INSTITUTO POLITÉCNICO DE LISBOA
ESCOLA SUPERIOR DE TECNOLOGIA DA SAÚDE DE LISBOA

UNIVERSIDADE DO ALGARVE
ESCOLA SUPERIOR DE SAÚDE

Avaliação das atitudes e comportamentos de cibersegurança dos profissionais de saúde em ambiente hospitalar

Paulo Manuel Roque da Silva Lopes Nunes

Orientadora

Professora Doutora Carina Soares da Silva

Instituto Politécnico de Lisboa

Escola Superior de Tecnologia da Saúde de Lisboa (ESTeSL)

Coorientador

Professor Doutor Mário João Gonçalves Antunes

Instituto Politécnico de Leiria

Escola Superior de Tecnologia e Gestão (ESTG)

MESTRADO EM GESTÃO E AVALIAÇÃO DE TECNOLOGIAS EM SAÚDE

Lisboa, 2019

INSTITUTO POLITÉCNICO DE LISBOA
ESCOLA SUPERIOR DE TECNOLOGIA DA SAÚDE DE LISBOA

UNIVERSIDADE DO ALGARVE
ESCOLA SUPERIOR DE SAÚDE

Avaliação das atitudes e comportamentos de cibersegurança dos profissionais da saúde em ambiente hospitalar

Paulo Manuel Roque da Silva Lopes Nunes

Orientadora

Professora Doutora Carina Soares da Silva

Instituto Politécnico de Lisboa

Escola Superior de Tecnologia da Saúde de Lisboa (ESTeSL)

Coorientador

Professor Doutor Mário João Gonçalves Antunes

Instituto Politécnico de Leiria

Escola Superior de Tecnologia e Gestão (ESTG)

MESTRADO EM GESTÃO E AVALIAÇÃO DE TECNOLOGIAS DA SAÚDE

Lisboa, 2019

“***Se a cultura é um facto aristocrático, a cultivação ciosa, assídua e solitária, de uma interioridade que se afina e opõe à vulgaridade da multidão (Heraclito:" Porque quereis extrair-me por toda a parte ò iletrados? Não escrevi para vós, mas para quem me pode compreender. Para mim, um vale cem mil, e nada a multidão"), então o simples pensamento de uma cultura partilhada por todos, produzida de modo a adaptar-se a todos, e elaborada à medida de todos, é um monstruoso contra-senso. A cultura de massas é a anti-cultura. Mas como nasce no momento em que a presença das massas na vida social se torna o fenómeno mais evidente de um contexto histórico, a "cultura de massa" não assinala uma aberração transitória e limitada : torna-se o sinal de uma queda irrecuperável, diante da qual o homem de cultura (último sobrevivente da pré-história destinada a extinguir-se) não pode senão dar um último testemunho em termos de Apocalipse.”***

(Umberto Eco; in Apocalípticos e Integrados)
1964

Agradecimentos

A concretização deste trabalho só foi possível graças ao suporte e colaboração de diversas pessoas a quem expresso os mais sinceros agradecimentos e uma palavra de apreço.

A Professora Doutora Carina Soares da Silva pela sua extraordinária capacidade construtiva e de aconselhamento teórico com que se dispôs ajudar-me neste trabalho, por todo o apoio e hábil orientação que permitiram a concretização deste projeto.

Ao Professor Doutor Mário João Gonçalves Antunes, coorientador deste trabalho, pelo seu "*know how*", apoio, confiança, entusiasmo e pelas orientações, reflexões e sugestões ao longo deste processo.

Aos meus Pais e irmão pelo suporte sempre constante em todos as fases da minha vida, pelo carinho, apoio e incentivo sempre presentes.

Um especial agradecimento à minha filha Sara e à sua irreverência e alegria própria da juventude que são contagiantes, o nunca baixar os braços perante as dificuldades da vida, uma fonte de motivação e orgulho da vida do pai.

Foi um processo pautado, por momentos complexos, alguns desertos e constantes desafios, vencidos com base numa perspetiva otimista e positiva de companheirismo, amizade e amor que nortearam esta etapa da minha vida e sem a qual não seria possível sem a tua presença Sónia.

Resumo

Introdução: A crescente digitalização das empresas e a sua crescente dependência da infraestrutura da *Internet* aumentaram as preocupações relacionadas com a privacidade e a confidencialidade dos dados. As instituições de saúde têm sido confrontadas com questões específicas, nomeadamente a sensibilidade dos dados, a especificidade dos equipamentos em rede e as competências médias em tecnologias de informação detidas pelos profissionais de saúde em Portugal.

Objetivos: Compreender o nível de relacionamento estabelecido pelos profissionais de saúde com a segurança da informação, avaliando atitudes e comportamentos em cibersegurança; identificar riscos e ações que possam ser tomadas para aumentar a sensibilização dos profissionais de saúde para a cibersegurança.

Metodologia: O estudo consiste em traduzir, adaptar e aplicar duas escalas de resposta tipo Likert previamente validadas e publicadas para avaliar as atitudes em relação à cibersegurança em ambiente empresarial (*ATC-IB*) e a comportamentos arriscados em cibersegurança (*RScB*) dos profissionais de saúde no ambiente hospitalar português. Trata-se de um estudo observacional, quantitativo, transversal e descritivo sobre atitudes e comportamentos de cibersegurança numa instituição de saúde em Portugal.

Resultados: A amostra foi constituída por 56 profissionais, 71% mulheres e 29% homens, divididos em quatro grupos profissionais, onde se obteve uma média (±SD) de 31,59 (±14,211) pontos para a escala *RScB* e 66,41 (±6,26) pontos para a escala *ATC-IB.* Não se observaram diferenças estatísticas entre os factores sociodemográficos estuados e a pontuação global das escalas.

Conclusões: Não se observaram diferenças estatísticas significativas entre os factores sociodemográficos e os valores obtidos em ambas as escalas. No entanto, os pontos das escalas para os diferentes domínios evidenciam diferença estatística entre idades, sexos e grupos profissionais por itens, sendo, portanto, pontos importantes para o desenvolvimento de estudos futuros. Os resultados evidenciaram uma relação entre os comportamentos adquiridos e as atitudes de envolvimento com o trabalho e compromisso organizacional, estabelecendo uma ponte para a quantificação em consciência.

Palavras chave: Cibersegurança, Consciencialização, Comportamentos, Atitudes, sistemas de informação saúde.

Abstract

Introduction: The growing digitization of businesses and its increasing dependence on *Internet* nfrastructure has boosted the concerns related to data privacy and confidentiality. Healthcare institutions have been challenged with specific issues, namely the sensitivity of data, the specificity of networked equipment and the average information technology skills held by of healthcare professionals in Portugal.

Objectives: To understand the relationship level established by healthcare professionals with the information security by assessing attitudes and behaviours in cybersecurity; to identify risks and actions that may be taken to enhance the healthcare professional's cybersecurity awareness.

Methodology: The study consists in translating, adjusting and applying two previously validated and published Likert-type response scales to assess attitudes towards cybersecurity in business environment (ATC-IB) and to the risky cybersecurity behaviours (RScB) of health professionals in the Portuguese hospital environment. This is an observational, quantitative, cross-sectional and descriptive study in cybersecurity attitudes and behaviours in a healthcare institution in Portugal.

Results: The sample was composed by 56 professionals, 71% women and 29% men, divided in four professional groups, where a mean (±SD) of 31.59 (±14.211) points was achieved for the cybersecurity risky behaviour (RScB) scale and 66.41 (±6,26) points for the cybersecurity and cybercrime in business attitudes scale (ATC-IB).

Conclusions: There was no-significant statistical differences between the sociodemographic factors and the scores obtained on both scales. However, the points of the scales for the different domains evidences a statistical difference between ages, genders and professional groups by items, which are therefore important points for the development of future studies. The results showed a relationship between acquired behaviours and the attitudes of involvement with work and organizational commitment, establishing a bridge for the quantification in awareness.

Keywords: Cybersecurity, Awareness, Behaviours, Attitudes, health Information Systems.

Índice Geral

Índice de tabelas

Índice de Figuras

Acrónimos, sinónimos e abreviaturas

AES	*Advanced Encryption Standard*
ANOVA	Análise de variância
ATC-IB	*Attitudes towards cybersecurity and cybercrime in business*
ATS	Avaliação de tecnologias de saúde
ATTNIPA	Assistente Técnico, Técnico de nível intermédio, Pessoal Administrativo.
CBeHIS	*Cross-Border eHealth Information Services*
CC	Consciencialização em Cibersegurança
CHBM	Centro Hospitalar Barreiro Montijo
CPC	Consciencialização para a Cibersegurança
CSI	Consciencialização em Segurança da Informação
DP	Desvio padrão
EPE	Entidade Pública Empresarial
eHealth	Saúde digital, todas as redes de informação e comunicação sobre saúde.
EUnetHTA	*European Network for Health Technology Assessment*
GATS	Gestão e Avaliação das Tecnologias em saúde
HIPAA	*Health Insurance Portability and Accountability Act*
HITEC	*The Health Information Technology for Economic and Clinical Health*
IA	Inteligência artificial
IoT	*Internet of things* (*internet* das coisas)
KAB	Modelo *KnowledgeAtittudeBehaviour*
ONRH	Observatório Nacional de Recursos Humanos
SER	Registo de Saúde Eletrónico
RGDP	Regulamento Geral de Proteção de Dados

RSA	*Rivest, Shamir and Adleman asymmetric encryption systems*
RScB	*Risky cybersecurity behaviours scale*
SI	Sistemas de informação
SIS	Sistemas de informação em saúde
SMS	Serviço de mensagens curtas, em inglês *Short Message Service*
SPMS	Serviços Partilhados do Ministério da Saúde, EPE
SW	*ShapiroWilk*
TI	Tecnologia da Informação
TIC	Tecnologias de informação e comunicação
TSDT	Técnico Superior de Diagnostico e Terapêutica
MFA	Autenticação multifatorial
EU	União Europeia
KW	*Kruskal-Wallis*
Wi-Fi	*wireless fidelity* ou fidelidade sem fio

1 Introdução

As questões relacionadas com a segurança da informação em saúde são múltiplas e complexas constituindo uma temática difícil de delimitar e gerir pela sua interdisciplinaridade e transversalidade.

As temáticas da segurança da informação e da relação que os profissionais estabelecem para a segurança dos dados que são confiados numa realidade em permanente alteração de sistemas de informação e virtualização de processos, telemedicina e inteligência artificial em saúde, interoperabilidade de sistemas, parcerias entre instituições de saúde, disponibilização de informação de saúde pública e privada em plataformas digitais, autonomia individual e a cidadania em saúde dos utentes e dos profissionais de saúde evidência a abrangência e a multidimensionalidade de saberes que dificultam os processos de tomada de decisão sobre segurança da informação e as suas implicações atuais e futuras para colmatar vulnerabilidades e aumentar a resiliência dos sistemas.

No entanto, e apesar do crescente alerta para os perigos e incidentes em cibersegurança pelas instituições responsáveis, e ao apelo à manutenção de um ambiente *online* seguro são poucos os estudos de avaliação e medição das diferenças individuais dos profissionais nas organizações ou entidades de saúde, que permitam determinar a existência de ameaça interna não intencional.

As Tecnologias da Informação (TI) evoluíram rapidamente nas últimas décadas, passando de um nicho tecnológico a uma realidade global em constante evolução. Na área da saúde não foi diferente, tendo a transformação digital das entidades de saúde potenciado novas oportunidades de desenvolvimento da qualidade, da investigação de novos tratamentos e uma melhor utilização dos dados e de gestão, iniciando um novo paradigma de medicina.

Contudo, esta transformação digital nem sempre foi acompanhada pela crescente preocupação em relação à cibersegurança de dados e equipamentos, tornando as entidades de saúde em alvos bastante atrativos por duas razões fundamentais: primeiro pelo valor dos dados confiados e segundo, por se regerem por medidas de cibersegurança básicas.

A presente dissertação pretende contribuir para a ampliação do conhecimento sobre aspetos humanos em segurança da informação, nos sistemas de informação da saúde (SIS) em particular pela sensibilidade dos dados de saúde contidos na forma sob a forma de

registos de saúde eletrónico (RSE). Propõe-se, portanto, conhecer quais os comportamentos e as atitudes em relação à cibersegurança atuais dos profissionais de saúde, em ambiente hospitalar.

O estudo da consciencialização em cibersegurança dos profissionais de saúde e dos factores sociodemográficos que condicionam a segurança dos SIS é pertinente porque quando os dispositivos e SIS não funcionam tal como previsto, a segurança e o acesso a cuidados de saúde de qualidade, durante todo o tempo e em todos os níveis da prestação, fica comprometida ficando os cidadãos privados de um direito fundamental. Quando qualquer dos dispositivos médicos ou SIS fica refém de programas mal-intencionados de encriptação, todo o sistema fica paralisado podendo existir fugas de informação valiosas de repercussões imprevisíveis e dando origem a lucros ilícitos com perdas de reputação das entidades de saúde envolvidas.

No contexto atual de mudanças tecnológicas que o setor da saúde vive é importante conhecer as atitudes e os comportamentos humanos em cibersegurança para melhor compreender, quer os impactos dessas mudanças, quer as atuais e futuras necessidades formativas das equipas. A análise de risco deverá ser teoricamente um ciclo contínuo e iterativo, essencial para o desenvolvimento de competências digitais próprias de um modelo holístico em cibersegurança, que acompanhem os novos paradigmas de saúde emergentes e os desafios que eles representam.

É importante compreender que todas as tecnologias desenvolvidas pelo homem apresentam vulnerabilidades de segurança, próprias da natureza e da imperfeição humana. Este facto por si só, não deverá ser encarado como algo desmotivante ou como uma inevitabilidade de uma causa perdida, mas como um facto próprio do processo de desenvolvimento tecnológico, inseridos num processo de melhoria continua. A melhor forma de minimizar vulnerabilidades conhecidas e desconhecidas das tecnologias é de controlar o risco de perda de informação ou de cativação de sistemas é através de um processo de gestão continua de análise, avaliação e mitigação, envolvendo todos num processo continuo de treino focado no pensamento proativo, nas boas práticas de segurança dos sistemas de informação como forma de prevenção e manutenção dos SIS e dos dados neles contidos.

1.1 Enquadramento e Relevância da Temática

Esta dissertação inserida no mestrado em Gestão e Avaliação de Tecnologias em Saúde (GATS) lecionada pela Escola Superior de Tecnologias de Saúde de Lisboa (ESTESL) é o culminar de uma investigação concretizada nos domínios da avaliação de tecnologias de saúde (ATS).

Para melhor enquadrar a temática da investigação é necessário clarificar inicialmente o conceito base inerente à conceção do domínio de ATS.

Segundo a *European Network for Health Technology Assessment* (*EUnetHTA)* a ATS é definida como um "*processo multidisciplinar, firmemente alicerçado em investigação e métodos científicos, que analisa e resume informação clínica, social, económica e ética relacionada com a utilização de tecnologia de saúde, de forma sistemática, robusta, transparente e sem viés. O seu objetivo é promover a informação necessária à formulação de políticas de saúde seguras e efetivas, focadas no doente, e que procurem atingir o melhor valor possível*" (1).

É necessário também compreender que a tecnológico atual tem evoluído rapidamente, por vezes demasiado rápido para a sociedade se adaptar a este processo acelerado de transformação "digital".

Nunca as sociedades e os seus cidadãos estiveram tão ligados e simultaneamente tão vulneráveis às manipulações, à contra informação e às notícias falsas que de qualquer forma tentam orientar as massas e extrair ou incutir tendências com os mais variados intuitos, nem sempre claros.

O sector da saúde acompanhou este desenvolvimento tecnológico, assistindo-se à evolução dos RSE e à expansão dos sistemas de informação em saúde (SIS) e da sua conectividade.

Atualmente a dependência dos sistemas de informação na área da saúde é crescente, alicerçando a medicina baseada na evidência. A partilha de resultados de análises, imagens médicas, diagnósticos e medicações ou tratamentos é algo transversal nas organizações de saúde. Os dados sensíveis circulam entre diferentes aplicações por diferentes profissionais, num logica de segurança que necessita de maior atenção.

Não é exagero dizer que tanto os provedores de serviços de saúde quanto os fornecedores precisam abordar a cibersegurança com maior preocupação das que são hoje praticadas. Hoje em dia, nenhuma entidade de saúde é uma ilha, o diagnóstico

médico encontra-se em constante evolução tornando-se personalizado, preventivo, preditivo e participativo centrado no indivíduo (2)(3).

