sigla em inglês de *Universal Serial Bus* que permite a conexão de periféricos, como por exemplo *pendrives*, impressoras, ratos, etc., sem haver necessidade de ligar ou desligar o computador.

barreira de segurança *firewall*, proteção no acesso a um computador e, sistemas de deteção de intrusões (IDS).

Na FA, os mecanismos tecnológicos e respetivas implementações de segurança estão divididos em 5 níveis (Mendes, 2018):

- Inventário - a primeira preocupação, ao nível tecnológico deverá ser o controlo de todos os seus ativos tecnológicos (*Routers*, *Switchs*, Servidores, Postos de Trabalho, etc) de modo a perceber o que é necessário proteger;
- Perímetro e Controlo da Rede – por exemplo através de *Firewalls*;
- Equipamentos e Dispositivos – através do controlo e configuração de s*oftware*, antivírus, entre outros;
- Aplicações – Autenticação, Autorização e Auditoria (AAA), encriptação, etc;
- Dados – *Backups*, Gestão de Acessos, etc.

Mendes (2018) reforça que "(…) a RTI utiliza mecanismos e implementações sobre esses Sistemas de Informação, que visam assegurar que cada um dos princípios é mantido (…)", nomeadamente através da utilização de mecanismos de encriptação na sua transmissão de modo a assegurar a Confidencialidade, de funções de *Hashing*[7] na salvaguarda da Integridade e de mecanismos de redundância para a Disponibilidade da informação.

Além destes mecanismos são utilizados, a nível tecnológico, outros mecanismos de segurança. Mecanismos de filtragem, através da existência de antivírus, de mecanismos de controlo de acesso, com uma barreira de segurança *firewall*, de mecanismos de confinamento, na proteção do acesso a um computador, e de mecanismos de inspeção com sistemas de deteção de intrusão.

Estes mecanismos estão configurados para atuarem automaticamente revelando-se como medida de segurança e prevenção de modo a assegurar e garantir os Princípios da Informação. Existem ainda outros mecanismos de auditoria, como por exemplo o *Software* de Análise de Vulnerabilidades, que são utilizados manualmente, sempre que haja necessidade (Mendes, 2018).

Outra medida importante é a "(…) acreditação das redes seguras (…)" (Telha, 2018) uma vez que atualmente, apesar do que refere o RFA 390-3 sobre a informação classificada, não existe nenhum SI desenvolvido na FA com acreditação de segurança (Lopes, 2018).

[7] Função *Hash* é um algoritmo criptográfico que permite a segurança da informação durante o processo de cifragem-decifragem.

No entanto, o chefe da RSI – repartição responsável pelo desenvolvimento e manutenção dos SI da FA – refere que estes sistemas asseguram os Princípios da Segurança da Informação com o acesso através do binómio *userid – password*, *passwords* fortes, bases de dados protegidas e regras de acesso para ir de encontro ao princípio de ver apenas o que deve, de acordo com as suas funções, restringindo tudo o resto (Lopes, 2018), não sendo, por isso, a ausência de acreditação um fator de falta de segurança relativamente aos SI desenvolvidos internamente.

2.1. Síntese Conclusiva

A Segurança da Informação dos SI, e sua prevenção, é de extrema importância para a FA devendo ser tomadas as medidas necessárias para garantir os Princípios da Segurança da Informação.

É comum pensar-se em segurança e prevenção em simultâneo e por isso o termo política de segurança e prevenção surge naturalmente associado às medidas necessárias para garantir a Segurança da Informação, incluindo o recurso a mecanismos de segurança a nível tecnológico.

Mecanismos de segurança que garantem a Confidencialidade através da existência de algoritmos criptográficos, a Integridade com funções de *Hashing* e a Disponibilidade com *backups*, são utilizados para a Garantia da Informação dos SI desenvolvidos na FA.

Além destes mecanismos, são utilizados, diariamente, vários mecanismos de segurança que asseguram que os Princípios da Segurança da Informação estejam garantidos na FA. É o caso do Sistema de Antivírus dos Postos de Trabalho da FA que, no período de 27JAN2018 a 27ABR2018, detetou 371 vírus e/ou *spyware and risks*[8]. O recurso a este mecanismo, neste caso de filtragem, contribui como medida de segurança e prevenção para a Garantia da Informação dos SI desenvolvidos na FA.

Por ter sido demonstrado que o recurso aos mecanismos de segurança, referidos como indicadores no modelo de análise desta investigação relativamente à primeira hipótese, contribui como medida de segurança e prevenção para a Garantia da Informação dos SI desenvolvidos na FA, se considera como validada a H1.

[8] Dados fornecidos pela Secção de CiberDefesa da DCSI/RTI

3. A Segurança da Informação e os utilizadores na FA

Sendo o utilizador o elemento mais fraco de um SI, é essencial que o seu comportamento contribua para a Segurança da Informação através da adoção de medidas de segurança e prevenção. Caso um utilizador não adote "(…) uma conduta de boas práticas põe em risco qualquer sistema" (Lopes, 2018), sendo "(…) a formação dos utilizadores […] indispensável à manutenção da Segurança da Informação na Força Aérea" (Mendes, 2018).

Para se poder investigar em que medida o comportamento dos utilizadores dos SI desenvolvidos na FA pode contribuir para a Segurança da Informação na FA, foi realizado um questionário a todos os militares e civis da FA utilizadores destes sistemas com o intuito de efetuar uma análise quantitativa à adoção de medidas de segurança e prevenção por parte destes utilizadores relativamente à Segurança da Informação, bem como o seu nível de consciencialização sobre esta temática. O questionário foi lançado *on-line* e esteve disponível para preenchimento entre os dias 20FEV2018 e 16MAR2018.

A Tabela 2 reflete a amostra do questionário ao qual responderam 558 utilizadores de 7176 registados nos 59 SI desenvolvidos internamente, sendo 6595 efetivos.

Tabela 2 – Amostra do questionário realizado na FA entre 20FEV2018 e 16MAR2018

Amostra	Número	Percentagem
Categoria		
Oficial	342	61,29%
Sargento	183	32,80%
Praça/Soldado	18	3,23%
Civil	15	2,69%
Género		
Masculino	439	78,67%
Feminino	119	21,33%
Idade		
18-30 anos	98	17,56%
31-45 anos	308	55,20%
46-60 anos	151	27,06%
Mais de 60 anos	1	0,18%
Total de Inquiridos: 558		

Fonte: (Autora, 2018)

Dos 558 que responderam ao questionário, 16 não utilizam nenhum dos SI desenvolvidos na FA e por isso o número de respostas consideradas para este estudo reduz para 542. Apesar desta redução, este número é suficiente para realizar uma análise aos dados recolhidos com um grau de confiança de 95% e margem de erro de 5% uma vez que ultrapassa os 364 recomendados (Huot, 2002, cit. por Santos, et al., 2016, p. 73), (SurveyMonkey, 2018), considerando-se por isso as respostas como válidas.

As questões realizadas foram, maioritariamente, da forma "(…) "fechadas" – onde o inquirido pode escolher a sua resposta numa lista preestabelecida" (Santos, et al., 2016, p.97-98), agrupadas de acordo com as medidas de segurança identificadas na fase exploratória e com o conhecimento dos utilizadores sobre mecanismos e medidas de segurança.

Os resultados a seguir apresentados resultam das questões realizadas sobre as medidas de segurança[9] estudadas neste trabalho a fim de analisar se as ações dos utilizadores estão de acordo com os procedimentos de segurança recomendados, bem como o seu conhecimento relativamente a mecanismos e medidas de segurança a adotar.

3.1. Apresentação e análise dos resultados

Cerca de 75% dos inquiridos concorda totalmente sobre a importância de efetuar as atualizações do sistema operativo e restantes aplicações, contudo este número reduz para 34,50% quando questionados sobre a realização imediata das atualizações ou o adiamento para o dia seguinte.

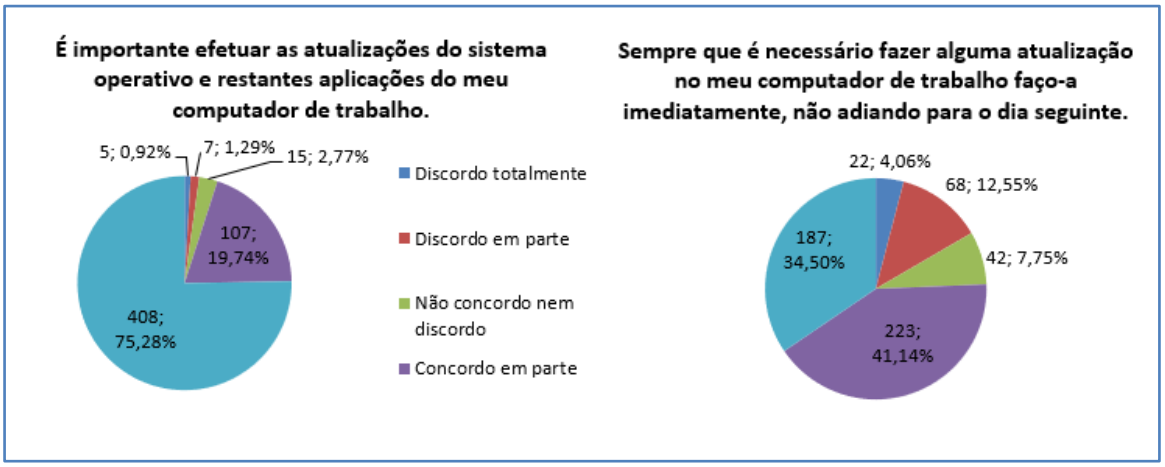

Figura 1 – Resultados "Atualizações de Segurança"

Fonte: (Autora, 2018)

[9] Estas medidas estão referidas no modelo de análise como indicadores da PD2/H2.

Embora a maioria dos utilizadores efetue cópias de segurança com regularidade, apresentando um comportamento adequado, existem ainda 28,41% que não o fazem e, dos que o fazem, 27,31% guardam a informação do computador de trabalho num dispositivo externo. Relativamente à periodicidade de efetuar cópias de segurança mensalmente as respostas dadas foram muito divididas não havendo um período ideal.