Os registos de doenças, de resultados laboratoriais ou tratamentos, inclusive os dados genéticos provenientes de equipamentos e dispositivos médicos com capacidade de conectar à *internet*, a intitulada *internet* das coisas (*IoT)*, dados de nutrição, estilo de vida e até histórico familiar, contidos numa única base de dados de forma a maximizar tratamentos e otimizar a medicina preventiva, possibilitam o desenvolvimento de novos estudos clínicos, análise de efeitos colaterais e/ou novas descobertas(4).

Estes novos avanços tecnológicos na área da informação e comunicação em saúde abrem a porta a novas e estimulantes possibilidades da medicina, tornando esta mais abrangente e mais participativa à sociedade moderna com diferentes perceções e novos comportamentos da realidade da saúde individual e coletiva.

A mudança de paradigma de saúde é impulsionada pelo avanço tecnológico registado quer no sistema digital em saúde, quer na tecnologia aplicada à saúde, passando pela partilha de conhecimentos e pelo aumento da literacia dos cidadãos.

O resultado é o desenvolvimento de novos modelos sociais de relacionamento de novos comportamentos e atitudes quanto à compreensão da realidade da saúde individual e coletiva, que traduz uma mudança na relação de confiança entre o profissional da saúde e o utente que cada vez mais informados e conhecedor da sua própria condição médica.

Esta nova forma de olhar para a saúde apresenta crescentes preocupações de segurança da informação e da aplicação dos novos utensílios digitais em saúde para os profissionais e para os cidadãos, os quais passarão, neste novo paradigma, a controlar os seus próprios dados de saúde podendo questionar a autoridade médica, pela crescente partilha de informação em redes de informação e comunicação sobre saúde, disponíveis *online*, dirigidas ao público em geral, mas também aos profissionais de saúde.

Inúmeros são os casos já conhecidos de ataques realizados e perda de reputação e informação sensível em entidades de saúde, sobressaído o ataque de *ransomware* ocorrido a 12 de maio 2017 que conseguiu afetar mais de 200 mil sistemas em 150 países incluindo o serviço nacional de saúde britânico (*NHS*) (5). Além do impacto negativo no *NHS* também foi divulgado o caso do Centro Médico *Presbyterian* em *Hollywood*, com uma paragem de 10 dias e ao pagamento de um resgate de 17 000 dólares(6)(7)(8).

Estes casos documentados e outros, conduziram à produção e divulgação de um conjunto de conselhos úteis e práticos de segurança em TI. No entanto, apesar do crescente alerta para os perigos e incidentes em cibersegurança pelas instituições responsáveis, e do apelo à manutenção de um ambiente *online* seguro, são poucos os estudos empíricos de avaliação e medição das diferenças individuais dos utilizadores em segurança da informação dentro das organizações ou entidades de saúde, que permitam determinar a existência de ameaça interna não intencional(9).

Esta lacuna de investigação entre a relação que os profissionais estabelecem para a segurança dos dados que são confiados favorece o desenvolvimento de políticas restritivas de segurança e de mitigação apenas através de soluções técnicas de limitação de acessos ou privilégios(10).

Mas a realidade é de ausência de sistemas perfeitos, isentos de vulnerabilidades quer estruturais quer de *software*. Este facto lança o mote para a necessidade de apostar no desenvolvimento de processos holísticos em cibersegurança.

Os últimos indicadores do Observatório Nacional de Recursos Humanos (ONRH) relativos ao envolvimento e lealdade dos profissionais referem discrepâncias entre os profissionais do setor público e do privado.

A resistência à mudança e à inovação por parte dos recursos humanos, é o indicador mais relevante do estudo (Figura 1.1), por demostrar a relutância existente para levar a cabo alterações nos procedimentos instituídos e que podem de alguma forma contribuir para uma vulnerabilidade de segurança.

É neste contexto complexo que se insere a temática da cibersegurança em saúde e a pertinência deste tema, onde a formação dos utilizadores é um importante catalisador da implementação das políticas de segurança da informação e das TIC das entidades de saúde.

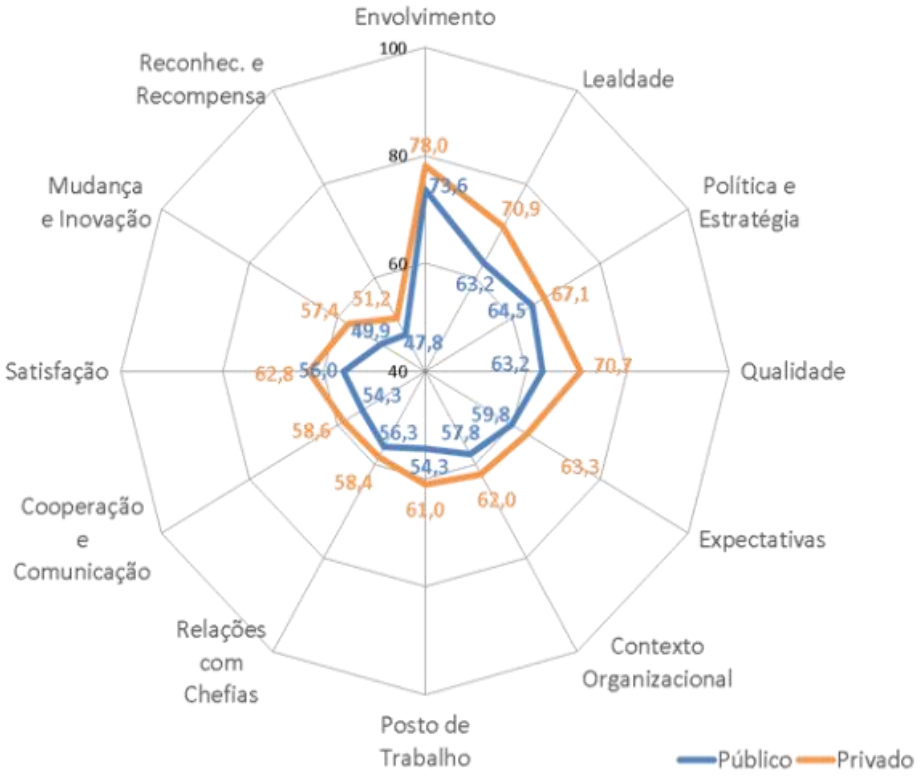


Figura 1.1 - Índices médios dos setores público e privado (2017).

fonte:http://www.onrh.org/barometro.php

1.2 **Objetivos**

É essencial num processo de gestão, conhecer inicialmente a realidade do capital profissional no sector da saúde antes de delinear qualquer estratégia de mitigação de vulnerabilidades, em particular as relacionadas com a segurança dos RSE, evitando falhas e desarticulações entre os profissionais e as políticas de segurança, aumentando a adesão dos mesmos à problemática da cibersegurança.

A cibersegurança em saúde sustenta-se em grande medida também na forma através da qual os profissionais de saúde olham para a segurança da informação, o dito "*awareness*".

Que ameaça representam os profissionais de saúde para a proteção dos direitos individuais e para a privacidade da circulação descentralizada de informação em todos os níveis da prestação de cuidados de saúde?

O objetivo principal é ajudar a estabelecer bases para uma pesquisa orientada para a consciencialização da cibersegurança em saúde em ambiente hospitalar, identificando as principais atitudes em relação à cibersegurança em entidades empresariais de saúde e dos principais comportamentos arriscados em cibersegurança. É da articulação entre estas duas esferas (atitudes e comportamentos) que se permite conhecer a vulnerabilidade humana no setor da saúde.

Para desenvolver o estudo exploratório da consciencialização em cibersegurança dos profissionais de saúde recorre-se a dois questionários de avaliação métrica validados e publicados internacionalmente que serão traduzidos e adaptados para português e para o setor da saúde sobre os comportamentos arriscados em cibersegurança dos profissionais de saúde e as atitudes em relação à cibersegurança em entidades empresariais.

1.3 Estrutura da Investigação

Esta dissertação é composta por oito partes distintas centradas sobre a temática da cibersegurança e na relação que os profissionais da saúde estabelecem com a segurança do doente e com a gestão da informação que lhes é confiada. Pretende-se compreender melhor as atitudes para a cibersegurança e os comportamentos arriscados em cibersegurança dos profissionais como forma de mitigar os riscos e as vulnerabilidades relacionadas com os recursos humanos e aumentar a resiliência das organizações.

Para atingir os objetivos anteriormente formulados estruturou-se o estudo nas seguintes partes: Conceitos Fundamentais em Cibersegurança para melhor centrar a temática, Metodologia aplicada para a investigação, Resultados obtidos e o respetivo estudo estatístico com os factores sociodemográficos, discussão, conclusão, limitações e a bibliografia.

2 Conceitos Fundamentais em Cibersegurança

Atualmente a cibersegurança e a ciberdefesa são dois temas emergentes e que constituem uma preocupação crescente para governos, cidadãos, empresas e profissionais, fruto do acentuado do desenvolvimento tecnológico e da dificuldade dos utilizadores em acompanhar esse mesmo desenvolvimento.

Neste capítulo enumeram-se alguns dos principais conceitos associados à temática da cibersegurança em geral e a sua extensão à problemática da saúde.

2.1 Ciberespaço e Cibersegurança

O ciberespaço pode descrever-se como um espaço virtual onde se encontram interligados vários equipamentos eletrónicos, desde de computadores e outros dispositivos. O ciberespaço acomoda ainda os sistemas de informação de implementação da logica do negócio e das pessoas que operam os dispositivos. As ligações efetuadas entre os vários dispositivos podem ser de fio ou sem fio (ou seja, wireless – por ondas de rádio, infravermelhos, satélite) ou ambas. De forma mais complexa, o ciberespaço é definido como a rede interdependente de infraestruturas de tecnologia de informação, incluindo a *Internet*, redes de comunicação, sistemas de computador e processadores e de controladores parte de indústrias críticas (11).

A definição de Cibersegurança é ampla, tal como o seu universo, pode assim, definir-se como um conjunto de tecnologias, processos e práticas desenhado para proteger as redes, os computadores e outros dispositivos eletrónicos, programas e dados, de potenciais ataques ou ameaças (12), assim como a implementação de procedimentos de consciencialização e formação em segurança de TI (13).

A visão de “Um ciberespaço aberto, seguro e protegido” - é algo que a União Europeia (UE) procura promover, pela manutenção dos valores europeus de liberdade e democracia e para garantir que a economia digital se desenvolve em condições de segurança, promovendo simultaneamente o debate entre os estados membros sobre a melhor forma de prevenir e dar resposta às crescentes perturbações e ataques na *Internet* (14).

2.1.1 Cibersegurança na Saúde

Até 2016 a cibersegurança era algo em suspenso nas organizações de saúde (15), para além do pouco investimento em medidas de segurança, compreensível em parte pela natureza dos serviços prestados, é referido na literatura a ausência de medidas básicas como as atualizações e *backups* (16)(17)(18).

Na realidade, nenhuma entidade prestadora de cuidados de saúde demostrava este tipo de preocupação (6), tornando difícil que a indústria da saúde consiga assim conservar a integridade, confidencialidade e a acessibilidade dos RSE sem a cibersegurança. O ataque ao sistema de informação *NHS* pelo vírus *wannacry*, um *ransomware*, constituiu um ponto de viragem na cibersegurança na saúde, despertando a indústria da saúde para uma problemática sistematicamente esquecida, por razões economicistas e levianas de moralidade (19).

Ransomware é o último de uma longa série de demonstrações da inaptidão coletiva e, talvez, do desinteresse coletivo e institucional que culminaram com o ataque de 2016 ao sistema de saúde. Apesar dos progressos registados ao nível da cibersegurança nas organizações de saúde desde 2016, continuam a existir entidades vulneráveis que não executam as medidas de controle e segurança básicas (6).

É necessário proteger os RSE, a reputação e a credibilidade das organizações de saúde e manter o sigilo profissional (20); com a implementação da cibersegurança em saúde é necessário equipar e modernizar os hospitais e respeitar o RGPD seguindo uma política de segurança sóbria, sem excessos ou obsessões, e com o envolvimento dos profissionais de todas as áreas da saúde numa perspetiva sócio-tecnológica (18) num processo holístico.

A importância de manter o controlo dos dados em saúde é uma questão basilar, através de um conjuntos políticas e procedimentos para a informação de saúde pessoal de qualquer indivíduo, cuja manipulação deve ser feita de forma confidencial, segura e precisa por um profissional adequado, em que a ética e as normas de qualidade que um serviço de saúde moderno deve assegurar (21).

Os sistemas de saúde na UE são uma componente essencial dos elevados níveis de proteção social contribuindo para a coesão e para a justiça social entre cidadãos dos estados membros, bem como para o desenvolvimento sustentável dos diferentes modelos de sistemas de saúde europeus (22).

Foi então delineada uma estratégia europeia comum em cibersegurança para a segurança das redes e da informação em julho de 2015, para colmatar possíveis vulnerabilidades e aumentar a resiliência dos sistemas de informação em saúde.

A Diretiva relativa à segurança das redes e dos sistemas informáticos (*NIS - network and information systems directive*) foi adotada pelo Parlamento Europeu em 6 de julho de 2016 e é a primeira legislação abrangente sobre cibersegurança adotada a nível da UE num contexto em que os ciberataques são cada vez mais frequentes e têm consequências mais graves. O objetivo é alcançar um nível semelhante de capacidades de cibersegurança em todos os Estados-Membros da UE. Em setembro de 2017, a Comissão europeia voltou a reforçar os instrumentos existentes e apresenta novas iniciativas para continuar a melhorar a ciberresiliência e a capacidade de resposta da EU (23).

2.1.2 Regulação da Cibersegurança em Saúde

A SPMS – Serviços Partilhados do Ministério da Saúde, EPE, é a entidade responsável pela estratégia de segurança da informação e Cibersegurança, aplicada nas entidades de saúde e decorrente das responsabilidades definidas no Despacho n.º 8877/2017, publicado em Diário da República n.º 194/2017, Série II de 2017-10-09. Na sua missão podemos observar a cooperação, a partilha de conhecimentos e informação e o desenvolvimento de atividades de prestação de serviços nas áreas dos sistemas e tecnologias de informação e de comunicação, garantindo a operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação do Ministério da Saúde, e promovendo a definição e utilização de normas, metodologias e requisitos que garantam a interoperabilidade e interconexão dos SIS, entre si e com os sistemas de informação transversais à Administração Pública (24).

A 30 de outubro de 2018 a SPMS publicou na sua circular 7/2018/SPMS, um conjunto de responsabilidades às entidades por ele abrangidas, entre as quais se destacam:

- A elaboração de relatórios regulares sobre o perfil evolutivo da implementação das políticas e controlos de segurança na entidade, de forma a permitir avaliar e comparar níveis de maturidade;
- A necessidade de garantir a disponibilização dos recursos humanos, tecnológicos e financeiros, necessários para assegurar o cumprimento dos níveis de serviço definidos pela SPMS, E. P. E.;

- Assumir um papel participativo e colaborativo na partilha de boas práticas e de melhoria contínua para responder à dinâmica evolutiva dos diversos contextos de cibersegurança;
- Cumprir as medidas e procedimentos na área da cibersegurança;
- Promover em tempo útil a disponibilidade dos meios de proteção, deteção, resposta e recuperação reportando aos órgãos competentes, sempre que confrontada com situações que comprometam a segurança;
- Acompanhar, apoiar e monitorizar o desenvolvimento de medidas de proteção, deteção, resposta e recuperação dos recursos críticos locais;
- Adotar o modelo de avaliação para a gestão e monitorização das medidas de segurança (25).

2.1.3 A estratégia de Cibersegurança em Saúde

No plano europeu, e no âmbito da estratégia de cibersegurança, a Comissão Europeia propôs a diretiva da UE relativa à segurança das redes e da informação (SRI). A Diretiva SRI (UE 2016/1148) foi o primeiro ato legislativo da UE em matéria de cibersegurança. O objetivo era reforçar a cibersegurança em toda a UE. A diretiva SRI foi adotada em 2016 e, subsequentemente, por se tratar de uma diretiva da UE, cada Estado-Membro começou a adotar legislação nacional, que segue ou "transpõe" a diretiva. Estas diretrizes dão aos países membros algum nível de flexibilidade para levar em conta as circunstâncias nacionais, por exemplo, para reutilizar estruturas organizacionais existentes ou para se alinhar com a legislação nacional existente.