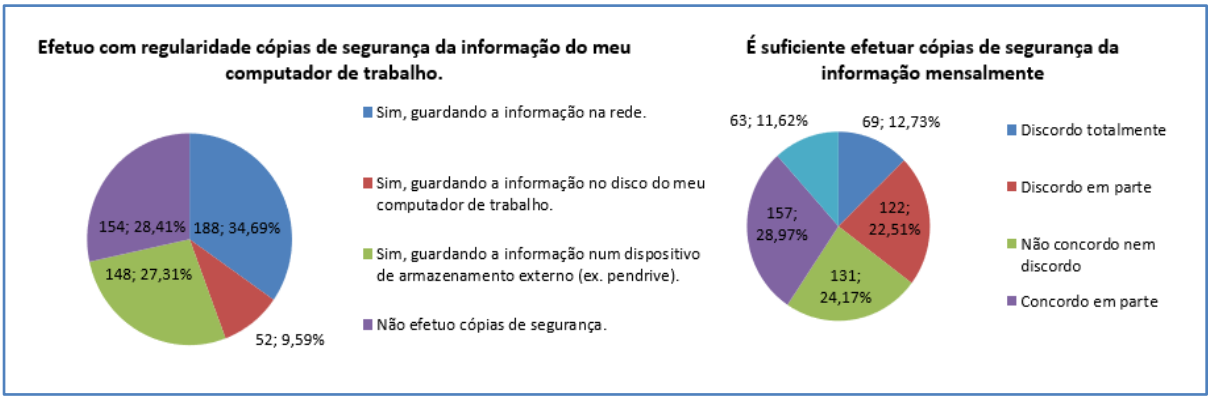

Figura 2 – Resultados "Cópias de Segurança"

Fonte: (Autora, 2018)

Qaunto à partilha de informação e do computador de trabalho, cerca de metade partilha ficheiros com outras pessoas e um quarto dos inquiridos chega mesmo a partilhar o seu computador de trabalho, o que pode comprometer a informação

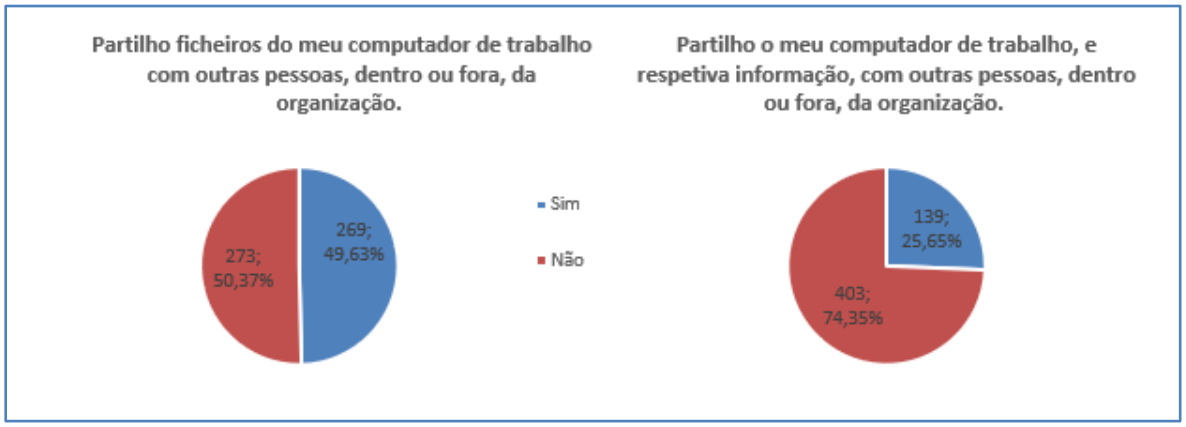

Figura 3 – Resultados "Partilha de Informação e do computador de trabalho"

Fonte: (Autora, 2018)

Também cerca de metade dos inquiridos liga no seu computador de trabalho dispositivos de armazenamento externo de outras pessoas. Porém, a maioria revela consciência do perigo ao discordar que este procedimento seja prudente.

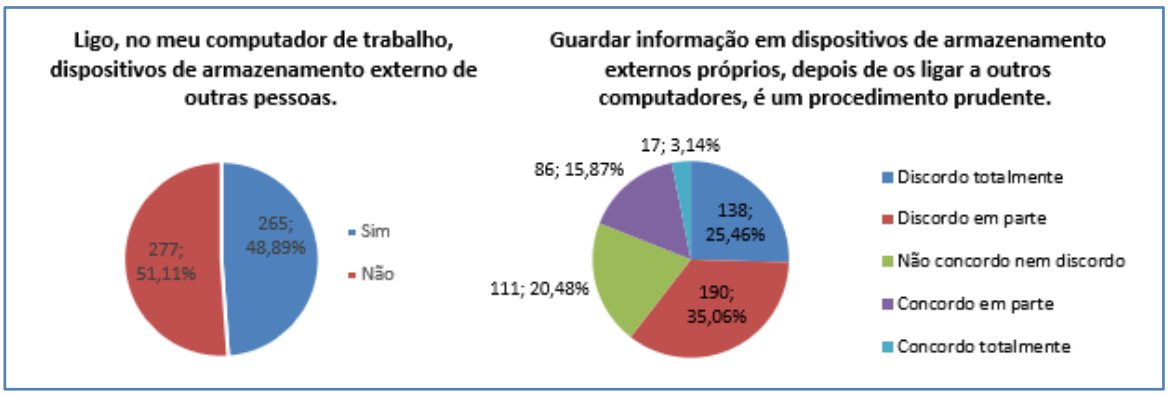

Figura 4 – Resultados "Dispositivos de armazenamento externo"

Fonte: (Autora, 2018)

O não bloqueio do computador poderá significar um risco para a segurança com 60,70% dos inquiridos a concordar totalmente e 22,32% em parte.

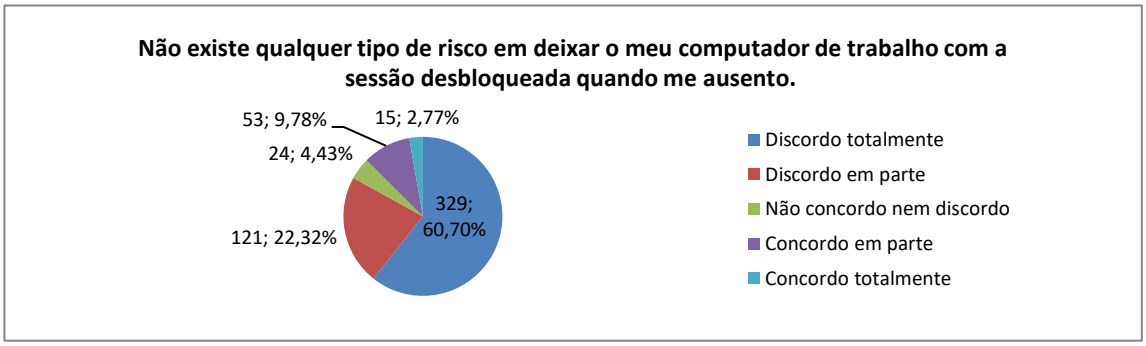

Figura 5 – Resultados "Bloqueio do computador"

Fonte: (Autora, 2018)

Apesar da maioria não utilizar senhas de acesso que o identifiquem (76,65%) e utilizarem números, letras e caracteres especiais (68,27%), cerca de 28%, utilizam a mesma senha para aceder aos diversos programas informáticos.

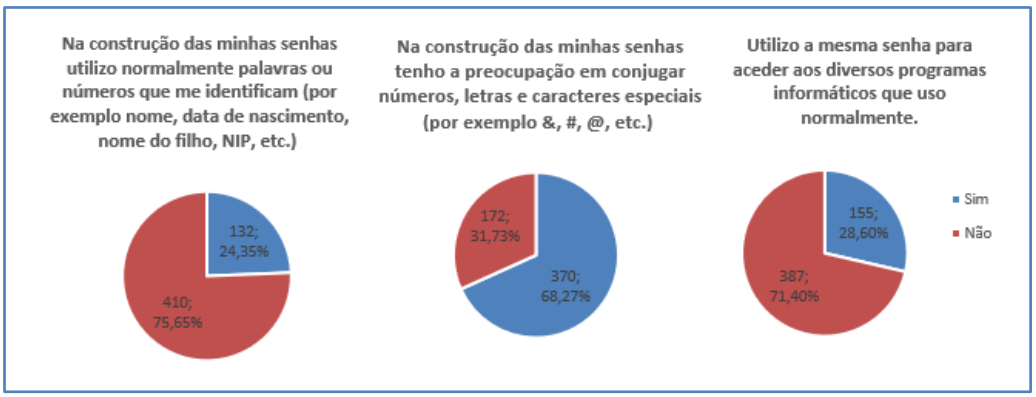

Figura 6 – Resultados "Senhas de acesso robustas e diferentes"

Fonte: (Autora, 2018)

Quando questionados sobre a compartilha ou divulgação das senhas, cerca de 90% dos utilizadores revela um comportamento adequado.

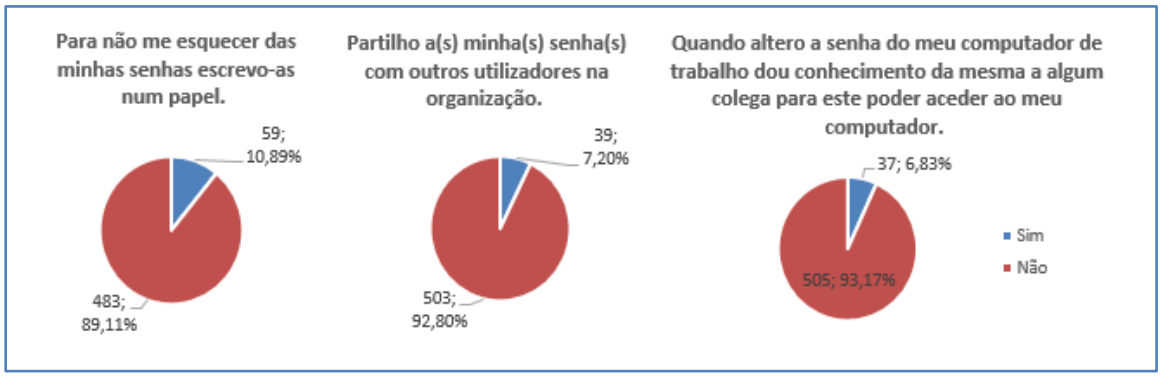

Figura 7 – Resultados "Partilha de senhas de acesso"

Fonte: (Autora, 2018)

Quase 61% discorda totalmente sobre a importância de analisar o assunto antes de abrir uma mensagem de correio eletrónico e 45,20% sobre eliminar uma cujo remetente é desconhecido. Estes comportamentos não são os recomendados constituindo uma ameaça à segurança. No entanto os inquiridos revelam ter um conhecimento adequado sobre a utilização da *Internet* relativamente à Segurança da Informação.