Neste sentido, a UE tomou a iniciativa de apoiar a gestão financeira relacionada com a cibersegurança a partir do orçamento da UE e simultaneamente reunir recursos com os Estados-Membros. A iniciativa permite identificar e apoiar projetos que são cruciais para aumentar a competitividade da indústria europeia de cibersegurança. O grande objetivo é transformar a cibersegurança numa vantagem competitiva das indústrias de diferentes setores (por exemplo, saúde, energia, transportes, finanças), por outro, estimular as autoridades públicas a protegerem os setores críticos com soluções de cibersegurança de ponta (26).

De acordo com o Plano Nacional de Saúde 2012-2016, o acesso a cuidados de saúde de qualidade, durante todo o tempo e em todos os níveis da prestação, é um direito fundamental do cidadão, a quem é reconhecida toda a legitimidade para exigir qualidade nos cuidados que lhe são prestados, sendo que a segurança é um dos elementos

fundamentais da qualidade em saúde. A segurança é um dado essencial para a confiança dos cidadãos no sistema de saúde e no Serviço Nacional de Saúde (SNS) em particular (27).

No plano Nacional de saúde extensão 2020, reforça-se políticas públicas contra a ocorrência de incidentes de segurança associados à prestação de cuidados de saúde por quatro eixos estratégicos transversais: Cidadania em Saúde, Equidade e Acesso Adequado aos Cuidados de Saúde, Qualidade em Saúde e Políticas Saudáveis.

Está subjacente o objetivo de obter ganhos em saúde, melhorar o desempenho do Sistema Nacional de Saúde, bem como a capacidade deste se desenvolver como um todo transversal a sociedade e aos cidadãos que a compõem. Estes objetivos passam por um fortalecimento de SIS para facilitar a tomada de decisão, integração de programas e projetos assim como intervenções focadas em resultados (28).

A crescente preocupação com o fortalecimento dos sistemas de informação em saúde, recorrente dos propostos estabelecidos no PNS levou a SPMS, EPE a lançar sob o lema "A Cibersegurança é uma matéria de todos", os "10 Mandamentos da Cibersegurança" (29) com o objetivo de aumentar o conhecimento e a utilização de boas práticas de todos os profissionais de saúde, sejam estes profissionais clínicos, prestadores de cuidados, profissionais TIC ou administrativos. Neste contexto, importa reforçar que a segurança é tanto maior quanto maior for a consciência ética dos seus utilizadores e as mudanças mais impactantes passam, principalmente, pelo desenvolvimento de uma Cultura e *Awareness* das organizações e dos seus profissionais nesta temática (29).

Assim, serão publicados e distribuídos pelas diversas entidades do SNS 10 mil post-its e autocolantes, com um conjunto de regras definidas de forma a que os profissionais de saúde possam melhor proteger os seus computadores e a privacidade dos seus utentes (29).

A implementação do Regulamento Geral sobre a Proteção de Dados (RGPD) é considerado como a base fundamental para uma das maiores alterações de sempre relativamente à forma como deve ser realizado o tratamento de dados pessoais na UE. A sua implementação ao ciberespaço da UE é simultaneamente um desafio e uma oportunidade, sendo este último particularmente relevante pelas implicações ao nível do melhoramento da cibersegurança (30).

Para o RGPD a denominação de dados pessoais sensíveis está relacionado com os dados que estão sujeitos a condições específicas para o seu tratamento,

nomeadamente direitos e decisões automatizadas. Um exemplo de dados sensíveis são os dados pessoais como a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde incluindo dados genéticos e amostras biológicas ou dados relativos à vida sexual ou orientação sexual de uma pessoa (31)(32).

A implementação de uma autenticação multifactorial forte, representa uma medida pratica mais eficiente em cibersegurança na saúde. Basicamente é exigir que dos profissionais a aplicação da autenticação multifactorial (*MFA*) para o acesso a aplicativos e sistemas de informação da entidade de saúde. Essa prática garante que as credenciais do profissional perdidas ou roubadas não possam ser usadas para obter acesso a sistemas internos não autorizados. A *MFA* bloqueia muitos ataques resultantes de roubos de credenciais, exigindo que os utilizadores apresentem informações adicionais para confirmar a sua identidade. Este sistema pode incluir fichas, métodos biométricos e um código enviado através de texto, e-mail ou voz (33).

2.1.4 Cibersegurança e a gestão de risco

É importante compreender que os riscos associados à cibersegurança podem ser geridos e mitigados, mas não eliminados. A escala e a complexidade associada à cibersegurança é demasiado grande para que possa existir uma solução definitiva, conduzindo as organizações a uma constante adaptação e coordenação eficazes para manter a resiliência dos sistemas contra ameaças criativas e dinâmicas. A análise de risco em cibersegurança deve, portanto ser um ciclo contínuo e iterativo defendido pelas principais partes interessadas, conduzido por uma equipa de profissionais qualificados em segurança da informação e ‘evangelizado’ por todo o pessoal com as boas praticas cibersegurança (34).

Os últimos estudos, apresentados em fevereiro 2018 pela *Microsoft/Marsh* (35) indicam que o risco de ciberataques cresceu em todos os setores económicos e governamentais. Os ataques têm-se modificado rapidamente quer em complexidade quer na forma como são geridos, em resultado especialmente do incremento e aplicação de tecnologias emergentes incluindo a inteligência artificial, a robótica, os equipamentos de IoT entre outros. Simultaneamente assiste-se a uma globalização dos ataques, que na maioria dos casos são patrocinados por estados/nações e pelo crime organizado (35).

Cada entidade deve proceder primeiro a uma avaliação do potencial de perdas, antes de implementar, qualquer programa de cibersegurança. Algo que é complexo para uma entidade e a quantificação económica das suas perdas de dados, recorrendo a estimativas. Este facto pode conduzir a investimentos insuficientes e/ou planos e políticas pobres em cibersegurança para o valor real dos seus dados. A crescente complexidade tecnológica e o impacto financeiro dos ciberataques nas organizações têm levado à adoção de políticas mais abrangentes e a investimentos na gestão de risco (35).

Os controlos dos SI devem ser adequados ao fim a que se destinam (ou seja, adequados e adequados à tarefa em questão, ou seja, capazes de atenuar os riscos da informação), eficazes (por exemplo, devidamente especificados, concebidos, implementados, utilizados, geridos e mantidos) e eficientes (fornecendo valor líquido à organização). O objetivo final é que a segurança da informação seja controlada como um todo, para uma mitigação adequada dos riscos da informação que a organização considera inaceitáveis e inevitáveis, de maneira razoavelmente económica e alinhada aos negócios. Esta segurança informação deve oferecer a flexibilidade necessária para a personalização das revisões necessárias com base em missões e objetivos de negócios, políticas e requisitos organizacionais, ameaças e vulnerabilidades emergentes conhecidas, considerações operacionais, dependências de sistema de informação e plataforma, e a exposição ao risco da organização (36).

2.1.5 A realidade internacional

A Lei de Portabilidade e Responsabilidade em Seguros de Saúde (*HIPAA*) dos EUA, de 1996, implementou salvaguardas para garantir que certas informações digitais em saúde estejam protegidas. A regra de segurança exige que as entidades abrangidas mantenham salvaguardas administrativas, técnicas e físicas razoáveis e apropriadas para garantir a confidencialidade, a integridade e a disponibilidade dos RSE que criam, recebem, mantêm ou transmitem (6).

A Lei de Tecnologia da Informação em Saúde para a Saúde Económica e Clínica (*HITECH*), parte da Lei dos Estados Unidos da América de Recuperação e Reinvestimento (*ARRA*) de 2009, foi incluída como atualização dos padrões *HIPAA* para fortalecer ainda mais a privacidade e a segurança das informações de saúde, além de adicionar requisitos específicos para a resposta e notificação de quebras de segurança (13).

A lei *HIPAA* e *HITECH* está a tornar-se um exemplo importante pela implementação de políticas, procedimentos e formação adequada aos funcionários de forma a garantir a segurança dos RSE (37).

O CINTESIS - Centro de Investigação em Tecnologias e Serviços de Saúde realizou um estudo de caracterização dos Hospitais Brasileiros relativamente à segurança dos SI e concluiu que existe uma grande heterogeneidade se não mesmo assimetria entre os vários hospitais relativamente à sua dimensão, à sua complexidade e à maturidade dos seus sistemas de informação. Estes investigadores constataram que ainda existe um desconhecimento de algumas medidas importantes na área da segurança informática. Apesar da legislação brasileira refletir as melhores práticas para o setor, verificou-se que apesar do esforço dos últimos anos ainda existe uma distância significativa entre a legislação e a realidade estudada. Os principais entraves referidos pelos autores são a consciencialização dos conselhos de administração para a problemática da cibersegurança e o escasso financiamento que dificulta a definição de um *roadmap* de implementação no terreno da legislação em vigor dada a dimensão geográfica e a complexidade da realidade do Brasil (38).

2.2 Vulnerabilidades

Uma vulnerabilidade, do ponto de vista do domínio da segurança da informação, pode ser definida como um defeito do sistema, um ponto de falha passível de ser explorado por alguma ameaça, permitindo o acesso não autorizado, com o objetivo de violar as políticas de segurança do mesmo. Este elemento pode ser um equipamento, uma instalação física, uma aplicação informática ou mesmo a intervenção humana. As vulnerabilidades de uma forma geral podem ser classificadas da seguinte forma:

Físicas: local (edifício, sala) onde se encontra a infraestrutura TI e SI. Deve haver cuidado na escolha dos locais onde serão instalados, respeitando os padrões exigidos para a correta proteção do espaço, de forma a prevenir acidentes naturais;

Hardware* e *Software: nestas podem incluir-se o desgaste do equipamento, a obsolescência, a má utilização, as avarias, assim como, as deficientes instalações ou configurações de *software*, falhas ao nível da sua implementação, incompatibilidades entre *hardware* e *software* que ao serem exploradas podem provocar o extravio de dados ou levar à indisponibilidade dos sistemas.

Armazenamento externo: São tipicamente pequenos e fáceis de transportar; considerados importantes vetores de infeção dos SI, danificáveis, corrompidos ou mesmo de fácil perda. (39)

Comunicação: nesta classe de vulnerabilidade podem incluir-se as perdas de comunicação, os acessos não autorizados à rede ou mesmo a máquinas. Para evitar o roubo de dados, deve-se ter o controlo de todas as máquinas que estão na rede e das suas comunicações.

Humana: incluem-se aqui as técnicas de engenharia social que se aproveitam das vulnerabilidades referentes ao factor humano, objeto de estudo neste trabalho.

2.2.1 Vulnerabilidade do Serviço Nacional de Saúde

O Serviço Nacional de Saúde atravessou entre 2011 e 2015 um período de retrocesso marcado pela crise económica em Portugal, tendo provocado um desinvestimento na saúde (40), que ainda hoje se reflete em especial nos Cuidados Primários de Saúde (CPS), onde o *hardware* apresenta mais de 15 anos e se encontra inadequado às necessidades dos profissionais e a necessidades de segurança (41).

Convém relembrar que muitos dos sistemas operativos utilizados, como é o caso do *Windows XP*, deixaram de ter atualizações e suporte (42)(43) constituindo uma vulnerabilidade que é conhecida e documentada desde 2014, e que facilita o ataque aos sistemas por *hackers* através da instalação de *malware,* como é o caso do *wannacry* (*ransomware*) e outros tipos de vulnerabilidades (6).

Em Portugal, apesar dos avanços já realizados, é necessário promover cada vez mais a prestação de cuidados de saúde em regime ambulatório, implementando uma adequada gestão da doença aguda (44) com recurso às novas tecnologias de informação e comunicação como é o caso da telemonitorização (45), torna-se imperativo o investimento em *hardware* e *software* e consequente aplicabilidade de procedimentos de cibersegurança.

Apesar destes objetivos divulgados existe uma persistente lacuna de investimento nos sistemas de informação em saúde, em especial nos centros de saúde primários, onde é notório que as redes informáticas têm mais de 15 anos e os computadores versões *Windows XP* e *Windows 7*. Estas situações provocam problemas nos sistemas de informação centrais do Ministério da Saúde e instabilidade na utilização das diferentes aplicações, remetendo para as Administrações Regionais de Saúde o *upgrade* ou

substituição dos computadores (41). Apesar de não existir uma estatística disponível para consulta, os hospitais do SNS têm uma realidade similar, constituindo assim uma das vulnerabilidades documentadas pela literatura como responsável, entre outros, pela infeção do vírus *ransomware* que decorreu em maio 2017, aliado ao factor humano (19).

2.2.2 A vertente humana da cibersegurança em Saúde

Os profissionais de saúde são formados e treinados para executar cuidados de saúde, na maioria das vezes sujeitos a elevados níveis de stress devido à sobrecarga de trabalho e de responsabilidades. No dia-a-dia trabalham em equipa, cooperam entre si dentro da hierarquia organizacional e existe uma tendência natural para confiar nos que os rodeiam, uma vez que o seu foco comum são os cuidados de saúde.

Apesar de cientes das boas práticas em cibersegurança, estas são relegadas para segundo plano fazendo com que os comportamentos e atitudes dos profissionais sejam a maior vulnerabilidade em termos de segurança.

Numa outra perspetiva, temos a engenharia social: método usado pelos *hackers* para obtenção indevida de senhas ou outro tipo de informação confidencial (18). É algo que faz parte da realidade dos utilizadores de tecnologias e que tanto pode ser usada para manipular, condicionar e reverter informação, como ser utilizada como ferramenta educativa, de segurança e critica da informação difundida, promovendo o ganho de conhecimentos (46).

2.3 Consciencialização para a Cibersegurança (CC)

Trata-se de uma abordagem que visa alertar e despertar os profissionais para a segurança dos sistemas de informação dentro das organizações. É uma forma de desenvolver a consciência coletiva para a problemática da segurança e de os motivar para a adesão às boas práticas (ciberhigiene), contribuindo para a proteção de informações valiosas e sensíveis (13).

No geral, pode-se caracterizar a CC como o conjunto de todas as estratégias que possam prevenir e mitigar os efeitos associados aos ciberataques (12) que quando aplicadas nas entidades, em particular nas da saúde, apresentam duas vertentes essenciais:

- Compreensão por parte dos profissionais da saúde do seu papel em conservar a informação segura segundo as políticas, regras e *guidelines* estabelecidas. Ou

seja, conhecer as implicações e importância do seu comportamento na segurança da informação.

- Empenho e envolvimento do profissional para as melhores práticas de segurança da informação estabelecidas pela entidade. Está diretamente ligada a uma disposição relativamente estável, avaliativa, que faz um indivíduo pensar, sentir ou comportar-se, positiva ou negativamente em relação a uma pessoa, grupo ou problema (47).

A definição do conceito de comportamento aliado às atitudes dos profissionais com conhecimentos adquiridos e desenvolvidos em segurança de informação, fundamentam o modelo de consciencialização *Knowledge– Attitude–Behaviour (KAB)* (48).

Este modelo defende que quanto maior forem os conhecimentos dos profissionais em segurança de informação dentro das entidades, melhores serão os seus comportamentos, sendo estes diretamente proporcionais a uma maior envolvência e empenho em segurança de informação (48).

Figura 2.1 - Adaptação gráfica do modelo I*nformation Security Awareness.*

Fonte: *Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, Zwaans T. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Comput Secur [Internet]. 2017;66:40–51. Available from: http://dx.doi.org/10.1016/j.cose.2017.01.004, tradução e adaptação Paulo Nunes.*

Enquanto que a complacência em segurança deve ser entendida como o cumprimento e a realização de atividades necessárias à manutenção da segurança no local de trabalho. A participação em segurança deverá ser entendida como o desenvolvimento dos comportamentos que permitem desenvolver as questões da segurança, mas que não são obrigatórios.

Assim o comportamento de segurança depende sempre dos conhecimentos que este tem sobre as regras de segurança a cumprir no desempenho das suas tarefas, as aptidões necessárias ao correto desempenho e, a sua motivação para desempenhar essas mesmas tarefas em segurança.

Os comportamentos de segurança para além dos fatores individuais (atitudes, diferenças individuais), também dependem de fatores organizacionais como o ambiente de trabalho ou a envolvente organizacional. Estes fatores vão influenciar o desempenho individual dos trabalhadores de forma direta ou indireta, mas serão facilitadores ou não do desenvolvimento dos comportamentos de segurança. As atitudes que nós percecionamos dos outros (colegas, chefias, gestão de topo) face às questões de segurança podem influenciar positiva ou negativamente os nossos comportamentos e atitudes.