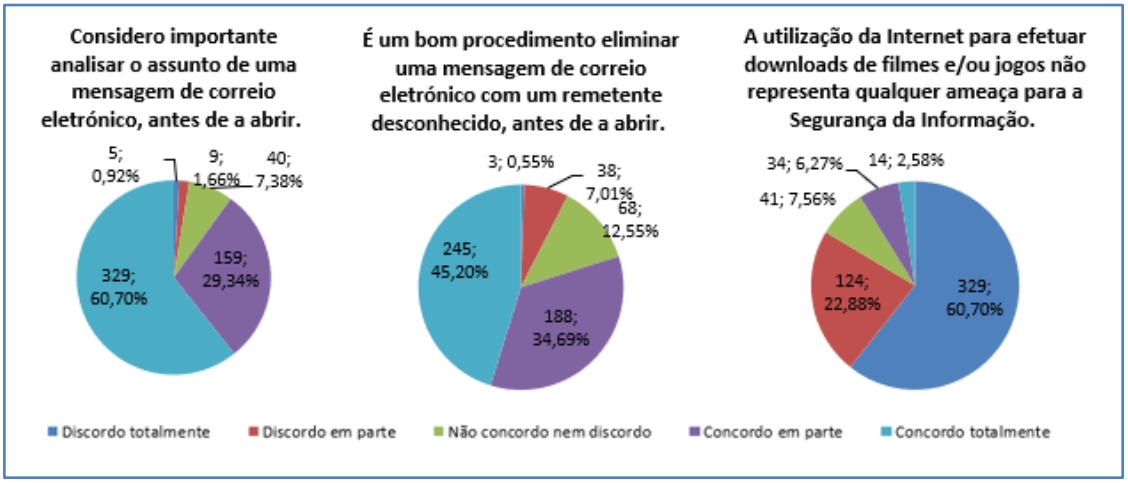

Figura 8 – Resultados "Utilização *Internet* e correio eletrónico"

Fonte: (Autora, 2018)

Aproximadamente 76% dos utilizadores tem noção de qual o comportamento a adotar em caso de incidentes estranhos com o seu computador, contudo cerca de 12% não o faz afirmando que nunca ninguém lhe disse para o fazer.

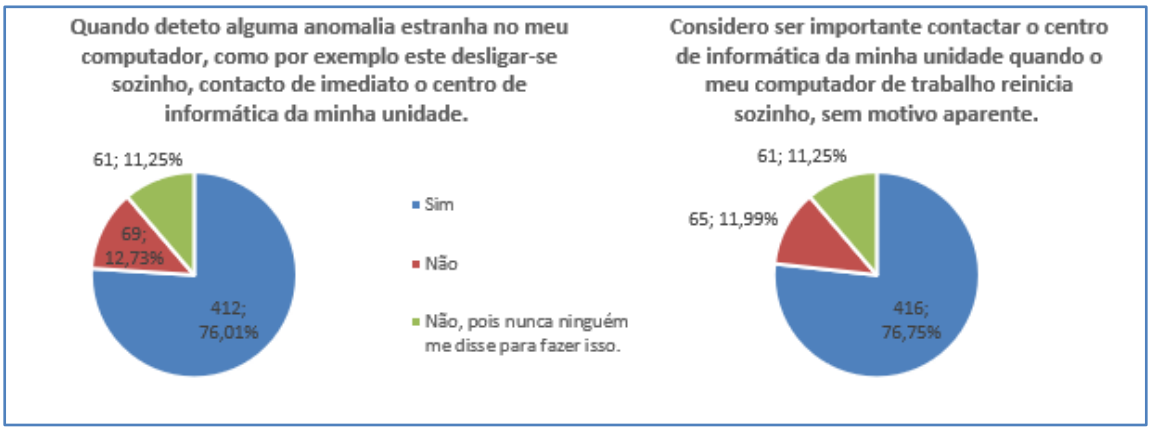

Figura 9 – Resultados "Reporte incidentes de segurança"

Fonte: (Autora, 2018)

Apesar de 50,55% dos inquiridos concordarem em parte que a existência de mecanismos de segurança é sinónimo de segurança, e 33,95% totalmente, é importante que tenham consciência da sua existência, verificando-se que existem ainda muitos utilizadores que desconhecem se têm instalado no computador de trabalho algum dos apresentados.

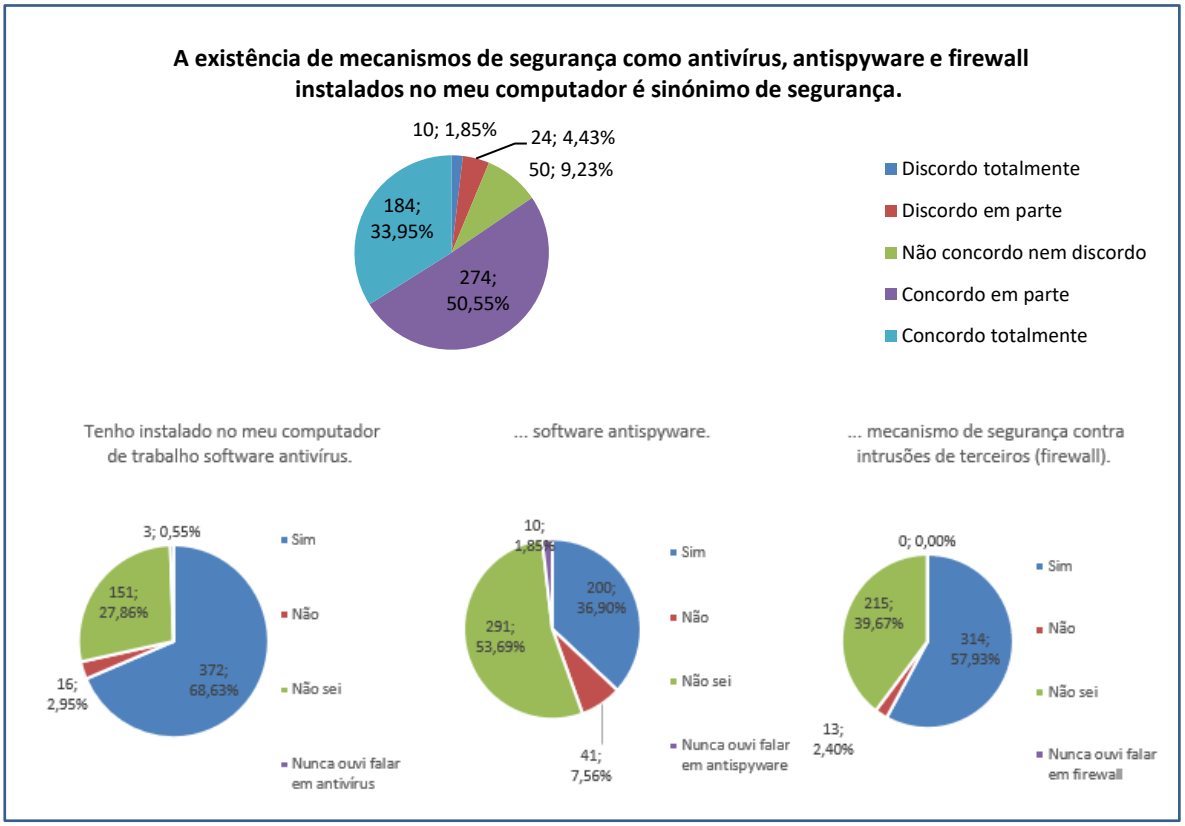

Figura 10 – Resultados "Mecanismos de segurança"

Fonte: (Autora, 2018)

Relativamente às medidas de segurança, a grande maioria, 80,44%, tem conhecimento do que fazer com quase 75% a concordar totalmente sobre a importância da sua divulgação.

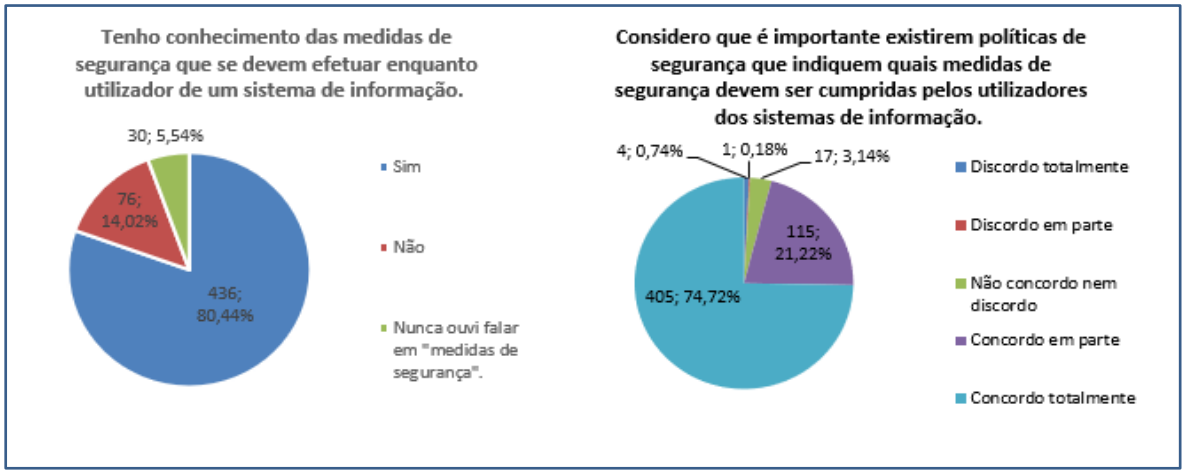

Figura 11 – Resultados "Medidas de segurança"

Fonte: (Autora, 2018)

E para 71,59%, deveriam ser realizadas sessões de sensibilização junto dos utilizadores, 52,21% divulgadas no portal interno, cerca de 43% durante a formação e 36,16% que cada SI deveria conter um manual de políticas de segurança a adotar. Das 24 respostas abertas dadas os utilizadores sugerem, maioritariamente, a divulgação das medidas de segurança por correio eletrónico interno.

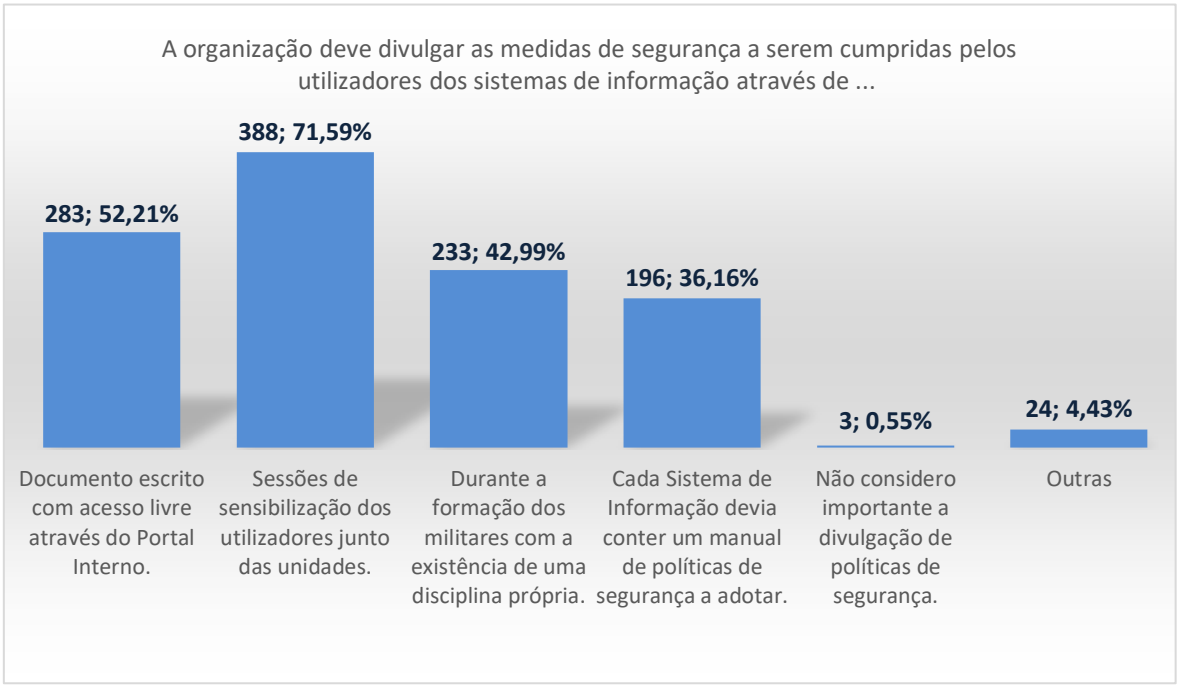

Figura 12 – Resultados "Meio divulgação medidas de segurança"

Fonte: (Autora, 2018)

À última questão, 65,87% responderam afirmativamente sobre terem conhecimento da existência de uma Política de Segurança da Informação. Porém, 21,03% já ouviram falar mas não sabem do que se trata.