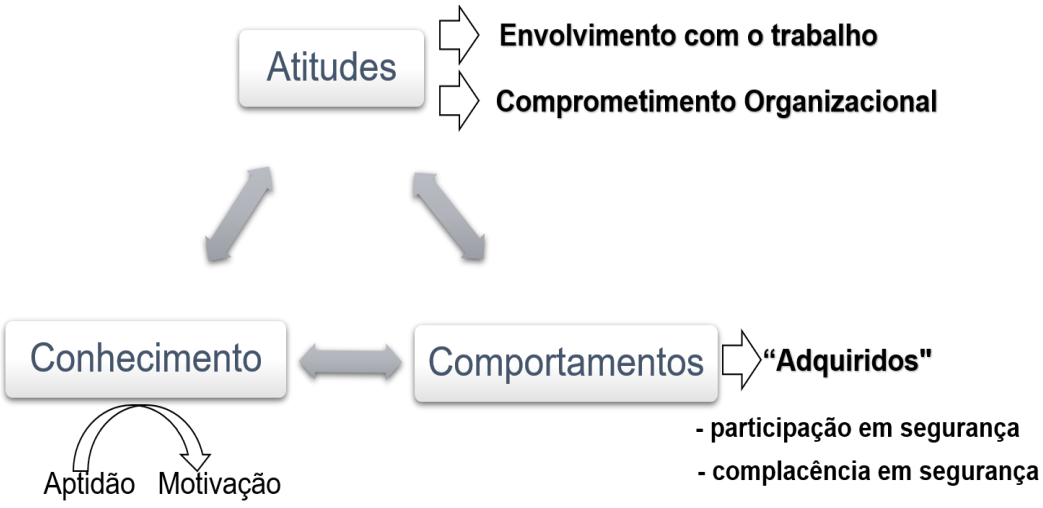


Figura 2.2 Consciencialização para a Cibersegurança resumo.

Paulo Nunes 2019

2.4 Ciberhigiene

Pode-se definir como sendo o processo de manutenção e proteção dos SI baseado na aplicação das boas práticas de segurança nas diversas vertentes das seguranças da informação com a finalidade de garantir o uso do ciberespaço sem problemas.

A ideia base é simples e consiste em incutir nos utilizadores hábitos de segurança aplicados aos sistemas de informação com o intuito da proteção pessoal. De uma forma prática pretende-se mitigar os riscos em resultado de uma perceção dos perigos (49).

Mais especificamente, consiste num processo continuo de treino dos utilizadores focado no pensamento proativo, nas boas práticas de segurança dos sistemas de informação como forma de prevenção e manutenção dos cuidados básicos de segurança. Porque um sistema nunca é totalmente seguro, devem-se realizar pequenas ações como a verificação de vírus com *software* antivírus, atualização do sistema operativo, verificação e instalação de atualizações de segurança, limpeza do disco rígido e alteração de senhas, de forma preventiva para aumentar a segurança dos SI (50)(51).

2.5 Ataques no Ciberespaço

2.5.1 Engenharia social

A engenharia social ou “Art of Deception” ou arte de enganar, termo aplicado por *Kevin D. Mitnick,* provavelmente o hacker mais famoso do mundo descrever os métodos aplicados para obtenção indevida de senhas ou outro qualquer tipo de informação confidencial. O autor ilustra como até mesmo os sistemas de informações mais bem protegidos são suscetíveis de ataques e como um burlão conseguem obter informação sensível com ataques de engenharia social.

É algo que faz parte da realidade dos utilizadores de tecnologias e que tanto pode ser usada para manipular, condicionar e reverter informação, como ferramenta educativa, de segurança e critica da informação difundida promovendo o ganho de conhecimentos.

A Engenharia Social constitui possivelmente um dos maiores riscos atuais à segurança da informação das organizações e aos seus profissionais. Os ataques são cada vez mais sofisticados, aproveitam-se da ingenuidade dos utilizadores, que na sua maioria não se apercebem que se trata de um ataque com perda de informação sensível.

Designa-se por engenharia social o processo de tentar convencer alguém de algo fictício, usando interações que podem revestir-se de várias formas: mensagens de correio eletrónico, interações através das redes sociais ou mesmo chamadas telefónicas.

Nos ataques de engenharia social são demonstradas competências sociais do atacante, com recursos a métodos da psicologia humana para explorar os sentimentos e as emoções de forma a controlar o comportamento da vítima (52).

Por norma os atacantes tentam enviam enviar solicitações de amizade aos profissionais hospitalares pelo *Facebook, Match.com, LinkedIn* e ou quaisquer outros *sites* da *Internet* onde se possam divulgam informações pessoais e onde ocorra interação social. Os profissionais devem ter conhecimentos suficientes para que nunca divulguem a sua posição GPS, ou *links* de localização, ou mesmo enviar atualizações divulgando os locais onde estarão a passar férias e a duração das mesmas (53).

2.5.2 Phishing

A palavra *Phishing*, é um neologismo criado a partir do inglês *fishing* (pesca) devido à semelhança entre as duas técnicas. Em ambos os casos, é utilizado um isco para conduzir o utilizador a fornecer informações confidenciais, como credencias para aceder a determinado serviço.

É um dos ataques mais frequentes na *internet* como forma de obtenção de informação confidencial para fins ilícitos. Das diversas formas de propagação do *phishing*, destacam-se o envio de *links* fraudulentos através de *website,* mensagens de *email* ou ainda por *SMS* (13). A maioria dos ataques por *phishing*, iniciam-se por um *email* cujo o conteúdo muito parecido com o original, iludindo facilmente os utilizadores menos experientes e com menos conhecimentos sobre o funcionamento da *internet* (12).

2.5.3 Malware

O termo *malware* refere-se a qualquer tipo de *software* malicioso que tenta infetar um computador ou um dispositivo móvel. Por norma os *hackers* usam o *malware* para vários fins, como a extração de informações pessoais ou credenciais de acesso, roubo de dinheiro ou a negação de acesso aos proprietários dos SI e dos dados.

Um ataque de *malware* normalmente divide-se em cinco categorias base, variando consoante o propósito do ataque e o ganho estimado:

Spyware e adware

Adware recolhe informações sobre os hábitos de navegação de um utilizador e envia anúncios *pop-up* em consonância com as preferências demonstradas.

O *spyware* também recolhe informações como o *Adware,* mas simultaneamente recolhe outro tipo de dados confidenciais, como senhas e números de contas.

Malware* de *botnet

Esta categoria de *malware* cria várias redes de computadores que ficam comprometidos e que podem ser controlados remotamente, por criminosos com os mais diferentes intuitos.

Cryptojacking* ou *cryptomining malware

Consiste no *malware* que envolve o sequestro de um computador ou rede de computadores para minar cripto moedas. Este *malware* procura atividades de *bitcoin* e, se encontrar, redireciona os fundos para uma carteira forjada.

Fileless malware

O *malware* sem arquivo que funciona apenas na memória do computador e não deixa qualquer arquivo para o *software* antivírus localizar. Apesar de desaparecer com *reboot* do sistema, este *malware* cria uma porta de entrada no sistema. É um problema nos SI que trabalham continuamente numa base 24x7 e onde não existem paragens frequentes dos sistemas de informação, tais como atividades financeiras e a área da saúde.

Ransomware

O *ransomware* ganhou destaque em 2016 quando uma onda deste tipo de *malware* encriptou vários computadores em todo o mundo e os manteve comprometidos até ao pagamento de um resgate (*ransom)* em *bitcoin* ou outras criptomoedas.

Um dos mais notórios foi o *ransomware wannacry / wannacryptor* que afetou grandes organizações em todo o mundo, incluindo *NHS*. Os atacantes exigiram US $ 300 em bitcoins para cada chave de desencriptação, embora eles nem sempre entregassem a chave. O *ransomware* encerrou os hospitais do *NHS* e afetou centenas de milhares de organizações e indivíduos que perderam dados valiosos. Em 2018, os ataques de *ransomware* diminuíram à medida que os atacantes voltaram a concentrar os seus esforços no *cryptojacking* ou *cryptomining malware* (54).

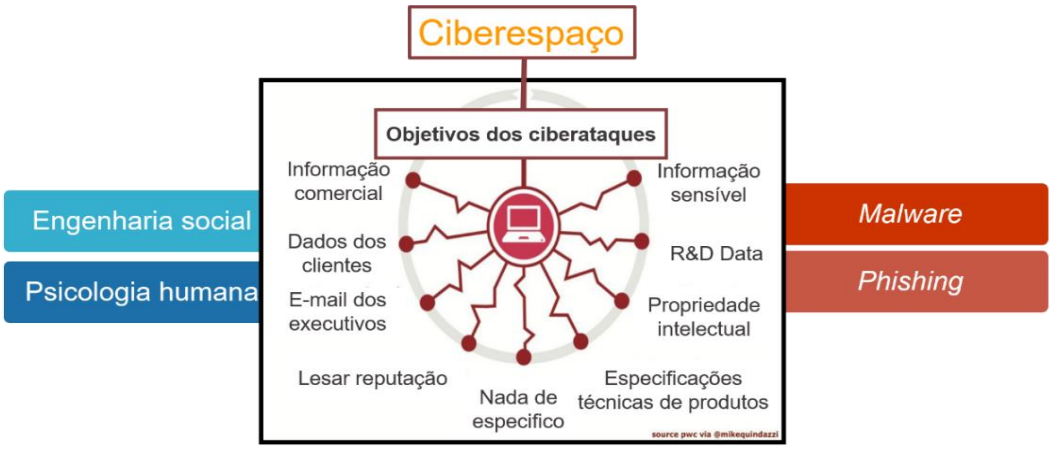


Figura 2.3 - Os objetivos dos ciberataques.

fonte: pwc via @mikequindazzi Adaptação gráfica Paulo Nunes

2.6 Sistemas de informação em Saúde

Os SI em saúde (SIS) podem ser definidos como um conjunto de aplicações interrelacionadas que recolhem, processam, armazenam, distribuem e destroem a informação que serve de apoio a todo o processo de tomada de decisão clínica e simultaneamente um auxiliar imprescindível na gestão das organizações de saúde (55).

Na área da saúde os sistemas de informação alicerçam a medicina baseada na evidência. Trata-se de uma peça fundamental para a tomada de decisão em tempo real de qualquer entidade de saúde podendo ser descrito como um sistema desenhado para a gestão de toda a informação clínica e administrativa da instituição, para a melhoria da qualidade da prestação dos cuidados de saúde e como ferramenta financeira. A implementação de SIS serve os seguintes propósitos:

- administrativos - pretende-se registar os dados demográficos dos doentes, bem como os dados do funcionamento de instituição (ex.: datas de internamentos de doentes);
- financeiros - pretende-se registar dados relativos aos custos ou receitas de serviços prestados (ex.: despesas a apresentar a subsistemas de saúde);
- stocks - pretende-se fazer a gestão de stocks de uma instituição (ex.: fármacos)
- clínicos – registo eletrónico de saúde e de doença dos utentes e dos cuidados prestados.

Os SIS geram um conjunto de dados sensíveis que é necessário compreender melhor a sua génese para desenvolver um processo de planeamento, organização, direção e controlo da informação, aos níveis estratégico, tático e operacional.

2.7 Registo de Saúde Eletrónico (RSE)

O Registo de Saúde Eletrónico (RSE) ou *Eletrónico Health Record* (EHR na nomenclatura inglesa) é um repositório de informações eletrónicas sobre o estado de saúde individual e cuidados de saúde prestados ou a desenvolver. As informações recolhidas são provenientes de diversas fontes e espaçadas ao longo do tempo de vida de uma pessoa, e servem diversos propósitos entre os quais informação clínica, educação, diversos tipos gestão, fins legais, Investigação, condições socioeconómicas entre outros que são suportadas pelo desenvolvimento tecnológico e pelo desenvolvimento da utilização das sociedades.

2.7.1 Filosofia RSE

Um RSE não se trata de uma simples evolução tecnológica do registo médico em papel, porque este evoluiu, ganhou dimensão e uniformidade, focando-se na saúde e bem-estar do utente e não apenas na condição da doença; é uma ferramenta que permite partilhar informação de forma segura, simples e acessível em tempo útil e serve também como apoio à decisão clínica.

2.7.2 O valor do RSE

A implementação do RSE mudou radicalmente a forma como as organizações de saúde executam os cuidados, como efetuam a gestão da entidade e da qualidade, bem como a forma como contabilizam os serviços prestados e consequentemente financiam o sistema (18).

A informação recolhida e expressa num RSE é volumosa, sensível e confidencial, em particular nas entidades de saúde e serviços oficiais prestadores de cuidados de saúde.

O grande valor do RSE prende-se com a dimensão da informação codificada e armazenada, não apenas quando analisados individualmente, mas também quando analisados em conjunto.

Num RSE pode-se armazenar e consultar diversa informação que vai desde um simples registo de peso, altura, tensão arterial, hábitos, medicação, alergias e história clínica, até aos dados socioeconómicos. Depreende-se facilmente que a informação contida nesta base de dados é valiosa e diversificada, de elevado valor comercial e que se torna apetecível a ciberataques (37).

2.7.3 Princípios de Segurança da Informação

A segurança do RSE define-se como o conjunto de regras fundamentais de proteção e preservação dos dados e dos ativos que o suportam nomeadamente sistemas, redes e infraestruturas. Trata-se de um conjunto de medidas de segurança físicas e lógicas dispostas de forma a garantir as regras básicas de segurança instituídas internacionalmente (4).

A forma de garantir a segurança dos dados baseia-se em dois pilares, essenciais para a disponibilização de informação em formato eletrónico, de acordo com as boas práticas internacionais de segurança. Esses pilares são:

1. Segurança Física – toda a informação é guardada de forma segura, usando normas internacionais, nomeadamente através da encriptação: *AES, RSA*. (confidencialidade, disponibilidade e integridade)

2. Segurança Lógica – a ativação dos dados garante que quem acede é quem diz que é e que posteriormente não o possam negar (autenticidade e não repúdio) (4).

Confidencialidade

Consiste em manter confidencial o RSE de forma a garantir a proteção dos dados dos utentes de acessos não autorizados, seja de forma acidental ou deliberada. A confidencialidade pode ser quebrada por razões técnicas ou organizacionais: mecanismos de controlo de acesso insuficientes, transmissão de informação não encriptada pela rede, partilha de senhas entre utilizadores, definição desadequada de privilégios dos utilizadores, falta de cuidado no manuseio do RSE, entre outros (56).

Integridade

Manter a integridade dos dados é impedir a corrupção ou manipulação indevida, quer de forma deliberada quer acidental. Esta prevenção aplica-se aos dados armazenados ou aos dados em trânsito nas redes. A alteração ou modificação não autorizada de RSE confidencial deve-se a erros no *software*, vírus, mau funcionamento do equipamento ou redes e ataques informáticos. A conservação da integridade nos sistemas de informação passa, entre outras técnicas, pela utilização de assinaturas digitais ou selos digitais (56).

Disponibilidade

Caracteriza-se por garantir o acesso autorizado à informação confidencial presente no RSE sempre que necessário, quando necessário, em particular nas situações emergentes. Os recursos e serviços podem ficar indisponíveis por avarias nos equipamentos ou no ambiente onde operam (por exemplo, quebras de energia, falhas nas aplicações, erros no manuseamento do sistema, ataques intencionais, causas naturais como incêndios ou inundações), insuficiência de recursos, etc. Para evitar quebras de disponibilidade, são necessários mecanismos de redundância, de recuperação das falhas, *backups* de proteção contra-ataques, entre outros (56).

Autenticidade e não repúdio

Na área da saúde em particular, existem situações especificas em que a informação contida no RSE é transacionada, modificada e ampliada, tornando-se importante garantir que os intervenientes são quem afirmam ser (autenticidade) e que posteriormente não possam negar a sua participação na transação da informação (não repúdio) (56).

2.7.4 A Interoperabilidade e interconexão dos RSE

A diversificação de prestadores de serviços de saúde, aos quais um indivíduo pode recorrer ao longo da sua vida, provoca uma dispersão do RSE por diferentes sistemas de informação, geralmente incompatíveis entre si (57). Atualmente, nenhuma entidade de saúde é uma ilha, o diagnóstico médico encontra-se em constante evolução tornando-se personalizado, preventivo, preditivo e participativo centrado no indivíduo.