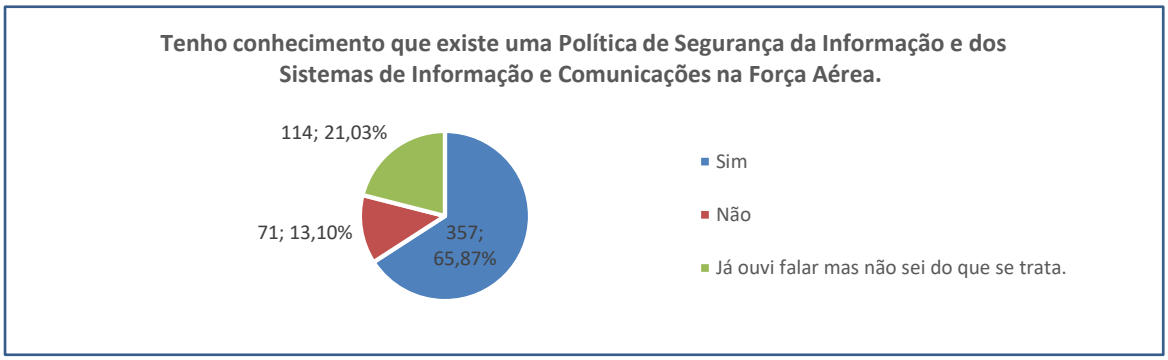

Figura 13 – Resultados "Política de Segurança da Informação"

Fonte: (Autora, 2018)

Por fim, relativamente ao grau de satisfação dos utilizadores em relação à Segurança da Informação dos SI desenvolvidos na FA, apresenta-se o seguinte gráfico com saldo bastante positivo onde, numa escala de 1 a 5, em que 1 significa que o utilizador está muito insatisfeito em relação à Segurança da Informação na FA, e 5 está muito satisfeito, quase 50% dos inquiridos respondeu com 4.

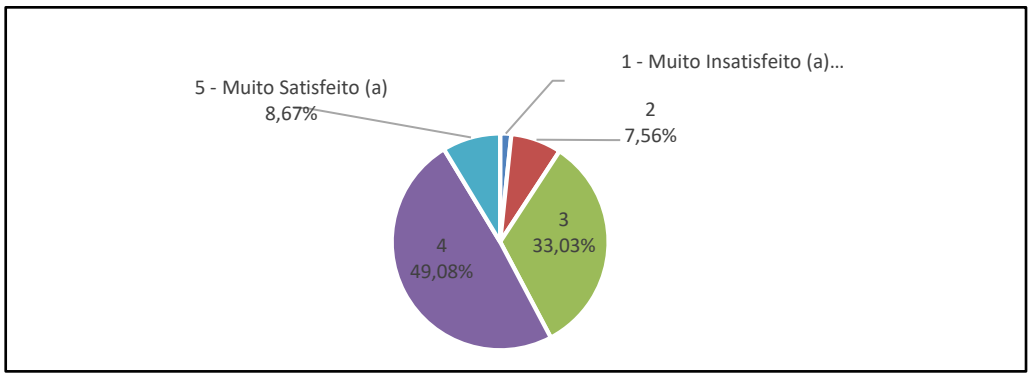

Figura 14 – Satisfação dos utilizadores em relação à Segurança da Informação na FA

Fonte: (Autora, 2018)

3.2. Síntese conclusiva

Para Morgado (2018), "(…) uma utilização consciente dos SI/TICs por parte dos utilizadores, contribui […] para uma melhoria da Segurança da Informação da FA". Telha (2018), acrescenta que "(…) a maior vulnerabilidade de um SI é o comportamento dos seus

utilizadores (…)" e que a "(…) única forma de minimizar os riscos é promover e instituir uma "cultura de segurança" (…)".

A formação dos utilizadores (Morgado, 2018) e o seu aconselhamento, para adoção de boas práticas (Lopes, 2018) contribui "(…) de uma forma sinérgica e contínua fazer face a uma realidade em que as ameaças se tornam cada vez mais globais (…)" (Telha, 2018) e somente "(…) através de uma educação de segurança […] e no esclarecimento dos Princípios, Conceitos e Medidas de Segurança, se obterá a Segurança da Informação" (CEMFA, 2008).

Partindo destas premissas, e através das medidas de segurança identificadas previamente, foi possível concluir da análise aos dados do questionário realizado que, de um modo geral, os utilizadores dos SI desenvolvidos na FA têm um comportamento considerado adequado, contribuindo para a Segurança da Informação através da adoção de medidas de segurança e prevenção, validando-se a hipótese H2.

Para a maioria dos inquiridos a importância da divulgação destas medidas durante a formação tem um peso significativo, contudo a sensibilização aos utilizadores é feita essencialmente através de "(…) cursos, palestras, exercícios e ações de formação adequados ao tipo de utilização e responsabilidade nos SI da FA" (Telha, 2018) e do exercício CiberPerseu com o "(…) objectivo de treinar e sensibilizar os utilizadores em questões relacionadas com a Segurança Informática" (Morgado, 2018).

A importância dada a esta sensibilização, tanto pelos utilizadores de SI como pela própria organização, valida a H3 uma vez que certifica que uma consciencialização por parte dos utilizadores de SI contribui com medida de segurança e prevenção para a Segurança da Informação na FA. Porém, Morgado (2018) refere que "(…) existe, ainda, algum trabalho a levar a cabo no âmbito da melhoria da *awareness* (…)"

Os utilizadores de SI são de facto a núcleo da Segurança da Informação, contudo Telha (2018) acrescenta que "(…) a falta de formação dos programadores e de analistas de sistemas (…)" é uma das principais vulnerabilidades à Segurança da Informação devendo ser também dada a devida importância a este assunto.

Outro fator, de grande importância, a ter em conta é a Engenharia Social, ou seja, a utilização de técnicas, por parte de *hackers*, ou piratas cibernéticos, para "(…) obter informações importantes ou sigilosas através de ações que enganam ou exploram a confiança das pessoas" (CNCS, 2017b). Deverá ser dada uma atenção contínua (Telha, 2018) uma vez

que "(…) a Engenharia Social é, hoje, a melhor forma de um atacante conseguir vantagem e explorar deficiências dos SI/TIC de uma Organização" (Morgado, 2018).

Apesar de não ser objetivo deste trabalho, foi também questionada a satisfação dos utilizadores relativamente à Segurança da Informação na FA de modo a ter uma panorâmica sobre a confiança que os militares e civis, utilizadores de SI desenvolvidos na FA, têm na organização. O resultado obtido foi positivo com a maioria dos inquiridos a mostrar-se bastante satisfeito demostrando um grande grau de confiança relativamente aos SI.

Conclusões

Com este trabalho de investigação pretendeu-se efetuar uma análise qualitativa à forma como a adoção de medidas de segurança e prevenção pode contribuir para a Segurança da Informação dos SI desenvolvidos na FA de modo a minimizar o risco de uma ameaça com origem nos seus utilizadores.

Após a revisão da literatura e identificado o estado da arte, foi reconhecido que a adoção de mecanismos e medidas que assegurem os princípios da Segurança da Informação deve ser considerada como um requisito essencial. A importância de os utilizadores dos SI estarem cientes da existência de mecanismos de segurança e de quais medidas de segurança devem adotar de modo a garantir a Segurança da Informação destes sistemas, uma vez que, de acordo com os vários autores estudados, o utilizador é o elemento mais fraco de um SI, é considerado igualmente fundamental.

Desta forma foi formulada a seguinte pergunta principal que serviu de fim condutor ao estudo de caso em investigação neste TII: De que forma a adoção de uma política de segurança e prevenção pode contribuir para a Segurança da Informação dos SI desenvolvidos na FA, de modo a minimizar o risco de uma ameaça com origem nos seus utilizadores?

Para obter resposta a esta questão optou-se por uma estratégia de investigação qualitativa, com reforço quantitativo, seguindo o raciocínio hipotético-dedutivo, possibilitando a construção do modelo de análise composto pela pergunta de partida, derivadas e respetivas hipóteses, conceitos, dimensões, indicadores e instrumentos de observação utilizados neste estudo.

Para a análise de dados recorreu-se aos principais meios de recolha de informação, a entrevista, a observação e o questionário. Houve necessidade ainda de realizar uma variada análise documental recorrendo a diversa bibliografia nacional e estrangeira.

Optou-se por dividir o trabalho em três capítulos. No primeiro foi feita a revisão da literatura e apresentado o modelo de análise seguido nesta investigação. Os dois últimos capítulos corresponderam a cada uma das perguntas derivadas, sendo o segundo dedicado aos mecanismos de segurança na FA e o terceiro, maioritariamente, à análise dos resultados obtidos no questionário sobre a Segurança da Informação e os utilizadores na FA.

Com esta investigação foi possível verificar que na FA, diariamente, se recorre a mecanismos, previamente referenciados, para assegurar que os Princípios da Segurança da Informação estejam garantidos. Essencialmente, são utilizados mecanismos de segurança que garantem a Confidencialidade através da existência de algoritmos criptográficos, a

Integridade com funções de *Hashing* e a Disponibilidade com *Backups*. A nível tecnológico recorrem-se ainda a outros mecanismos de segurança identificados como mecanismos de filtragem através da existência de antivírus, de controlo de acesso com uma barreira de segurança *firewall*, de confinamento na proteção do acesso a um computador, e de inspeção com sistemas de deteção de intrusão.

O recurso a estes mecanismos permite a Garantia da Informação na organização através da utilização automática, ou manualmente sempre que haja necessidade, garantindo que os Princípios da Segurança da Informação estão assegurados.