A adoção de normas de interoperabilidade no setor da saúde tem-se tornado cada vez mais indispensável devido à existência de uma grande diversidade conceptual, de plataformas de *hardware* e *software* distintas, da necessidade e urgência de procura e comunicação de informações clínicas e administrativas em tempo real, bem como a viabilização do uso de sistemas de apoio à decisão cada vez mais sofisticados (21).

Convém relembrar que, os cidadãos têm o direito de aceder aos seus dados pessoais, incluindo os dados relativos à sua saúde, tal como previsto no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que estabelece as condições para o tratamento lícito de dados pessoais, incluindo dados relativos à

saúde. No entanto, a maioria dos cidadãos ainda não podem aceder (nem partilhar de forma segura) os seus dados de saúde através das fronteiras (58).

Assim a UE em 2017 emitiu as *guidelines* para o desenvolvimento de um *framework* comum de apoio às ambições de uma rede de saúde *online eHN (eHealth Network)* para suportar as políticas de sustentabilidade relativas à interoperabilidade transfronteiriça de saúde *online,* estabelecendo a ligação entre as políticas de saúde e a prestação de serviços pelos Estados-Membros (EM). O objetivo do documento é propor uma diretriz sobre a Interoperabilidade dos Registos Eletrónicos Profissionais para apoiar o alinhamento entre os Estados Membros no fornecimento de Serviços de Informações sobre *eHealth* transfronteiriços, *Cross-Border eHealth Information Services* (*CBeHIS*). Este documento serve como uma versão preliminar da futura diretriz sobre a unificação da interoperabilidade dos registos eletrónicos profissionais entre os estados membros (59).

A possibilidade de os cidadãos e os prestadores de cuidados de saúde acederem e partilharem em segurança aos RSE, ou seja, coleções de registos médicos longitudinais ou documentação similar de um indivíduo, em formato digital, dentro e fora das fronteiras traduz uma série de benefícios tais como a melhoria da qualidade dos cuidados prestados aos cidadãos, redução do custo dos cuidados de saúde para as famílias e apoio à modernização da saúde, e o desenvolvimento de um espaço único onde os cidadãos podem circular livremente e em segurança entre os Estados-Membros (58).

Os desenvolvimentos destas plataformas de *hardware* e *software* em saúde interligados e interoperáveis no espaço europeu permite a partilha de informação eficaz e eficiente, representam hoje uma importante tendência e uma mudança de paradigma de medicina que deverá ser acompanhada das respetivas medidas em cibersegurança.

Esta necessidade de standardização de Interoperabilidade e da interconexão de sistemas é um passo importante para a integração das tecnologias digitais na saúde e nas abordagens de cuidados prestados, permitindo o alinhamento das tecnologias e das Semânticas utilizadas na UE e das suas políticas entre estados membros.

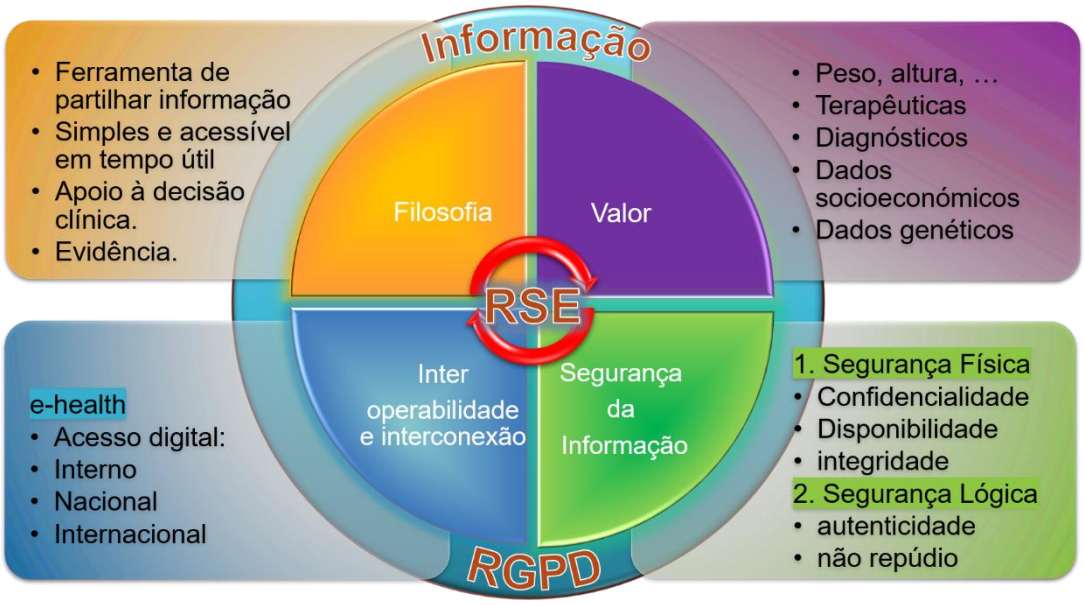


Figura 2.4 Registos de saúde Eletrónicos

Paulo Nunes 2019

2.8 Novos paradigmas de saúde

A realidade que vivemos num mundo em constante evolução, reflete-se no desenvolvimento de novos paradigmas tal como a introdução de tecnologias *blockchain*, desenvolvida por *Satoshi Nakamoto*, que se define como uma cadeia de informação encriptada, acessível mundialmente por uma chave que cria uma cadeia de conteúdo apenas por acréscimo, imutável e com carimbo de data/hora (60). Esta tecnologia é formada por blocos de dados que contêm registos de transações e os respetivos proprietários, de forma a garantir e conservar a integridade, confidencialidade, autenticidade e disponibilidade da informação que guardam (57).

A aplicação desta tecnologia à saúde está a revolucionar a forma como a informação em saúde é criada, recebida, armazenada, destruída proporcionando a aplicabilidade de outras tecnologias como o *cloud* e *big data*, que fomentaram o aparecimento de vários aplicativos e serviços de saúde inteligentes (61), e os desenvolvimento de novos modelos em saúde.

Um dos maiores trunfos da nossa sociedade é a crescente determinação dos consumidores de cuidados de saúde em gerir melhor a sua própria saúde utilizando a *Internet* para recolher informações e a sua capacidade de auto-organização utilizando ferramentas de redes sociais (3).

Na última década temos assistido à gradual transição dos dados para o armazenamento na *cloud* em código aberto e sob uma política de transparência que permite a criação de um modelo cooperativo de dados em saúde centrada no indivíduo. Este modelo acompanha o desenvolvimento de um novo paradigma médico denominado de medicina P4, que significa medicina personalizada, preventiva, preditiva e participativa centrada no doente e recorrendo aos cuidados de saúde modernos fundamentados na tecnologias e na genética (3).

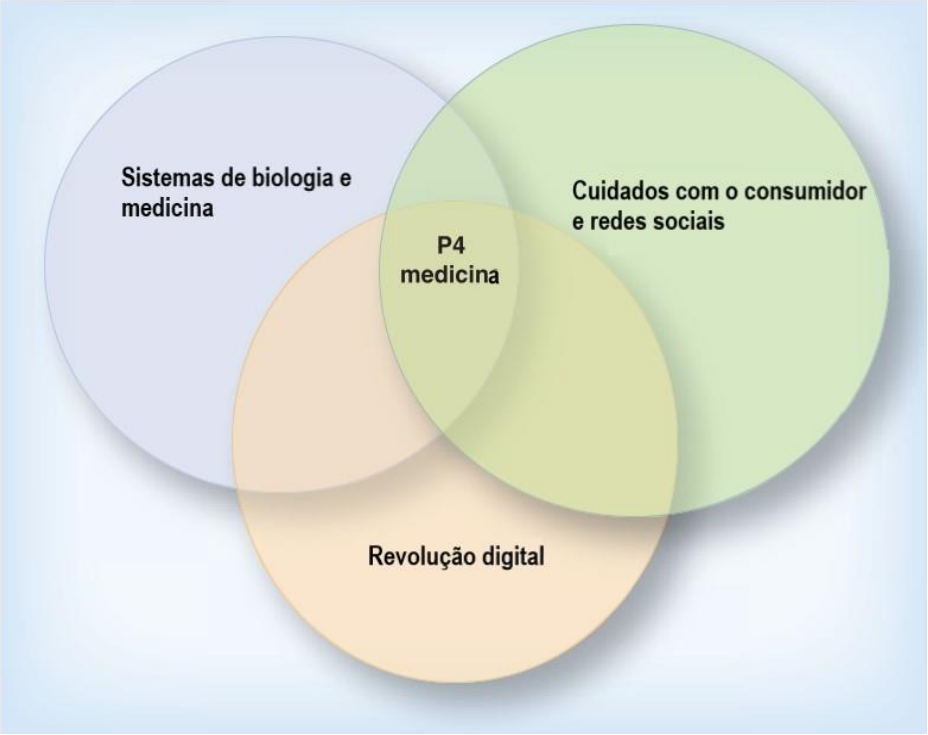


Figura 2.5 – Os pilares da medicina P4.

Fonte:Van Roessel I, Reumann M, Brand A. Potentials and Challenges of the Health Data Cooperative Model. Public Health Genomics. 2018;20(6):321–31

Na medicina P4, o primeiro "P", de prevenção, ações realizadas para evitar a ocorrência da doença e à redução da exposição aos factores de risco. O segundo, de predição, tem o objetivo de identificar doenças que podem aparecer, com base em mapeamento populacional e investigação genética. O terceiro, de participação, faz com que se crie uma relação mais humana entre o médico, o paciente e a sociedade como um todo. E o quarto, de personalização, trabalha com propostas individualizadas, conforme as necessidades de cada paciente (3)(62)(2).

As organizações de saúde deixaram de ser os únicos locais a efetuar os RSE. Hoje quer no hospital quer em casa ou até mesmo nos transportes, já é possível em tempo real registar, armazenar e monitorizar dados de saúde. O desenvolvimento de pequenos equipamentos pessoais (*wearable devices*) com conectividade à *Internet* (*IoT*) e com a capacidade de rastrear a atividade humana estão a mudar os cuidados de saúde. A maioria destes equipamentos são capazes de enviar estatísticas de saúde para smartphones, *smartwatches* ou *smartbandas* em tempo real, no entanto, apenas fornecem os dados para análise, embora não estejam integrados na prática clínica (63).

Facilmente se identifica o potencial da aplicabilidade deste modelo passando desde o benefício da partilha de conhecimento, capacidade dos cidadãos controlarem os seus dados de saúde e quem tem acesso aos mesmos, assim como, contribuir para a redução nas despesas de saúde (2).

Apesar das vantagens destes novos e aliciantes modelos em saúde, a realidade é que lança novos desafios à cibersegurança em saúde, especificamente relacionados com os acessos não autorizados à informação pessoal e sensível, incluindo os dados sensíveis que circulam na *Internet*. Neste sentido é necessário a formação e a sensibilização dos cidadãos para a utilização segura e ciente das Tecnologias de Informação e de Comunicação (TIC), reduzindo a sua exposição aos riscos do ciberespaço. Outro desafio é a aplicabilidade do regime de proteção de dados, incluindo a privacidade e a segurança de dados, restrição dos cidadãos, divulgação de resultados clínicos, a *big data* com interesses manipuladores e comerciais (2), demonstrando-se assim a importância da cibersegurança e da sua aplicabilidade global aos utilizadores.

A pertinência desta temática está bem presente no desenvolvimento da primeira edição do curso *online* de cibersegurança que permitirá ao cidadão adquirir um conjunto de competências relacionadas com os comportamentos seguros no ciberespaço e, desta forma, contribuir para a consciencialização em cibersegurança e para navegação livre e segura na *Internet* (64).

"NAU – Ensino e Formação à Distância para Grandes Audiências" é a iniciativa nacional para construção e operação de uma infraestrutura técnica e operacional de suporte à publicação e dinamização de conteúdos *MOOC* (*Massive open online course*) em ambientes virtuais de aprendizagem com ferramentas *web* 2.0 e ou uso de redes sociais. O Projeto NAU, transversal a diversos ministérios, desenvolve ações de formação para um maior número de funcionários e cidadãos, com maior qualidade, com maior frequência e menores custos (65).

3 Metodologia

O estudo desenvolvido consiste numa primeira fase na tradução para português da versão inglesa de duas escalas previamente validadas e publicadas internacionalmente por *L. Hadlington* (9).

Trata-se de duas escalas do tipo *Likert* avaliatórias dos comportamentos arriscados em cibersegurança - *Risky Cyber security Behaviours* (*RScB*) e das atitudes em relação à cibersegurança em ambiente empresarial - *Attitudes towards Cybersecurity in Business* (*ATC-IB*) que foram adaptadas para português e aplicadas aos profissionais de saúde em ambiente hospitalar português para conhecer as diferenças individuais dos profissionais nas organizações ou entidades de saúde em cibersegurança.

3.1 Enquadramento teórico das escalas

Para estabelecer uma relação entre as características de personalidade dos utilizadores dos SI e os respetivos comportamentos, desenvolveu-se uma investigação no campo da ciberpsicologia aplicando-se o modelo '*Big Five'* ou modelo dos cinco factores. Este modelo baseia-se numa escala desenvolvida em 1961 por *Ernest Tupes e Raymond Christal* e aperfeiçoada ao longo dos anos por vários autores. Carateriza-se por identificar os traços e estrutura da personalidade humana através de cinco factores, designadamente: abertura para novas experiências (*openness to experience*); Consciencialização (*conscientiousness*); Extroversão (*extraversion*); Neuroticismo ou Instabilidade Emocional (*neuroticism*) e por fim a Agradabilidade (*agreeableness*) (66).

Para estabelecer uma correlação entre atitudes e personalidades, *Chris G. Sibley* e *John* acrescentaram ao modelo duplo que incorpora a ideologia e o preconceito ao modelo da personalidade de Cinco Factores, formulando uma relação direta na qual constataram que as pessoas com baixo nível de abertura para novas experiências e alto nível de consciência expressavam motivações superiores de coesão em segurança (67).

No contexto da Segurança da Informação entende-se que as atitudes são a vertente psicológica de um comportamento, são as perceções, expectativas e conhecimentos, que juntos podem influenciar a avaliação de algo ou de alguém. Globalmente a avaliação pode conduzir a um comportamento, pensamento ou a sentimentos. Pelos pensamentos e sentimentos, podemos concretizar comportamentos, e pelos

comportamentos podemos deduzir atitudes, estabelecendo-se uma relação entre a impulsividade e a segurança da informação (9)(68)(69).

Com a massificação dos SI a todos a áreas de atividade, surgiu um novo paradigma sobre a segurança da informação e a sua partilha. Rapidamente se compreendeu que os utilizadores são o elo mais fraco da cadeia da segurança da informação, motivando o desenvolvimento de ferramentas de avaliação e quantificação dessa vulnerabilidade. Nesta quantificação os principais erros humanos foram atribuídos às quebras de segurança e à perda de informação. Hoje em dia, e numa perspetiva holística, considera-se as pessoas/utilizadores como a "primeira linha de defesa" das diferentes ameaças de SI (70).

O questionário *Human Aspects of Information Security Questionnaire (HAIS-Q)* desenvolvido por *Parsons et al (2013)* aplicou uma escala composta por 63 itens, dividido em três subáreas que mede separadamente conhecimentos, atitudes e comportamentos (71). O objetivo deste questionário era compreender os níveis de consciencialização em segurança da informação (48).

A ausência de consenso na comunidade científica relativamente a uma ferramenta standard de quantificação e comparação dos traços da personalidade com certos comportamentos de segurança dos utilizadores motivou Serge Egelman e Eyal Peer (2015) a desenvolverem novas escalas métricas para a avaliação dos comportamentos de segurança dos sistemas de informação dos utilizadores: a *Security Behavior Intendions Scale* (*SeBIS*), trata-se de uma escala que traduz a adesão dos utilizadores às boas praticas de segurança dos sistemas de informação (69). O *SeBIS* compreende 16 itens projetados para avaliar a adesão aos conselhos de segurança dos sistemas de informação. Esta escala inclui quatro subescalas dirigidas às atitudes em relação aos domínios da elaboração e aplicabilidade de senhas, proteção de dispositivos digitais, envolvimento e reconhecimento proativo e por fim a atualização de *software*(9).

No desenvolvimento de uma métrica efetiva cujo objetivo é relacionar comportamentos de segurança e diferentes níveis de consciencialização, *Gizem Ögütçü et al* em 2015, desenvolveram quatro escalas: Escala de Comportamento de Risco (RBS), Escala de Comportamento Conservador (CBS), Escala de Exposição à Ofensa (EOS) e a Escala de Perceção de Risco (RPS) (71).

As violações de segurança comuns nas organizações são atribuídas a erros humanos. Existe a necessidade de aumentar a consciencialização da segurança da informação dentro das organizações, dos seus funcionários e das suas capacidades para se

envolverem em comportamentos inseguros em cibersegurança. Factores como o género e a idade podem afetar os diferentes comportamentos em cibersegurança (9).

A pesquisa dedicada à exploração e categorização das apelidadas “ameaças internas” provenientes de ataques maliciosos de funcionários insatisfeitos ou com motivações financeiras, tem registado nos últimos anos um crescente aumento. Esta vertente maliciosa foi acompanhada de medidas e de mecanismos tecnológicos específicos de deteção e apreensão, que mitigaram esse risco.

Os factores humanos relacionados com aspetos de gestão deficiente como a falta de atenção aos detalhes e ignorância, os quais estão ligados à ascensão do “*insider*” acidental ou não intencional (oportunista) revelam uma ausência de estudos ou de medidas para a sua mitigação dentro das organizações ou entidades (72).

Esta é a base do estudo desenvolvido por *Lee Hadlington* (2017), inicialmente com a caracterização e exploração dos factores humanos fundamentais que podem contribuir para que um indivíduo se torne uma ameaça não intencional, desenvolvendo um conjunto de quadros-chave desenhados para a mitigação de tais ameaças. Posteriormente desenvolveu o estudo exploratório da relação entre comportamentos arriscados em cibersegurança, atitudes em relação à cibersegurança num ambiente empresarial, dependência relativa à *Internet* e impulsividade. No estudo *Lee Hadlington* apresenta as escalas *Abbreviated impulsiveness scale (ABIS), Online cognition scale (OCS), Risky cybersecurity behaviours scale (RScB) e Attitudes towards cybersecurity and cybercrime in business (ATC-IB)* (9).

A pesquisa realizada demonstra que existe uma discrepância entre os aspetos da personalidade, o uso problemático da *Internet* e as atitudes dos funcionários, como os potenciais comportamentos e envolvimento nas políticas de segurança da informação das empresas ou entidades.

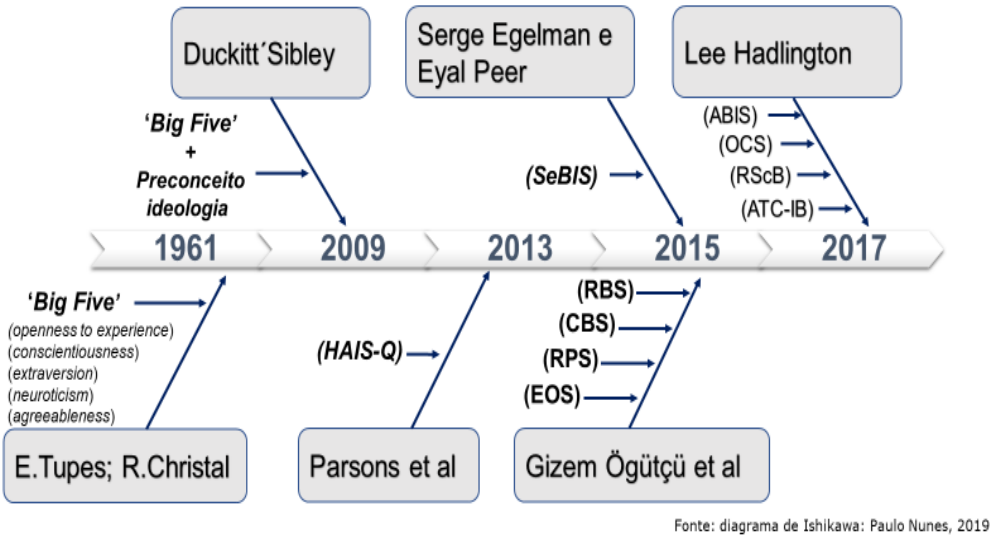


Figura 3.1 Diagrama de Ishikawa do desenvolvimento das escalas

Paulo Lopes Nunes, 2019

No desenvolvimento da temática *Aivazpour* (66) replicaram o trabalho de *Hadlington*(9), concluindo que a sua pesquisa juntamente com a pesquisa de Egelman (69), fornece um bom ponto de partida para o estudo da impulsividade em comportamentos de cibersegurança arriscados. A replicação apesar de mais centrada na impulsividade, reforça os argumentos para a existência de ligação entre a impulsividade e os comportamentos arriscados, mas salienta a necessidade para estudos mais rigorosos, nomeadamente, quais os comportamentos de segurança que são influenciados pelas dimensões de impulsividade (66).

A necessidade de desenvolvimento de escalas *Risky cybersecurity behaviours scale (RScB) e Attitudes towards cybersecurity and cybercrime in business (ATC-IB),* mencionadas nas conclusões de *Aivazpour,* impulsionaram *Hadlington* para uma melhoria, iniciando um estudo com o objetivo de explorar se o tamanho da empresa, idade ou atitudes influencia a relação dos funcionários com os comportamentos arriscados em cibersegurança e com a consciencialização geral sobre crimes cibernéticos.

3.2 Tipo de estudo

Trata-se de um estudo observacional, quantitativo, transversal e descritivo das atitudes e comportamentos em cibersegurança numa entidade de saúde comparando a métrica obtida pelas duas escalas com os factores sociodemográficos e com o grupo profissional. Este estudo procura conhecer a consciencialização em cibersegurança nas entidades de saúde.

3.3 Critérios de inclusão e de exclusão

O estudo está desenhado para a participação sob a forma de questionário de todos os profissionais de saúde com idades compreendidas entre os 18 e os 69 anos da entidade hospitalar, excluindo-se os participantes que não completem o questionário.

3.4 Ferramentas utilizadas

3.4.1 Escala de comportamentos arriscados em cibersegurança (RScB)

Escala parcialmente baseada na escala *SeBIS* desenvolvida por *Egelman et all*, a qual foi criada com a contribuição de investigadores forenses digitais e com autoridades em direito (69).

A escala apresentada avalia comportamentos que podem traduzir práticas de cibersegurança pobres, e que se refletem numa vulnerabilidade humana para as empresas e entidades de saúde especificamente.

A escala *RScB* é do tipo Likert com uma pontuação que varia dos 0 aos 120 pontos, sendo que os valores mais elevados são indicadores de comportamentos mais arriscados, geralmente associados a baixos níveis de consciencialização em cibersegurança (9). Esta escala (Apêndice 10.10) é composta por vinte itens Likert de sete níveis, pontuados de 0 a 6 pontos (0 = Nunca 6 = Diariamente), onde se pede aos participantes que classifiquem os seus comportamentos em cibersegurança retrospetivamente nos últimos seis meses. Esta escala apresenta itens com pontuação inversa nas perguntas 11 e 18.

3.4.2 Atitudes em relação à cibersegurança (ATC-IB)

A escala para conhecer as atitudes em relação à cibersegurança em ambiente empresarial foi publicada em 2017 por L. Haldlington e foi desenvolvida no sentido de explorar a perceção dos profissionais em face às ameaças do cibercrime e da consciencialização das políticas de cibersegurança dentro da entidade.

A *ATC-IB* é uma escala do tipo Likert que vária na globalidade entre os 25 e os 100 pontos, sendo que pontuações mais elevadas são sinónimo de um envolvimento positivo na temática da cibersegurança e simultaneamente uma forte consciencialização em segurança e pontuação mais baixa indica um envolvimento mais fraco e uma consciência limitada em cibersegurança.

A *ATC-IB* é formada por vinte e cinco itens Likert (Apêndice 10.10) de quatro níveis de respostas pontuadas de 1 a 4 pontos (1 = Concordo Totalmente; 2 = Concordo; 3= Discordo e 4 = Discordo Totalmente), esta escala contém itens com pontuação inversa nomeadamente os itens 2,14,15, 19, 20 e 21.

3.4.3 Recursos digitais

Disponibilizou-se os questionários na plataforma "*Online Pesquisa*" (*Zurich-based company enuvo GmbH*), uma plataforma gratuita para estudantes que permite a divulgação dos questionários e posterior participação "*online*". Para evitar a participação múltipla do mesmo participante, bloqueou-se o ID de sessão de navegação dos participantes por definição de um cookie próprio da plataforma digital.

Apesar deste procedimento limitar a adesão à participação pareceu ser a forma mais simples de garantir a participação individualizada nos questionários. Para a análise estatística dos dados, recorreu-se aos programas *IBM SPSS* (*Statistical Package for the Social Sciences,* versão 22) e ao programa *Microsoft Office Excel* para *Office 365*.

3.4.4 Métodos estatísticos

A análise dos dados consistiu em: estatística descritiva e exploratória; coeficiente de correlação *Spearman*; comparação de grupos independentes, de modo a determinar se as diferenças entre eles são estatisticamente significativas (*Anova, Mann-Whitney e Kurskal-Wallis)*.

Para verificação dos pressupostos de normalidade aplicaram-se os testes de *Shapiro-Wilk*. Para a análise da consistência interna das escalas calculou-se o alfa de Cronbach. Qualquer referência a questões de consistência interna (fiabilidade) de uma determinada medida, constituída por vários itens do tipo Likert onde se deseja medir o nível de concordância ou não concordância com uma determinada afirmação, suscita referência imediata ao índice alfa de Cronbach para determinar a sua fiabilidade(73). Na avaliação da consistência interna de um questionário parte-se do princípio de que se o questionário avalia uma determinada característica, todas as questões do questionário devem abordar aspetos diferentes desta dimensão, ou seja, todos as questões devem correlacionar-se moderadamente umas com as outras e cada uma deve correlacionar-se com o total. A coerência interna representa a média das correlações entre todas as questões do questionário (74). Considerou-se o nível de significância de 5%.

3.5 Procedimentos Éticos

Entende-se por investigação toda a iniciativa que visa gerar conhecimento original através da aplicação de metodologias científicas, sabendo que, todos os passos que são realizados estão indiscutivelmente ligados às questões fundamentais da ética, uma vez que o objeto de estudo e o destinatário do conhecimento é o homem.

O presente estudo, teve em consideração todos os princípios éticos fundamentais consagrados pelo *The European Code of Conduct for Research Integrity*, que configuram uma investigação responsável, segundo a recomendação do Conselho Nacional de Éticas para a Ciência da Vida(75).

3.5.1 Confidencialidade e anonimato

O autor deste estudo respeita e assegura o cumprimento das regras decorrentes da entrada em vigor do Regulamento Geral de Proteção de Dados (RGPD) da UE. Os dados recolhidos são anónimos, confidenciais, tratados informaticamente e armazenados em bases de dados específicas para o efeito.

Em conformidade com a declaração de Helsínquia *(World Medical Association – WMA, 2002)* todos os participantes foram informados dos objetivos do estudo, autor, propósito e os dados recolhidos. A participação no estudo foi voluntária e sujeita a aceitação dos propostos estabelecidos no consentimento informado (Apêndice 10.1).

Os dados recolhidos são anónimos, confidenciais, tratados por SI e armazenados em bases de dados específicas para o efeito.

A plataforma digital designada para o estudo não permite armazenar informação que possa associar as respostas a quem participou, conservando desta forma o anonimato e a confidencialidade dos dados obtidos.

3.5.2 Obtenção da permissão do autor primário

Requereu-se autorização ao autor das escalas *RScB* e *ATC-IB*, o Professor Doutor *Lee Hadlington*, da Universidade de *Montfort, Leicester*, através de correio eletrónico, para realizar a tradução e aplicabilidade para a língua portuguesa dos mesmos, a qual foi gentilmente concedida (Apêndice 10.2).

3.5.3 Comissões de Ética.

Procedeu-se às respetivas autorizações das organizações envolvidas, para aplicação dos questionários, nomeadamente Centro Hospitalar Barreiro Montijo (Apêndice 10.3). e do grupo ClaraSaúde (Apêndice 10.4). No cumprimento do protocolo de investigação, obteve-se parecer positivo das respetivas comissões de ética das entidades ClaraSaúde, Centro Hospitalar Barreiro Montijo (CHBM) e da Escola Superior de Tecnologias da Saúde de Lisboa.

3.6 Processo de tradução e validação

O processo de tradução e validação dos questionários originais (apêndice 10.5) teve como *guidelines* a metodologia sugerida por *D.Beaton* (76)(77) a qual é composta por cinco fases: tradução, síntese, retradução, painel de peritos e pré-teste.

1ª fase: tradução dos dois questionários de inglês para Português. Esta tradução foi realizada por duas pessoas independentes, um tradutor oficial (Apêndice 10.6 e 10.7) e uma Técnica Superior Coordenadora (Apêndice 10.8), obtendo-se duas traduções independentes.

2ª fase: síntese das duas versões traduzidas, nesta fase procedeu-se à comparação dos dois questionários traduzidos para determinar eventuais discrepâncias de tradução.

3ª fase: retradução das duas versões dos questionários de português para inglês, este processo teve como objetivo assegurar que as traduções realizadas refletem os mesmos itens originalmente propostos (Apêndice 10.9).

4ª fase: As duas versões em português foram apresentadas a um painel de peritos constituído por três professores do IPLeiria e uma professora da ESTeSL, que deliberaram por consenso as equivalências semânticas, idiomáticas, experiencial e conceptuais dos itens da versão final adaptada das terminologias para a língua portuguesa dos questionários *RScB* e *ATC-IB* (Apêndice 10.10).

5ª fase: A versão final do questionário foi pré-testada numa entidade de saúde privada (Labocentro), em plataforma digital, corrigindo-se algumas dificuldades de aplicação e preenchimento. Neste processo de pré teste responderam quarenta e cinco profissionais permitindo identificar os seguintes pontos de melhoria: a possibilidade de acessos múltiplos à plataforma e a dificuldade de aplicação da escala de Likert de 7 pontos à janela temporal inquirida (Apêndice 10.11).

3.7 Objetivos

Os objetivos do presente estudo traduzem-se nas seguintes hipóteses de investigação:

H1 – *Verificar se existem diferenças significativas dos valores médios da RScB entre as faixas etárias, classes profissionais e género;*

H2 - *Verificar se existem diferenças significativas entre os valores médios da escala ATC-IB entre as faixas etárias, classes profissionais e género;*

H3 - *Verificar se existe correlação entre os valores da escala RScB e da escala ATC-IB considerando as diferentes idades;*

H4 – *Determinar se existe diferenças por itens da escala RScB e da escala ATC-IB considerando as diferentes as faixas etárias, classes profissionais e género;*

4 Resultados

4.1 Análise da Consistência Interna

Calculou-se o alfa de Cronbach para os 20 itens que compõem o questionário *RScB*, onde se obteve um valor de 0,745 e para os 25 itens do questionário *ATC-IB* com um valor de 0,723. No estudo referência o Alfa de Cronbach foi de 0,823 para a escala *RScB* e de 0,744 e de 0,764 para a escala *ATC-IB*

Segundo vários autores, e de um modo geral, um instrumento ou teste é classificado como tendo fiabilidade apropriada para o desenvolvimento do estudo proposto, quando o α é pelo menos 0.70. Contudo, em alguns cenários de investigação das ciências sociais, um α de 0.60 é considerado aceitável desde que os resultados obtidos com esse instrumento sejam interpretados com precaução e tenham em conta o contexto de computação do índice numa meta-análise da utilização do α de Cronbach na literatura das ciências sociais e humanas, observou um α médio de 0.70 (na medição de valores) a 0.82 (na medição da satisfação com o trabalho) (78).

4.2 Caracterização da amostra

Os questionários foram disponibilizados à população alvo numa plataforma digital nos SI da entidade de saúde. O processo de recolha de dados foi inicialmente preconizado para o mês de dezembro de 2018, estendendo-se até 15 de janeiro 2019.

De uma população de 1726 profissionais, segundo os dados expressos no relatório de contas CHBM de 2018, obtiveram-se no total 65 participações o que traduz uma taxa de participação de 3,8%. Após a aplicação dos critérios de inclusão e exclusão obteve-se uma amostra constituída por 56 respostas.