Assim, decorrente das entrevistas realizadas e da análise documental efetuada, foi possível confirmar que o recurso a estes mecanismos contribui, efetivamente, para a Segurança da Informação dos SI desenvolvidos na FA, permitindo validar a H1: O recurso a mecanismos de segurança contribui, como medida de segurança e prevenção, para a Garantia da Informação dos SI desenvolvidos na FA. A H1 está diretamente relacionada com a PD1, confirmando que o recurso a mecanismos de segurança contribui para a Segurança da Informação na FA.

Contudo, deverá ser preferencialmente tomada uma medida de segurança preventiva com origem nos próprios utilizadores para não existir sequer o risco de uma ameaça à Segurança da Informação.

De acordo com vários autores, o ponto mais vulnerável e elemento mais fraco de um sistema são os utilizadores, tornando-se vital a sua consciencialização para a adoção de medidas de segurança e prevenção de modo a contribuir para Segurança da Informação dos SI.

É fundamental que numa organização os utilizadores dos SI adotem medidas de segurança preventivas que correspondam aos requisitos definidos na política de segurança da organização. No entanto, se estes não tiverem conhecimento de quais medidas adotar poderão, inconscientemente, constituir-se como uma ameaça para Segurança da Informação da organização onde trabalham.

Com base nesta abordagem foi efetuado um questionário com o objetivo de analisar de que forma os utilizadores dos SI desenvolvidos na FA estão consciencializados sobre o comportamento e medidas de segurança e prevenção a adotar, de modo a contribuírem para Segurança da Informação.

Através dos indicadores identificados como medidas de segurança e prevenção a adotar pelos utilizadores foi possível concluir que, de um modo geral, os utilizadores dos SI

desenvolvidos na FA adotam um comportamento considerado adequado e de acordo com o recomendado contribuindo para a Segurança da Informação através da adoção de medidas de segurança e prevenção validando-se, assim, a segunda hipótese.

No entanto, as medidas de segurança não garantem a 100% a proteção da Segurança da Informação contra todas as ameaças, mas, quando adotadas pelos utilizadores dos SI, minimizam esse risco e por isso deverão ser melhorados alguns aspetos:

- o comportamento relativamente às cópias e atualizações de segurança uma vez que os resultados obtidos revelam que os utilizadores, apesar de estarem conscientes sobre a sua importância, ainda não cumprem de imediato com o pedido;
- a partilha da informação é outro fator a ter em conta. Contudo, apesar do comportamento não ser o recomendado, poderá ser uma inevitabilidade da função e por isso a importância dos utilizadores em estarem conscientes deste perigo;
- a utilização de senhas de acesso fortes, alteração frequente, ou a sua partilha, são uma importante medida de segurança e prevenção a adotar pelos utilizadores de SI e, de facto, a maioria dos utilizadores cumpre com estas medidas. Porém, existe ainda uma grande fatia que não o faz podendo ser considerado como um risco;
- a não importância revelada pelos utilizadores relativamente ao correio eletrónico constitui uma ameaça à segurança devendo ser reforçada;
- a consciencialização dos utilizadores deve ser o ponto focal da Segurança da Informação. No entanto alguns utilizadores revelam desconhecimento sobre a existência de mecanismos e medidas de segurança a adotar.

Derivado deste desconhecimento foi igualmente possível aferir que para a maioria dos inquiridos é muito importante existirem sessões de sensibilização junto dos utilizadores e que, para além da divulgação das medidas de segurança no portal interno, a organização deve divulgar as medidas de segurança a serem cumpridas pelos utilizadores dos SI durante a formação dos militares com a existência de uma disciplina própria.

Porém, a sensibilização aos utilizadores é feita essencialmente através de cursos, palestras, exercícios e ações de formação adequadas ao tipo de utilização e responsabilidade, revelando-se como insuficiente para o grande número de utilizadores de SI que existem atualmente na FA.

O facto da organização e dos próprios utilizadores valorizarem a importância da consciencialização relativamente ao comportamento que os utilizadores devem adotar, uma

vez que estes poderão significar uma ameaça, contribui para a Segurança da Informação. Desta forma valida-se a H3: A consciencialização (*Awareness*) dos utilizadores dos SI desenvolvidos na FA, relativamente ao comportamento a adotar, contribui como medida de segurança e prevenção para a Segurança da Informação na FA. Porém, existe ainda algum trabalho a desenvolver no âmbito da melhoria do *Awareness*.

A validação das hipóteses H2 e H3 permite responder à PD2, confirmando-se que a consciencialização e a adoção de medidas de segurança e prevenção por parte por utilizadores dos SI desenvolvidos na FA contribui para a Segurança da Informação na FA.

Por fim, após a prova de todas as hipóteses, foi possível responder à pergunta de partida concluindo-se que a adoção de uma política de segurança e prevenção, através da implementação de um conjunto de normas, indicações ou instruções a seguir pelos utilizadores e respetivos responsáveis, contribui para a Segurança da Informação dos SI desenvolvidos na FA de modo a minimizar o risco de uma ameaça com origem nos seus utilizadores.

Com esta investigação foram igualmente alcançados os objetivos propostos no início e, por isso, foi possível compreender de que forma os utilizadores dos SI desenvolvidos na FA estão consciencializados sobre a Segurança da Informação de modo a melhorar o atual paradigma da Segurança da Informação na organização através da implementação de medidas de segurança e prevenção, destacando-se os seguintes contributos:

- Foi validado o cumprimento dos Princípios da Segurança da Informação através do recurso aos principais mecanismos de segurança contribuindo para a Garantia da Informação na organização;
- Verificou-se que, de um modo geral, os utilizadores adotam as medidas de segurança recomendadas, contribuindo para a Segurança da Informação na FA, apesar de terem que ser ainda melhorados alguns pontos;
- Verificou-se que os utilizadores dos SI desenvolvidos na FA estão consciencializados relativamente ao comportamento a adotar;
- Apesar da FA dar a devida importância à consciencialização dos utilizadores relativamente à Segurança da Informação, é necessário desenvolver ainda algum trabalho nesta área de modo a abranger um maior número de utilizadores.

Decorrente desta análise recomenda-se:

À DIVCSI:

- A revisão do atual RFA 390-3 de modo a abranger a proteção da informação não classificada ou mesmo a criação de uma nova Política de Segurança destinada apenas a este tipo de informação.

À DCSI:

- Manter o recurso dos referidos mecanismos de segurança de modo a assegurar os Princípios da Segurança da Informação;
- Disponibilizar a adequada formação dos programadores e analistas de sistemas relativamente à Segurança da Informação;
- Efetuar uma maior divulgação das medidas a adotar pelos utilizadores relativamente aos SI através do portal interno e/ou por GW;
- Desenvolver mais ações de formação sobre a Segurança da Informação abrangendo um número mais alargado de utilizadores;
- Manter uma atenção contínua à Engenharia Social informando os utilizadores sobre este risco.

Aos Administradores de Informação:

- Durante as ações de formação, reforçarem o aconselhamento e práticas a adotar por parte dos utilizadores dos respetivos SI.

Estudos específicos:

- Face ao tempo disponível este trabalho está limitado tanto em extensão como de abordagem e por isso, após identificada a importância do utilizador de SI, apenas foi objeto de estudo o elemento humano como ameaça à Segurança da Informação, recomendando-se a elaboração de estudos específicos que abranjam outras ameaças e/ou vulnerabilidades.

Finalmente, resta referir que o processo de segurança não é algo que se possa dizer que tem um princípio e um fim bem determinados. É um processo constante e continuado ao longo do tempo e implica a não existência de tréguas pois estas podem constituir-se como ameaças ou vulnerabilidades à Segurança da Informação de uma organização.

Bibliografia

Arthur, L., 2009. *Segurança da Informação – Conceitos.* [Em Linha] s.l.: LinkedIn SlideShare. Disponível em: https://pt.slideshare.net/luiz_arthur/seguranca-da-informao-conceitos [Acedido em 13 Out. 2017]

Associação para a Promoção e Desenvolvimento da Sociedade da Informação, 2017. *Glossário.* [Em Linha] Lisboa: APDSI. Disponível em: http://www.apdsi.pt/index.php/portugues/menu-secundario/glossario.html [Acedido em 25 Nov. 2017]

Centro Nacional de Cibersegurança, 2017a. *A Segurança da Informação - Informação ao Colaborador.* [Em Linha] Lisboa: CNCS. Disponível em: https://www.cncs.gov.pt/content/files/brochura_2.pdf [Acedido em 25 Nov. 2017]

Centro Nacional de Cibersegurança, 2017b. *Glossário.* [Em Linha] Lisboa: CNCS. Disponível em: https://www.cncs.gov.pt/recursos/glossario/ [Acedido em 14 Nov. 2017]

Chefe do Estado-Maior da Força Aérea, 2008. *POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DOS SISTEMAS DE INFORMAÇÃO E COMUNICAÇÕES DA FORÇA AÉREA* (RFA 390-3). Alfragide: DIVCSI

Chefe do Estado-Maior da Força Aérea, 2011a. *POLÍTICA DE CIBERDEFESA DA FORÇA AÉREA* (RFA 390-6). Alfragide: DIVCSI

Chefe do Estado-Maior da Força Aérea, 2011b. *POLÍTICA DE GESTÃO DA INFORMAÇÃO DA FORÇA AÉREA* (RFA 391-1). Alfragide: DIVCSI

Chefe do Estado-Maior da Força Aérea, 2015. *Plano Diretor dos Sistemas de Informação da Força Aérea*. Alfragide: DIVCSI

Dhillon, G., 2001. Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security*, [Em Linha] 20 (2), pp. 165-172. Disponível em: https://pdfs.semanticscholar.org/5771/bbd18b8442682427db81c1fd9eee9e098f67.pdf [Acedido em 28 Dez. 2017]

Francisco, G. E. M., 2016, *Processo de Awareness dos Utilizadores nas Redes Militares.* [Em Linha] Lisboa: Academia Militar. Disponível em: http://hdl.handle.net/10400.26/15162 [Acedido em 22 Mai. 2018]

Gaivéo, J. M., 2008, *As Pessoas nos Sistemas de Gestão da Segurança da Informação.* [Em

Linha] s.l.: Universidade Aberta. Disponível em: https://repositorioaberto.uab.pt/bitstream/10400.2/1272/1/Tese-Jos%C3%A9Gaiv%C3%A9o%20-%20Vers%C3%A3oFinal.pdf [Acedido em 30 Nov. 2017]

Garcia, J. B. D., 2002. *A Segurança nos Sistemas de Informação no Exército Português. Contributos para a sua definição (2000/2002).* Trabalho Individual de Longa Duração - Curso de Estado Maior. Instituto de Altos Estudos Militares.

InfoSec Institute, s.d.. *CIA Triad*. [Em Linha] s.l.: INFOSEC. Disponível em: http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/the-security-cia-triad/#gref [Acedido em 29 Dez. 2017]

Instituto de Estudos Superiores Militares, 2015a. *Trabalhos de Investigação – NEP / ACA – 010*. Lisboa: IESM.