A idade média dos participantes é de 44,25 anos com um desvio padrão de 9,249. A mediana tem um valor de 43 anos e a moda apresenta um valor de 40 anos. Relativamente à distribuição das frequências verifica-se que apresentam uma assimetria positiva (Coeficiente de assimetria 0,034). Na avaliação dos extremos, o participante mais novo tem 27 anos e o mais sénior tem 61 anos. Procedeu-se a uma estratificação da variável idade de acordo com as seguintes faixas etárias: ≤37; [38;43]; [44;53] e ≥53, que apresenta a seguinte distribuição: $n_{\leq 37}$=16 ou 28,6% dos participantes; $n_{[38;43]}$=14 ou 25% dos participantes; $n_{[44;53]}$=14 ou 25% dos participantes e por fim $n_{\geq 53}$=12 ou 21,4% dos inquiridos.

Relativamente ao género observou-se que 40 participantes são indivíduos do género feminino (71%) e 16 participantes são indivíduos do género masculino (29%).

Através da distribuição da amostra por idade e género na pirâmide etária (figura 5.1) pode-se verificar o predomínio de participantes do género feminino com uma distribuição caracterizada por dois picos de participantes entre a idade dos 40 anos e a idade dos 56 anos. A variável idade não é normalmente distribuída SW(56)=0,954, p=0,32 sendo a idade, por género seguem um distribuição normal para género masculino SW(16)=0,977, p=0,939 e não segue uma distribuição normal para o género feminino SW(40)=0,934, p=0,022.

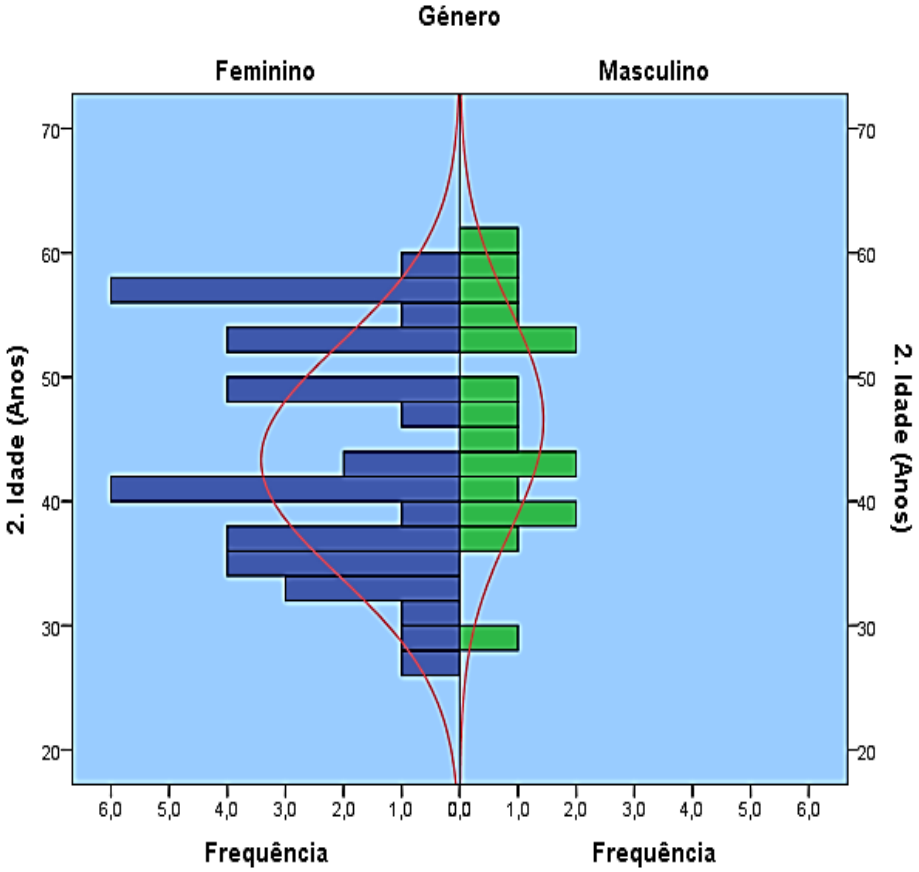


Figura 4.1 - Pirâmide idade por género

Trata-se de uma amostra heterogénea a nível dos grupos profissionais sendo composta por: Assistentes Operacionais 8,9% (n=5); Assistente Técnico/Técnico de nível intermédio/Pessoal Administrativo 3,6% (n=2); Enfermeiros 33,9% (n=19); Médicos 17,9% (n=10); Técnico Superior 3,6% (n=2); Técnico Superior de Diagnóstico e Terapêutica 32,1% (n=18).

4.3 Caracterização descritiva da escala *RScB* e *ATC-IB*

A escala *RScB* composta por 20 itens assume valores entre os 0-120 pontos, sendo que no estudo desenvolvido observou-se valores entre 0 e 64 com a média obtida pelos 56 participantes de 31,59 pontos com um desvio padrão de 14,211 pontos, mediana 30 e moda 24. Valores mais elevados desta escala são indicativos de comportamentos mais arriscados em cibersegurança.

A escala *ATC-IB*, composta por 25 itens pode assumir valores entre os 25-100 pontos, onde neste estudo observaram-se valores que variam entre um mínimo de 48 e o máximo de 82 pontos. A média obtida da escala pelos 56 participante foi de 66,41 com um desvio padrão de 6,263, mediana 67 e moda 65. A pontuação mais baixa indicam um envolvimento mais pobre e uma atitude limitada em cibersegurança num ambiente empresarial.

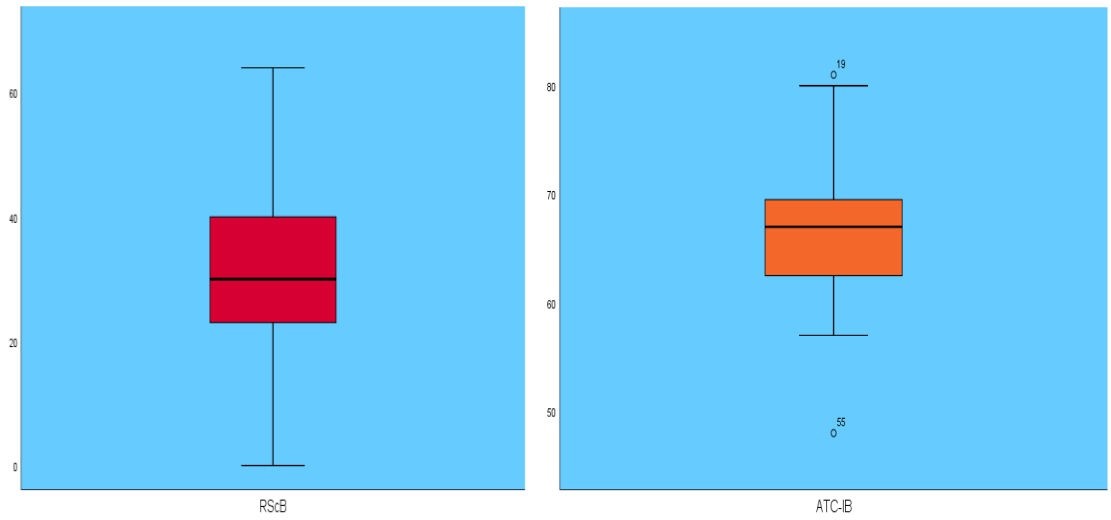


Figura 4.2 – Diagrama em caixa das escalas RScB e ATC-IB.

Para verificação dos pressupostos de normalidade para os testes paramétricos que se apresentam nas próximas secções, aplicou-se o teste de *Shapiro-Wilk (*SW) para as escalas *RScB* e *ATC-IB* para cada categoria das variáveis: faixa etária, grupos profissionais e género. Assume-se que a variável *RScB* que se encontra normalmente distribuída para as faixas etárias compreendidas entre (<=37(SW(n=16)=0,911, *p*=0,122);([38;43] SW(n=14)=0,935,*p*=0,353);([44;53]SW(n=14)=0,938,*p*=0,397);(>=53 SW(n=12)=0,889, *p*=0,115), assim como para todos os grupos profissionais, (Assistente Operacional SW (n=5) =0,933, *p*=0,614; Enfermeiro SW(n=19)=0,991, *p*=0,999; Médico

SW(n=10)=0,929, *p*=0,434;TSDT SW(n=18) =0,905, *p*=0,070). Pode-se também assumir que os valores da *RScB* apresentam uma distribuição normal para o género feminino e masculino (SW(n=40)=0,975,*p*=0,523;SW(n=16)=0,975,*p*=0,911).

A variável *ATC-IB* tem distribuição normal em todas as faixas etárias (<=37 (n=16=0,937, *p*=0,308); ([38;43] SW(n=14)=0,932, *p*=0,325); ([44;53] SW (14) =0,858, *p*=0,029); [>=53] SW(n=12) =0,959, *p*=0,766. Relativamente à normalidade da escala nas diferentes os grupos profissionais (Assistente Operacional SW(n=5)=0.981, *p*=0.942; (Enfermeiro SW(n=19)=0.945, *p*=0.323); (Médico SW(n=10)=0.945, *p*=0.615); (TSDT SW(n=18)= 0.937, *p*=0.258). do género. Também se verifica a normalidade para todas observando-se no género feminino (SW (n=40) =969, *p*=0,325) e no masculino (SW (n=16) =964, *p*=0,739).

4.4 Comparação dos valores *RScB* entre os faixas etárias, classes profissionais e género.

Para identificar diferenças significativas dos valores médios da escala *RScB* entre as diferentes faixas etárias, procedeu-se a uma ANOVA a um factor, onde se pode concluir que não existem diferenças estatísticas significativas entre os valores médios da escala *RScB* nas diferentes faixas etárias (F=1,189, g.I.=52, *p*=0,323).

Comparando os valores médios da escala *RScB* nas diferentes classes profissionais, existiu a necessidade de remover classes profissionais por insuficiente número de participantes para efeitos estatísticos, ficando a amostra com 52 participantes distribuída pelos seguintes grupos profissionais Assistente Operacional; Enfermeiro; Médico e TSDT. Através da ANOVA a um factor, também se concluiu que não existem diferenças estatísticas significativas (F=0,675, g.I.=51, *p*=0,571).

Para comparar os valores médios da escala *RScB* entre o género feminino e o masculino, aplicou-se o teste *Mann-Whitney* para duas amostras independentes, uma vez que não se verifica os pressupostos de normalidade da variável idade. Concluiu-se que não existem diferenças estatisticamente significativas entre os valores da mediana da escala *RScB* e os géneros feminino e masculino (U=285,5, *p*=0,531).

4.5 Comparação dos valores *ATC-IB* entre os faixas etárias, grupos profissionais e género

Para identificar diferenças significativas dos valores médios da escala *ATC-IB* entre as diferentes faixas etárias, procedeu-se a uma ANOVA a um factor, onde se pode concluir que não existem diferenças estatísticas significativas entre os valores médios da escala *ATC-IB* nas diferentes faixas etárias (F=0,418, g.I.=52, *p*=0,741).

Comparando os valores médios da escala *ATC-IB* nas diferentes classes profissionais através da ANOVA a um factor, existindo a necessidade de remover classes profissionais por insuficiente número de participantes por motivos estatísticos, obtendo-se uma amostra com 52 participantes distribuída pelos seguintes grupos profissionais Assistente Operacional; Enfermeiro; Médico e TSDT. também se concluiu que não existem diferenças estatísticas significativas (F=1,071, g.I.=51, *p*=0,370).

Para comparar os valores mediana da escala *ATC-IB* entre o género feminino e o masculino, aplicou-se o teste *Mann-Whitney* para duas amostras independentes, uma vez que não se verifica os pressupostos de normalidade da variável idade. Concluiu-se que não existem diferenças estatisticamente significativas entre os valores médios da escala *ATC-IB* e os géneros feminino e masculino (U=310,0, *p*=0,856).

4.6 Correlação entre *RScB* e *ATC-IB*

Determinou-se o coeficiente de correlação de *Spearman* para avaliar se a escalas *RScB* está relacionada com a escala *ATC-IB* e com a idade.

Verificou-se que existe uma correlação estatisticamente significativa entre *RScB* e a *ATC-IB* sendo esta negativa e moderada (rs(n=56)=-0,414, *p*=0,002). Relativamente, à idade verificou-se que não existe uma correlação com a *RScB* (rs(n=56)=-0,062, *p*=0,652) ou com a *ATC-IB* (rs(n=56)=0,126, *p*=0,354).

4.7 *RScB*/*ATC-IB* discriminado por item.

Na globalidade não se verificaram diferenças estatísticas significativas entre os 56 participantes, em função dos valores totais das escalas. Procedeu-se à exploração das diferenças estatísticas por item da escala de comportamentos e da escala de atitudes, na determinação de eventuais diferenças. Para o efeito, recorreu-se ao Teste de

Kruskal-Wallis para amostras Independentes para cada item das respetivas escalas por faixa etária, grupo profissional e género.

Observaram-se diferenças estatísticas significativas entre respostas dos participantes por faixa etária para os itens da *RScB*: item 3-usa a mesma palavra-passe para diferentes *websites*, rejeitando-se a hipótese nula de distribuição igual entre faixas etárias com χ2(3)=7,977, *p=0,046*, com a comparações múltiplas que determina diferenças estatísticas entre as faixais etárias [38;43] e as faixas etária ≥53 com *p=0,025* e com a faixa etária ≤37 com *p=0,012.* Para o item 6-usa Wi-Fi de livre acesso público, com $\chi^2(3)=12,006$, *p*=0,007 com diferenças estatísticas entre as faixas etárias [44;53]-[38;43] com *p=0,003* e na faixa etária >=53-[38;43] com *p*=0,005. Para o item 10-Utiliza a *pen drive* pessoal com a finalidade de transferir informação nos computadores da instituição, com $\chi^2(3)=9,994$, *p*=0,019 com diferenças estatísticas entre as faixas etárias [44;53]->=53 com *p=0,019* e na faixa etária [44;53]-[38;43] com *p*=0,004. Por fim no item 19- Descarrega informação e material de *websites* para o computador de trabalho sem a preocupação da sua autenticidade, com $\chi^2(3)=8,424$, *p*=0,038 com diferenças estatísticas nas faixas etárias entre os <=37->=53 com *p=0,006*, na faixa etária entre os[38;43]->=53 com *p*=0,025 e na faixa etária entre os [44;53]->=53 com *p=0,048 (figura 5.3).*

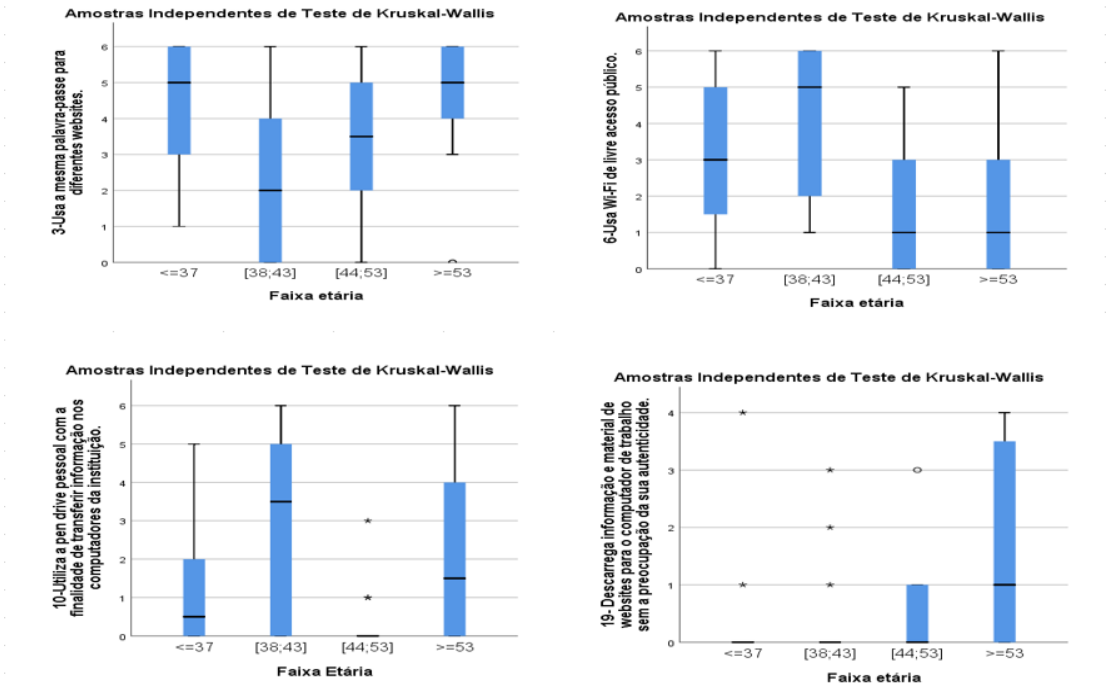


Figura 4.3 – Diagramas em caixa dos itens RScB que apresentam diferenças estatísticas por faixa etária.