Instituto de Estudos Superiores Militares, 2015b. *Regras de Apresentação e Referenciação para os Trabalhos Escritos a realizar no IESM – NEP / ACA – 018*. Lisboa: IESM.

Júnior, J. R. A., 2005. *A Segurança em Sistemas de Informação*. [Em Linha] s.l.: s.n.. Disponível em: http://www.contecsi.fea.usp.br/envio/index.php/contecsi/2contecsi/paper/download/1189/470 [Acedido em 28 Dez. 2017]

Lopes, D. V. V., 2018. Entrevista ao Chefe da RSI [Entrevista]. Alfragide (18 março 2018)

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

Martins, J., Silva, J., Pimentel, C., Galindro, A., Rocha, J. e Custódio, M., 2016. Sensibilização e Treino em Cibersegurança – Exercício de Recolha de Informação. *PROELIUM Série VII - Revista da Academia Militar*, 10, 141-160.

Mendes, J. M. V. P., 2018. Entrevista ao Chefe da RTI [Entrevista]. Alfragide (02 maio 2018)

Morgado, J. A. N. V. P., 2018. Entrevista ao Diretor da DCSI [Entrevista]. Alfragide (09 abril 2018)

Pimenta, A. M. S., Quaresma, R.F.C., 2016. A segurança dos sistemas de informação e o comportamento dos usuários. *Journal of Information Systems and Technology Management.* [Em Linha] 13 (3), pp. 533-552. Disponível em: http://www.jistem.fea.usp.br/index.php/jistem/article/view/10.4301%25S1807-

17752016000300010/634 [Acedido em 12 Out. 2017]

Rhee, H.-S., Kim, C., Ryu, Y. U., 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, [Em Linha] 28 (8), pp. 816-826. Disponível em: https://www.academia.edu/9001815/Self-efficacy_in_information_security_Its_influence_on_end_users_information_security_practice_behavior [Acedido em 28 Dez. 2017]

Rodrigues, F. J. L., 2016. Principais Ameaças no Contexto da Cibersegurança. *CEDIS Working Papers | Direito, Segurança e Democracia*, [Em Linha] 48. Disponível em: http://cedis.fd.unl.pt/blog/project/principais-ameacas-no-contexto-da-ciberseguranca/ [Acedido em 12 Out. 2017]

Santos, L. A. B., Garcia, F. M. G. P. P., Monteiro, F. T., Lima, J. M. M. V., Silva, N. M. P., Silva, J. C. V. F., Piedade, J. C. L., Santos, R. J. R. P., Afonso, C. F. N. L. D., 2016. *Cadernos do IESM: Orientações metodológicas para a elaboração de trabalhos de investigação*. Lisboa: IESM.

SurveyMonkey, 2018. *Calculadora de tamanho de amostra.* [Em Linha] s.l.: SurveyMonkey, Disponível em: https://pt.surveymonkey.com/mp/sample-size-calculator/ [Acedido em 28 Mar. 2018]

Telha, A. C. D. O. R., 2018. Entrevista ao Chefe da DIVCSI [Entrevista]. Alfragide (24 abril 2018)

Tomé, L., 2018. Dinâmicas Sociais e Organizacionais. In: CPOS FA-PG, 2018. *Geopolítica Mundial e Segurança Internacional*. Instituto Universitário Militar, 26 de abril de 2018. Lisboa: IUM.

União Europeia, 2016. *Relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União* (Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016) [Em Linha] Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=PL [Acedido em 02 Dez. 2017]

Workman, M., Bommer, W.H., Straub, D., 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, [Em Linha] 24, 2799-2816. Disponível em: http://130.18.86.27/faculty/warkentin/BIS9613papers/WorkmanBommerStraub2008_CompInHumanBeh24_ThreatControl_SecLapses.pdf [Acedido em 28 Dez. 2017]

Zúquete, A., 2013. Segurança em Redes Informáticas. 4ª Ed. Aumentada. Lisboa: FCA – Editora de Informática.

Apêndice A — Modelo de Análise

Pergunta de partida (PP)	Perguntas derivadas (PD)	Hipóteses (H)	Conceitos	Dimensão	Indicadores	Instrumentos de Observação
PP: De que forma a adoção de uma política de segurança e prevenção pode contribuir para a Segurança da Informação dos SI desenvolvidos na FA, de modo a minimizar o risco de uma ameaça com origem nos seus utilizadores?	**PD1:** De que maneira o recurso a mecanismos de segurança contribui para a Segurança da Informação na FA?	**H1:** O recurso a mecanismos de segurança contribui, como medida de segurança e prevenção, para a Garantia da Informação dos SI desenvolvidos na FA	Prevenção Garantia da Informação	Segurança da Informação	Garantia de Confidencialidade Garantia de Integridade Garantia de Disponibilidade	Análise Documental Entrevistas
			Mecanismos de Segurança	Tecnológica	Existência de *antivírus* Proteção no acesso a um computador Barreira de segurança *firewall* Sistemas de deteção de intrusões (IDS)	Análise Documental Entrevistas
	PD2: Em que medida os utilizadores dos SI desenvolvidos na FA podem contribuir para a Segurança da Informação na FA?	**H2:** A adoção de medidas de segurança e prevenção por parte dos utilizadores dos SI desenvolvidos na FA, contribui para a Segurança da Informação na FA.	Medidas de Segurança e Prevenção	Segurança da Informação	Atualizações de Segurança Cópias de Segurança Partilha de informação Dispositivos de armazenamento externo Bloqueio do computador Senhas de Acesso robustas e diferentes Partilha de senhas de acesso Utilização Internet e correio eletrónico Reporte incidentes de segurança	Questionário Entrevistas
		H3: A consciencialização (Awareness) dos utilizadores dos SI desenvolvidos na FA, relativamente ao comportamento a adotar, contribui como medida de segurança e prevenção para a Segurança da Informação na FA.	Awareness	Cognitiva	Conhecimento dos utilizadores sobre a existência de mecanismos e medidas de segurança	Questionário
				Formação	Ações de Formação Cursos Palestras	Entrevistas Análise Documental

Apêndice B — Questionário

*Obrigatório

1. Caraterização da amostra

1.1. Categoria *

Por favor selecione uma opção.

- ○ Oficial
- ○ Sargento
- ○ Praça/Soldado
- ○ Civil

1.2. Género *

Por favor selecione uma opção.

- ○ Masculino
- ○ Feminino

1.3. Idade *

Por favor selecione uma opção.

- ○ 18-30 anos
- ○ 31-45 anos
- ○ 46-60 anos
- ○ Mais de 60 anos

2. Pergunta eliminatória

Existem cerca de 59 sistemas de informação desenvolvidos na Força Aérea, entre o Portal Interno da Força Aérea, PLUS (MGI, PSI, MGM, MGO), SIAGFA (RH, SIGAP-MCR, ABAST, SIGMA-MCR, SIGOP, SIGAUT, SIPAV, GESTCRED, SCA, etc...), eDocs, entre outros.

2.1. Utiliza no seu posto de trabalho algum Sistema de Informação desenvolvido na Força Aérea? *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

3. Segurança da Informação

O Centro Nacional de Cibersegurança (CNCS) define Segurança da Informação como "(…) um processo organizado e estruturado que permite preservar a confidencialidade, integridade e a disponibilidade da informação".

3.1. Qual é o seu grau de satisfação em relação à Segurança da Informação dos Sistemas de Informação desenvolvidos na Força Aérea? *

Por favor selecione uma opção de 1 (um) a 5 (cinco), sendo que 1 corresponde a "Muito insatisfeito(a)" e 5 a "Extremamente satisfeito(a)".

	1	2	3	4	5	
Muito insatisfeito(a)	○	○	○	○	○	Extremamente satisfeito(a)

4. Atualizações de Segurança

4.1. É importante efetuar as atualizações do sistema operativo e restantes aplicações do meu computador de trabalho. *

Por favor selecione uma opção.

- ○ Discordo totalmente
- ○ Discordo em parte
- ○ Não concordo nem discordo
- ○ Concordo em parte
- ○ Concordo totalmente

4.2. Sempre que é necessário fazer alguma atualização no meu computador de trabalho faço-a imediatamente, não adiando para o dia seguinte. *

Por favor selecione uma opção.

- ○ Discordo totalmente
- ○ Discordo em parte
- ○ Não concordo nem discordo
- ○ Concordo em parte
- ○ Concordo totalmente

5. Cópias de Segurança

5.1. Efetuo com regularidade cópias de segurança da informação do meu computador de trabalho. *

Por favor selecione uma opção.

- ○ Sim, guardando a informação na rede.
- ○ Sim, guardando a informação no disco do meu computador de trabalho.
- ○ Sim, guardando a informação num dispositivo de armazenamento externo (ex. *pendrive*).
- ○ Não efetuo cópias de segurança.

5.2. É suficiente efetuar cópias de segurança da informação mensalmente. *

Por favor selecione uma opção.

- ○ Discordo totalmente
- ○ Discordo em parte
- ○ Não concordo nem discordo
- ○ Concordo em parte
- ○ Concordo totalmente

6. Partilha de informação e do computador

6.1. Partilho ficheiros do meu computador de trabalho com outras pessoas, dentro ou fora, da organização. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

6.2. Partilho o meu computador de trabalho, e respetiva informação, com outras pessoas, dentro ou fora, da organização. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

7. Dispositivos de armazenamento externo

7.1. Ligo, no meu computador de trabalho, dispositivos de armazenamento externo de outras pessoas. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

7.2. Guardar informação em dispositivos de armazenamento externos próprios, depois de os ligar a outros computadores, é um procedimento prudente. *

Por favor selecione uma opção.

- ○ Discordo totalmente
- ○ Discordo em parte
- ○ Não concordo nem discordo
- ○ Concordo em parte
- ○ Concordo totalmente

8. Bloqueio do computador

8.1. Não existe qualquer tipo de risco em deixar o meu computador de trabalho com a sessão desbloqueada quando me ausento. *

Por favor selecione uma opção.

- ○ Discordo totalmente
- ○ Discordo em parte
- ○ Não concordo nem discordo
- ○ Concordo em parte
- ○ Concordo totalmente

9. Senha de acesso (parte 1)

9.1. Utilizo a mesma senha para aceder aos diversos programas informáticos que uso normalmente. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

9.2. Na construção das minhas senhas utilizo normalmente palavras ou números que me identificam (por exemplo nome, data de nascimento, nome do filho, NIP, etc.) *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

9.3. Na construção das minhas senhas tenho a preocupação em conjugar números, letras e caracteres especiais (por exemplo &, #, @, etc.) *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

10. Senha de acesso (parte 2)

10.1. Para não me esquecer das minhas senhas escrevo-as num papel. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

10.2. Partilho a(s) minha(s) senha(s) com outros utilizadores na organização. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

10.3. Quando altero a senha do meu computador de trabalho dou conhecimento da mesma a algum colega para este poder aceder ao meu computador. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

11. *Internet* e Correio Eletrónico

11.1. Considero importante analisar o assunto de uma mensagem de correio eletrónico, antes de a abrir. *

Por favor selecione uma opção.

- ○ Discordo totalmente
- ○ Discordo em parte
- ○ Não concordo nem discordo
- ○ Concordo em parte
- ○ Concordo totalmente

11.2. É um bom procedimento eliminar uma mensagem de correio eletrónico com um remetente desconhecido, antes de a abrir. *

Por favor selecione uma opção.

- ○ Discordo totalmente
- ○ Discordo em parte
- ○ Não concordo nem discordo
- ○ Concordo em parte
- ○ Concordo totalmente

11.3. A utilização da *Internet* para efetuar downloads de filmes e/ou jogos não representa qualquer ameaça para a Segurança da Informação. *

Por favor selecione uma opção.

- ○ Discordo totalmente
- ○ Discordo em parte
- ○ Não concordo nem discordo
- ○ Concordo em parte
- ○ Concordo totalmente

12. Incidentes com os sistemas de informação

12.1. Quando deteto alguma anomalia estranha no meu computador, como por exemplo este desligar-se sozinho, contacto de imediato o centro de informática da minha unidade. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não

- ○ Não, pois nunca me disse para fazer isso.

12.2. Considero ser importante contactar o centro de informática da minha unidade quando o meu computador de trabalho reinicia sozinho, sem motivo aparente. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não
- ○ Não, pois nunca me disse para fazer isso.

13. Mecanismos de segurança

13.1. Tenho instalado no meu computador de trabalho software *antivírus*. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não
- ○ Não sei
- ○ Nunca ouvi falar em *antivírus*

13.2. Tenho instalado no meu computador de trabalho software *antispyware*. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não
- ○ Não sei
- ○ Nunca ouvi falar em *antispyware*

13.3. Tenho instalado no meu computador de trabalho um mecanismo de segurança contra intrusões de terceiros (*firewall*). *

Por favor selecione uma opção.

- ○ Sim
- ○ Não
- ○ Não sei
- ○ Nunca ouvi falar em *firewall*

13.4. A existência de mecanismos de segurança como *antivírus*, *antispyware* e *firewall* instalados no meu computador é sinónimo de segurança. *

Por favor selecione uma opção.

- ○ Discordo totalmente
- ○ Discordo em parte
- ○ Não concordo nem discordo
- ○ Concordo em parte
- ○ Concordo totalmente

14. Medidas de segurança

14.1. Tenho conhecimento das medidas de segurança que se devem efetuar enquanto utilizador de um sistema de informação. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não
- ○ Nunca ouvi falar em "medidas de segurança"

14.2. Considero que é importante existirem políticas de segurança que indiquem quais medidas de segurança devem ser cumpridas pelos utilizadores dos sistemas de informação. *

Por favor selecione uma opção.

- ○ Discordo totalmente
- ○ Discordo em parte
- ○ Não concordo nem discordo
- ○ Concordo em parte
- ○ Concordo totalmente

14.3. A organização deve divulgar as medidas de segurança a serem cumpridas pelos utilizadores dos sistemas de informação através de ... *

Por favor selecione uma ou mais opções.

- ☐ Documento escrito com acesso livre através do Portal Interno.
- ☐ Sessões de sensibilização dos utilizadores junto das unidades.
- ☐ Durante a formação dos militares com a existência de uma disciplina própria.
- ☐ Cada Sistema de Informação devia conter um manual de políticas de segurança a adotar.
- ☐ Não considero importante a divulgação de políticas de segurança.
- ☐ Outra: _____

14.4. Tenho conhecimento que existe uma Política de Segurança da Informação e dos Sistemas de Informação e Comunicações na Força Aérea. *

Por favor selecione uma opção.

- ○ Sim
- ○ Não
- ○ Já ouvi falar mas não sei do que se trata.

Apêndice C — Respostas abertas “Meio de divulgação

Outras
Pop-ups que fiquem abertos durante x tempo, 1 min, por exemplo, de forma a dar dicas de segurança
Divulgação por newsletter via GW
DIRECTIVA INTERNA
Durante a formação dos militares com informação inserida numa disciplina associada e não própria.
e-mail
DIvulgar por GW
Por GW com dicas de segurança da informação
pop-ups aleatóricos nas aplicações
Cumprimento do estipulado no SEGMIL1 e AD70-1 SDIP 293, etc
Email regulares da DCSI para divulgação de boas práticas na utilização de SI e material informático da FAP.
Através das newsletters enviadas pelo self-service
um briefing na apresentaçáo do militar
Documento que é assinado pelo militar em como tomou conhecimento sempre que é colocado e sempre que existirem atualizações
Na janela de Login deveriam existir "informações diárias" sobre procedimentos, cuidados a ter, alertas, dicas... etc... Ninguém lê os manuais e apesar de necessários, não são práticos.
divulgação de newsletters por GW
Execução de exercícios para treino e teste das medidas de segurança. Cursos obrigatórios em e-learning.
Documento escrito ou online mas ambos com necessidade de validação/assinatura
aplicação de todas as respostas anteriores excepto a não divulgação de politicas de segurança
Por GroupWise, referente aos sistemas que tem instalados
Uso de newsletters por via de GW
MSG temporária no Login Script do utilizador (Novell Client) com tópicos curtos e a explicar onde ir para ter acesso à informação. Nem todos os militares lêem o Portal Interno de alto a baixo!
Devia ser associado o acesso a um sistema de informação a um elemento de segurança fisica (exemplo cartão de acesso á unidade)
Deveriam ser feitas auditorias periódicas e inopinadas e sessões expositivas dos procedimentos de segurança.
Documento escrito com acesso livre através do Portal Interno., Sessões de sensibilização dos utilizadores junto das unidades., Newsletter Groupwise

Apêndice D — Entrevistas realizadas

Todas as entrevistas realizadas foram feitas via *e-mail*.

Entrevista ao Diretor da DCSI - BGEN/ENGEL José Augusto N. V. Passos Morgado

Respostas por e-mail a 9 de abril de 2018

1. Na sua opinião, quais são atualmente as principais ameaças e/ou vulnerabilidades à Segurança da Informação nos SI desenvolvidos na FA?

Ao nível das Ameaças poder-se-ão destacar as Ameaças Cibernéticas a nível global, nomeadamente, o Ciberterrorismo e a Cibercriminalidade. A maioria destas ameaças tem como objetivo a disrupção dos SI/TIC indispensáveis ao funcionamento da estrutura macro da sociedade, colocando em causa a Segurança da Informação Digital e os 3 princípios básicos que lhe estão subjacentes: Confidencialidade, Integridade e Disponibilidade.

Ao nível das Vulnerabilidades poder-se-ão salientar: i) vulnerabilidades de âmbito tecnológico (conhecidas e desconhecidas) e que podem ser exploradas pelos atacantes dos SI/TICs; e ii) vulnerabilidades inerentes a uma deficiente utilização daqueles SI/TICs.

2. Que medidas de segurança e prevenção podem contribuir para que os princípios da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade) estejam assegurados na utilização destes sistemas?

A Força Aérea tem como objetivo, no âmbito da CiberDefesa - através da política definida no contexto do seu Manual RFA 390-6 - cumprir o princípio de defesa em profundidade, princípio, este, que consiste na implementação/edificação de diversas barreiras de segurança informática para proteção das SI/TIC. Estas barreiras, para além das medidas de natureza técnica que lhes estão subjacentes, incluem, ainda, outros tipos de medidas/ações, das quais se destacam, de entre outras, as seguintes: formação dos utilizadores, normativos de utilização e segurança física no acesso a instalações.

3. Na sua opinião, qual a importância do utilizador de SI para a Segurança da Informação na FA?

A utilização deficiente dos SI/TIC constitui, hoje, talvez a maior ameaça à segurança daqueles sistemas. De facto, a formação dos Utilizadores relativamente à utilização correta e adequada dos SI/TICs, e o seu conhecimento sobre as ameaças de natureza Cibernética a que estão sujeitos aqueles Sistemas é indispensável à manutenção da Segurança da Informação na Força Aérea. Como exemplo ilustrativo relativamente aos riscos inerentes à deficiente utilização dos SI/TIC refere-se, por exemplo, que a Engenharia Social é, hoje, a melhor forma de um atacante conseguir ganhar vantagem e explorar deficiências dos SI/TICs de uma Organização.

4. De que modo o comportamento dos utilizadores dos SI desenvolvidos na FA pode contribuir para a Segurança da Informação na FA?

Uma utilização consciente dos SI/TICs por parte dos utilizadores constitui um fator muito importante para a Segurança da Informação, seja nos SI desenvolvidos na Força Aérea, seja nos SI adquiridos por este Ramo das Forças Armadas a parceiros. O foco deverá estar centrado na Segurança da Informação, visto que todos os Sistemas em produção processam Informação da Organização.

5. De que forma a adoção de medidas de segurança preventivas pelos utilizadores pode contribuir para a Segurança da Informação na FA?

Em conformidade com o exposto, uma utilização consciente dos SI/TICs por parte dos Utilizadores, contribui, em grande parte, para uma melhoria da Segurança da Informação da Força Aérea.

6. Considera que os utilizadores de SI desenvolvidos na FA têm conhecimento de quais as medidas de segurança a adotar para a Segurança da Informação na FA?

Considero que existe, ainda, algum trabalho a levar a cabo no âmbito da melhoria da awareness dos utilizadores relativamente aos SI/TICs da Força Aérea.

7. Existe alguma formação/sensibilização sobre a "Segurança da Informação" aos utilizadores dos SI desenvolvidos na FA?

Existe formação na área da Segurança Informática na AFA e no CFMTFA, bem como no Curso de Gestão de Matérias Classificadas ministrado no EMFA. Para além disso é realizado, anualmente, na Força Aérea, o Exercício CiberPerseu, com o objectivo de treinar e sensibilizar os utilizadores em questões relacionadas com Segurança Informática.

8. Em caso de resposta afirmativa à questão anterior, de que forma é transmitido esse conhecimento? (por exemplo: pessoal qualificado para dar formação, cursos de formação na AFA e CFMTFA com palestras sobre o assunto, etc…)

No CFMTFA, por exemplo, as formações e palestras sobre Segurança Informática são dadas em conjunto por militares do CFMTFA e da DCSI. A restantes palestras e ações de sensibilizações são transmitidas por militares da DCSI.

Entrevista ao Chefe da DIVCSI - COR/ENGINF Ana Cristina D. O. Rodrigues Telha
Respostas por e-mail a 24 de abril de 2018

1. Na sua opinião, quais são atualmente as principais ameaças e/ou vulnerabilidades à Segurança da Informação nos SI desenvolvidos na FA?

As duas principais vulnerabilidades à segurança da Informação nos SI desenvolvidos na Força Aérea prendem-se com a falta de formação dos programadores e de analistas de sistemas bem como a falta de um processo de auditoria de segurança ao código e à arquitetura dos Sistemas de Informação.

2. Que medidas de segurança e prevenção podem contribuir para que os princípios da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade) estejam assegurados na utilização destes sistemas?

Algumas das medidas fundamentais para garantir os cinco pilares da Segurança e a Superioridade da Informação (Confidencialidade, Integridade, Disponibilidade, Autenticação e Não-Repúdio) são as seguintes:

- Definição clara de Doutrina e Políticas de Segurança (inclui a definição de uma estratégia);
- Acreditação das Redes Seguras;
- Existência de um "Business Continuity Plan";
- WAC (*Workstation Access Control*), para controlar as portas *USB* e proteger os dados nos dispositivos USB;
- Software AV (Anti-Virus) atualizado nas workstations e servidores;
- Utilização de apenas software autorizado e testado;
- Utilização de autenticações e passwords fortes;
- Sistemas de Deteção/Prevenção de Intrusão (IDS/IPS);
- *System Patching;*
- *System Log Audinting*;
- Dispositivos que protejam as nossa fronteiras (*Firewall, Proxy Servers, Mail Guard*);
- Resposta a incidentes.

3. Na sua opinião, qual a importância do utilizador de SI para a Segurança da Informação na FA?

As ameaças podem ser Internas (Acidentais ou deliberadas), Externas ou Acidentais (Fogo, Inundação, etc.). Várias estatísticas provam que as maiores ameaças para os SI das Organizações são Internas.

4. De que modo o comportamento dos utilizadores dos SI desenvolvidos na FA pode contribuir para a Segurança da Informação na FA?

Alguns dos comportamentos preventivos são:

- Utilização rigorosa das políticas de segurança instituídas;
- Mudança frequente de passwords;
- Utilização de passwords fortes;
- Utilização segura dos dispositivos de armazenamento móveis;

- Atenção contínua à Engenharia Social utilizada por "hackers", para conduzir as pessoas a realizarem ações que normalmente não fariam a um desconhecido, como por exemplo fornecer a "password" da rede Wifi da Organização, conta/palavra passe de utilizador de acesso ao seu computador, ou para finalizar dados pessoais;

- Evitar o acesso a links ou sites suspeitos;

- Manter-se atento aos *malwares* (incluindo *ransomware* e *phishing*), os *scarewares*, os *botnets*, os ataques de negação de serviço (DoS) e os ataques em redes sociais. Uma pessoa distraidamente, num gesto de rotina, pode abrir um ficheiro infetado (sendo sempre necessário pensar antes de clicar).

- Comunicar superiormente sempre que suspeite de uma tentativa ou quebra de segurança.

5. De que forma a adoção de medidas de segurança preventivas pelos utilizadores pode contribuir para a Segurança da Informação na FA?

Se a maior vulnerabilidade de um SI é o comportamento dos seus utilizadores, a única forma de minimizar os riscos é promover e instituir uma "cultura de segurança". Só a implementação de uma "cultura de segurança", entendida como um conjunto de valores, atitudes, percepções, competências e padrões de comportamento, irá permitir de uma forma sinérgica e contínua fazer face a uma realidade em que as ameaças se tornam cada vez mais globais e em que os cenários mais inverosímeis parecem, afinal, poder concretizar-se quando menos se espera.

6. Considera que os utilizadores de SI desenvolvidos na FA têm conhecimento de quais as medidas de segurança a adotar para a Segurança da Informação na FA?

É difícil de saber se todos os utilizadores têm conhecimento das melhores práticas de segurança. No entanto, considera-se já existir na FA, de um modo geral, algum conhecimento e sensibilização para a importância este assunto. Agora, se isso se traduz na aplicação concreta de medidas de segurança não se consegue avaliar.

7. Existe alguma formação/sensibilização sobre a "Segurança da Informação" aos utilizadores dos SI desenvolvidos na FA?

Sim, já existe.

8. Em caso de resposta afirmativa à questão anterior, de que forma é transmitido esse conhecimento? (por exemplo: pessoal qualificado para dar formação, cursos de formação na AFA e CFMTFA com palestras sobre o assunto, etc…)

Existem cursos, palestras, exercícios e ações de formação adequados ao tipo de utilização e responsabilidade nos SI da FA. O Exercício Ciber Perseu por exemplo, é aproveitado para avaliar e sensibilizar os utilizadores nas Unidades sobre as melhores práticas de segurança. Por outro lado, existem outras formações para quem tem responsabilidades mais específicas na utilização dos SI como é

o caso do curso de segurança dado pelo Subregisto ou um do IDN. A nível dos currículos dados na AFA ou no CFMTFA desconhece-se qual a abrangência da formação e sensibilização nesta área da segurança da informação.

Entrevista ao Chefe da RTI - TCOR/TINF José Manuel Ventura Pereira Mendes

Respostas por e-mail a 02 de maio de 2018

1. **Na sua opinião, quais são atualmente as principais ameaças e/ou vulnerabilidades à Segurança da Informação nos SI desenvolvidos na FA?**

Ameaças Cibernéticas existentes no mundo global, como o ciberterrorismo e a cibercriminalidade. A maioria destas ameaças tem como alvo redes indispensáveis ao funcionamento da estrutura macro da sociedade, colocando em causa a Segurança da Informação Digital e os 3 princípios básicos (Confidencialidade, Integridade e Disponibilidade).

Ao nível das vulnerabilidades, podemos enunciar as vulnerabilidades tecnológicas conhecidas e desconhecidas, que podem ser exploradas pelos atacantes nos SI/TICs e a vulnerabilidade humana na deficiente utilização dos SI/TICs.

2. **Relativamente à Segurança da Informação dos SI desenvolvidos internamente, que mecanismos de segurança são utilizados na FA como medida de segurança e prevenção, e como é feito essa utilização?**

Podemos dividir os mecanismos tecnológicos e respetivas implementações de segurança utilizadas em 5 níveis essenciais: Inventário, Perímetro e Controlo da Rede, Equipamentos e Dispositivos, Aplicações e Dados.

A primeira preocupação de uma Organização ao nível tecnológico será o controlo de todos os seus Ativos Tecnológicos (*Routers*, *Switchs*, Servidores, Postos de Trabalho, etc). Sem Inventário o processo de segurança diminui drasticamente, visto que não conseguimos perceber o que necessitamos de proteger.

Para os outros níveis são utilizados diversos mecanismos, como por exemplo:

Perímetro e Controlo da Rede – *Firewalls*, IPs, SIEM, ...

Equipamentos e Dispositivos – Controlo e Configuração de Software, *Patching*, Anti-Vírus e Anti-*Malware*, *Software* de Analise de Vulnerabilidades ...

Aplicações – Autenticação, Autorização e Auditoria (AAA), Encriptação, Software de Análise de Vulnerabilidades ...

Dados – Backups, Gestão de Acessos, *Logging* ...

A maioria destes mecanismos é configurado para atuar automaticamente, sendo que os mecanismos de auditoria, como por exemplo o Software de Análise de Vulnerabilidades, são utilizados manualmente em determinadas circunstâncias.

3. **De que forma os SI desenvolvidos na FA asseguram os princípios da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade) da FA?**

Em primeiro lugar, o desenvolvimento desses Sistemas de Informação deve ser efetuado segundo boas práticas previstas em normativos sobre segurança (por exemplo, OWASP).

Em produção, a RTI utiliza mecanismos e implementações sobre esses Sistemas de Informação, que visam assegurar que cada um dos princípios é mantido, como por exemplo:

Confidencialidade da Informação – utilização de mecanismos de encriptação na sua transmissão;

Integridade da Informação – utilização de funções de Hashing na sua salvaguarda;

Disponibilidade da Informação – utilização de mecanismos de redundância.

4. **Na sua opinião, qual a importância do utilizador de SI para a Segurança da Informação na FA?**

A Engenharia Social é, hoje, a melhor forma de um atacante conseguir ganhar vantagem e explorar os SI/TICs de uma Organização. A formação dos Utilizadores na utilização dos SI/TICs e o conhecimento destes sobre as ameaças Cibernéticas a que estes estão sujeitos é indispensável à manutenção da Segurança de Informação na Força Aérea.

Entrevista ao Chefe da RSI - TCOR/TINF Duarte Virgílio Veiga Lopes

Respostas por e-mail a 27 de março de 2018

1. **Quantos utilizadores dos SI desenvolvidos na FA existem atualmente?**

No dia 4 de janeiro de 2018, existiam 7176 utilizadores registados, sendo 6595 efetivos.

2. **Existe, atualmente, algum SI desenvolvido na FA com acreditação de segurança?**

Não.

3. **Na sua opinião, quais são atualmente as principais ameaças e/ou vulnerabilidades à Segurança da Informação nos SI desenvolvidos na FA?**

Os SI desenvolvidos internamente na FA são para uso interno. Quero com isto dizer que funcionam apenas dentro da WAN da FA, podendo no entanto funcionar na rede da defesa nacional (SICOM). Assim, a protecção, para estes SI, é essencialmente da protecção periférica.

4. **Que medidas de segurança e prevenção podem contribuir para que os princípios da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade) estejam assegurados na utilização destes sistemas?**

Um bom SGBD; Uma boa rede de comunicações; Um Data Centre robusto e protegido;

Formação e aconselhamento dos utilizadores, para adoção de boas práticas.

5. **De que forma os SI desenvolvidos na FA asseguram os princípios da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade) da FA?**

   Acesso através do binómio USERID – Password; Passwords fortes; Regras de acesso para ir ao encontro do princípio – ver apenas o que deve, de acordo com as suas funções, e restringir tudo resto; Base de dados protegidas; Constante assessoria e aconselhamento dos utilizadores.

6. **Na sua opinião, qual a importância do utilizador de SI para a Segurança da Informação na FA?**

   O utilizador é peça fundamental, se um utilizador não seguir uma conduta de boas práticas põe em risco qualquer sistema.

7. **De que modo o comportamento dos utilizadores dos SI desenvolvidos na FA pode contribuir para a Segurança da Informação na FA?**

   Se tiver comportamentos de risco como: A partilha de senhas de acesso (passwords); Retirar informação para uso indevido; Ter dados guardados no PC em vez de estarem na rede.

8. **De que forma a adoção de medidas de segurança preventivas pelos utilizadores pode contribuir para a Segurança da Informação na FA?**

   Sendo o utilizador um dos focos de elevado risco, estes devem ter: Formações adequadas; Devem ser "evangelizados" no sentido de adotarem boas práticas no uso dos SI.

9. **Considera que os utilizadores de SI desenvolvidos na FA têm conhecimento de quais as medidas de segurança a adotar para a Segurança da Informação na FA?**

   Sim considero até porque os Administradores de Informação (AdI's) levam a cabo ações de formação, aconselhamento e práticas adotar, para que não haja, quer dados incoerentes nos sistemas, quer problemas de segurança dos mesmos