Relativamente à análise dos itens do questionário *RScB* comparando os resultados entre os grupos profissionais, houve necessidade de realizar um pequeno ajuste devido à existência de grupos profissionais constituídos apenas por dois participantes. Por coerência estatística estes grupos profissionais foram excluídos reduzindo a dimensão da amostra estudada para 52 participantes.

Verifica-se diferenças estatísticas significativas entre os grupos profissionais para os seguintes itens da escala *RScB*: 6-Usa Wi-Fi de livre acesso público, rejeitando-se a hipótese de distribuição idêntica entre os grupos profissionais $\chi^2(3)=7{,}995$, $p=0{,}046$ com diferenças estatísticas significativas entre os grupos profissionais: Médico-TSDT, p=0,023 e Enfermeiro-TSDT, p=0,022. Verificou-se que no item 17-Carrega em *links* de *email* enviados por amigos próximos ou de colegas de trabalho, existem diferenças estatísticas entre grupos profissionais rejeitando-se a hipótese de distribuição igual com $\chi^2(3)=8{,}786$, $p=0{,}032$ com diferenças estatísticas significativas entre os grupos profissionais: Médico-TSDT, p=0,014; Médico-Assistente Operacional, $p=0{,}045$; Enfermeiro-TSDT, $p=0{,}044$ (figura 5.4).

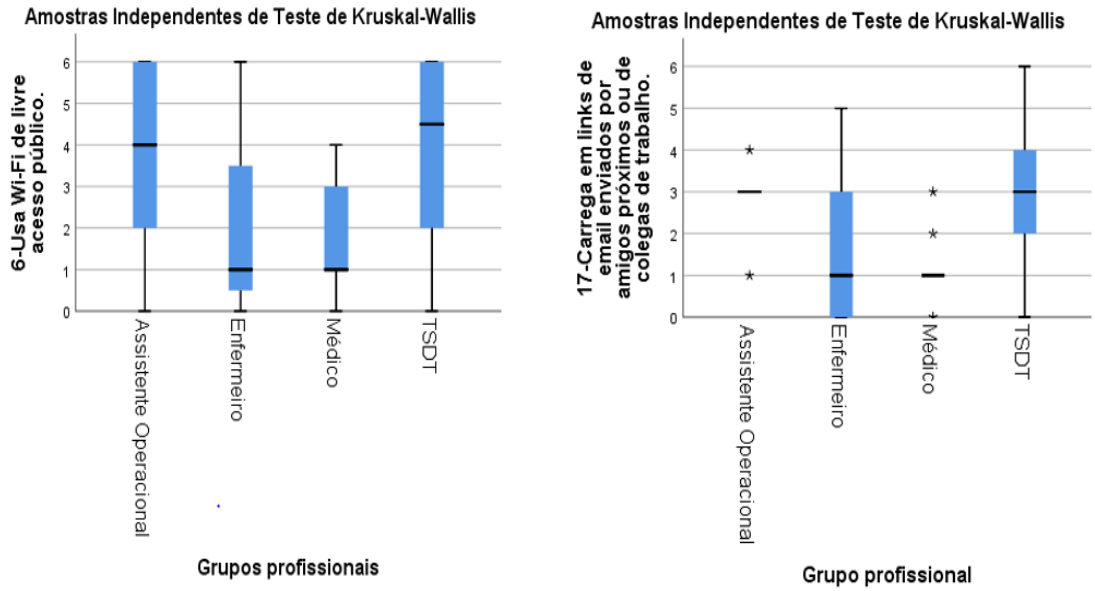


Figura 4.4- Diagramas em caixa dos itens RScB que apresentam diferenças estatísticas por grupo profissional.

Finalmente, estudou-se a distribuição dos itens da *RScB* por género, recorrendo-se ao teste de Mann-Whitney, verifica-se que existem diferenças estatísticas entre géneros no item 12- Descarrega conteúdos digitais (música, filmes, jogos, etc…) de fontes não fidedignas. Com U=140,500, $p=0{,}001$ (figura 5.5).

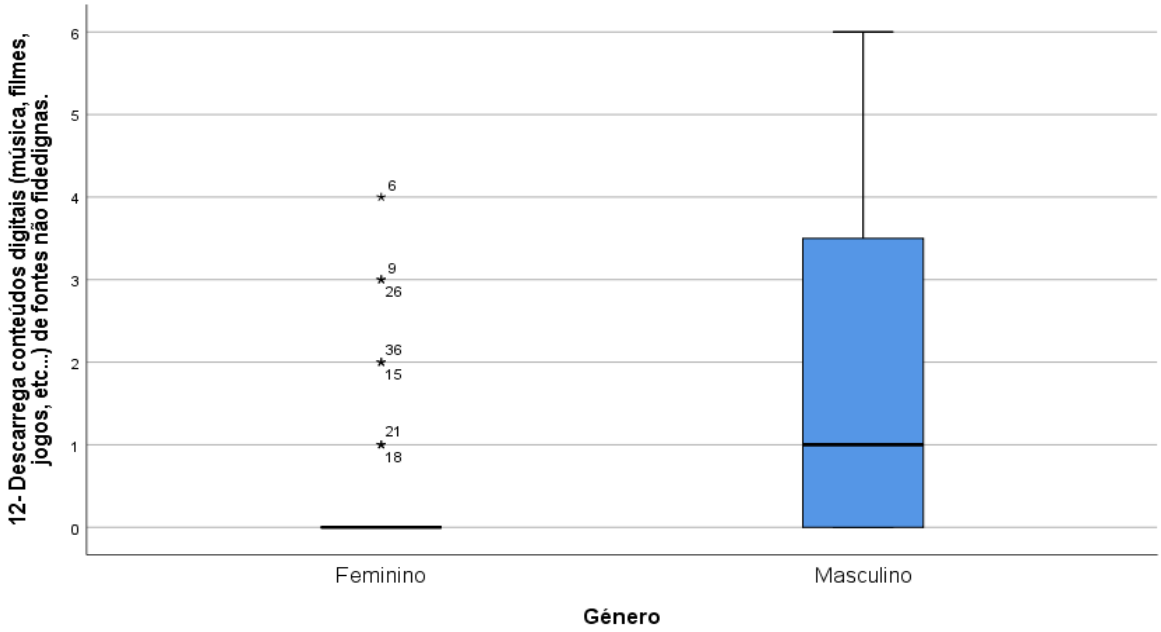


Figura 4.5 - Diagramas em caixa dos itens RScB que apresentam diferenças estatísticas por género.

Relativamente aos itens da *ATC-IB* verifica-se que não existem diferenças entre faixas etárias, no entanto, existem diferenças estatísticas significativas entre respostas dos participantes por grupo profissional para o item 7 da *ATC-IB* "Os sistemas de informação oferecem toda a proteção que uma instituição necessita", com $\chi^2(3)=8{,}126$, $p=0{,}046$ com diferenças estatísticas significativas entre os grupos profissionais: Assistente Operacional-TSDT, $p=0{,}037$; Assistente Operacional-Enfermeiro, $p=0{,}021$; Assistente Operacional-Médico, $p=0{,}005$.

Relativamente ao item 12 da escala *ATC-IB* "A Autoridade está demasiado ocupada para se preocupar com o cibercrime" rejeitando-se a hipótese de distribuição igual entre os grupos profissionais, com $\chi^2(3)=10{,}513$, $p=0{,}015$ com diferenças estatísticas significativas entre os grupos profissionais: Assistente Operacional-Médico, $p=0{,}020$ e Enfermeiro-Médico, $p=0{,}002$ (figura 5.6).

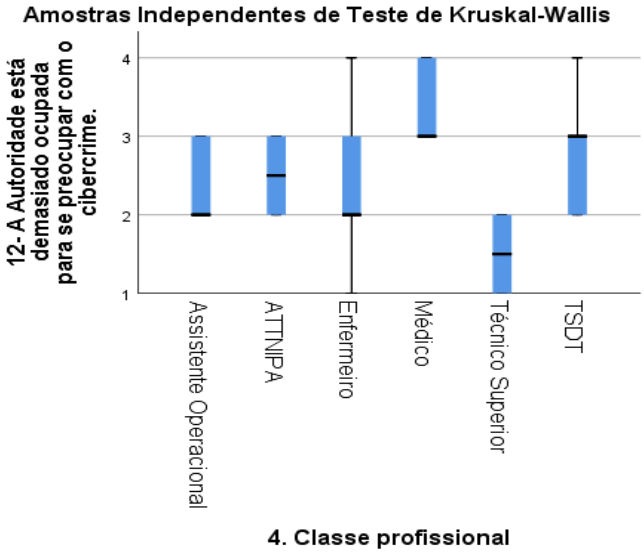


Figura 4.6 - Representação gráfica da distribuição das respostas por grupo profissional do Item 12 da ATC-IB

Finalmente, estudou-se a distribuição dos itens da *ATC-IB* por género, recorrendo-se ao teste de *Mann-Whitney*. Verifica-se que existe diferenças significativas entre género, no item da 6- Não creio que a segurança informática seja uma prioridade na minha instituição, u=214, p=0,039 e no item 8- Creio que denunciar o cibercrime é uma perda de tempo, u=222, p=0,046 (figura 5.7).

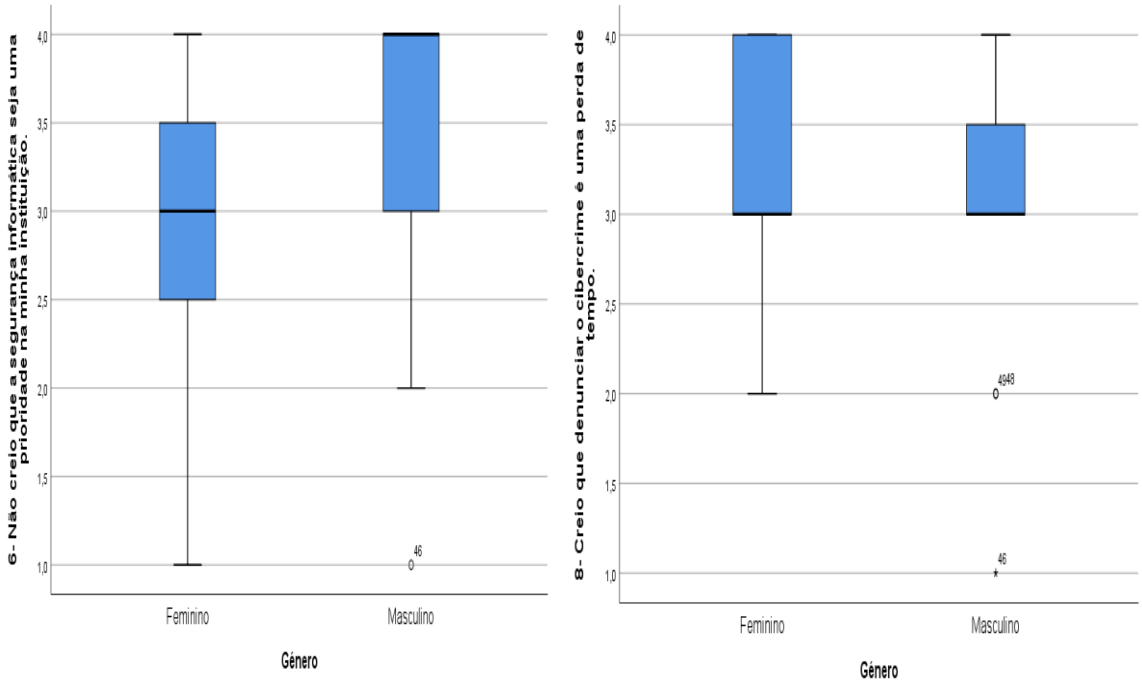


Figura 4.7 Diagramas em caixa dos itens da ATC-IB com diferenças estatísticas por género.

4.7.1 RScB - Resumo por item

Para ter uma perceção global do comportamento de arriscados em cibersegurança dos profissionais de saúde apresenta-se de seguida a distribuição dos itens em frequências e percentagens do questionário *RScB* (Tabela 5.1 e 5.2).

Tabela 4.1 Resumo dos itens 1 ao 8 da RScB por frequências e percentagem.

1- Partilha palavras-passe com amigos e colegas

		Frequência	%	% válida	% acumulativa
Válido	Nunca	38	67,9	67,9	67,9
	por semestre	5	8,9	8,9	76,8
	por trimestre	3	5,4	5,4	82,1
	por mês	3	5,4	5,4	87,5
	por quinzena	4	7,1	7,1	94,6
	por semana	2	3,6	3,6	98,2
	Diariamente	1	1,8	1,8	100,0
	Total	56	100,0	100,0	

2- Usa ou cria palavras-passe pouco complicadas ou com menos de 8 caracteres

		Frequência	%	% válida	% acumulativa
Válido	Nunca	22	39,3	39,3	39,3
	por semestre	10	17,9	17,9	57,1
	por trimestre	7	12,5	12,5	69,6
	por mês	3	5,4	5,4	75,0
	por quinzena	2	3,6	3,6	78,6
	por semana	3	5,4	5,4	83,9
	Diariamente	9	16,1	16,1	100,0
	Total	56	100,0	100,0	

3-Usa a mesma palavra-passe para diferentes websites.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	8	14,3	14,3	14,3
	por semestre	4	7,1	7,1	21,4
	por trimestre	5	8,9	8,9	30,4
	por mês	9	16,1	16,1	46,4
	por quinzena	3	5,4	5,4	51,8
	por semana	12	21,4	21,4	73,2
	Diariamente	15	26,8	26,8	100,0
	Total	56	100,0	100,0	

4- Usa sistemas de armazenamento online para partilhar ou guardar informação pessoal e sensível.(google drive, dropbox, onedrive, etc..)

		Frequência	%	% válida	% acumulativa
Válido	Nunca	22	39,3	39,3	39,3
	por semestre	6	10,7	10,7	50,0
	por trimestre	5	8,9	8,9	58,9
	por mês	6	10,7	10,7	69,6
	por quinzena	5	8,9	8,9	78,6
	por semana	3	5,4	5,4	83,9
	Diariamente	9	16,1	16,1	100,0
	Total	56	100,0	100,0	

5- Insere informação de pagamento em websites que não têm informação/certificação de segurança explícita.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	41	73,2	73,2	73,2
	por semestre	5	8,9	8,9	82,1
	por trimestre	6	10,7	10,7	92,9
	por quinzena	3	5,4	5,4	98,2
	por semana	1	1,8	1,8	100,0
	Total	56	100,0	100,0	

6-Usa Wi-Fi de livre acesso público.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	11	19,6	19,6	19,6
	por semestre	11	19,6	19,6	39,3
	por trimestre	5	8,9	8,9	48,2
	por mês	7	12,5	12,5	60,7
	por quinzena	7	12,5	12,5	73,2
	por semana	4	7,1	7,1	80,4
	Diariamente	11	19,6	19,6	100,0
	Total	56	100,0	100,0	

7-Confia num amigo ou colega próximo para conselhos em aspetos de segurança online.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	12	21,4	21,4	21,4
	por semestre	9	16,1	16,1	37,5
	por trimestre	9	16,1	16,1	53,6
	por mês	8	14,3	14,3	67,9
	por quinzena	4	7,1	7,1	75,0
	por semana	6	10,7	10,7	85,7
	Diariamente	8	14,3	14,3	100,0

8-Descarrega antivírus gratuitos de fontes desconhecidas.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	43	76,8	76,8	76,8
	por semestre	5	8,9	8,9	85,7
	por trimestre	3	5,4	5,4	91,1
	por mês	2	3,6	3,6	94,6
	por quinzena	2	3,6	3,6	98,2
	Diariamente	1	1,8	1,8	100,0
	Total	56	100,0	100,0	

Tabela 4.2 Resumo dos itens 9 ao 20 da RScB em frequências e percentagem.

9-Desativa o antivírus do computador de trabalho para que possa descarregar informação de websites.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	45	80,4	80,4	80,4
	por semestre	6	10,7	10,7	91,1
	por trimestre	2	3,6	3,6	94,6
	por mês	2	3,6	3,6	98,2
	por quinzena	1	1,8	1,8	100,0
	Total	56	100,0	100,0	

10-Utiliza a pen drive pessoal com a finalidade de transferir informação nos computadores da instituição.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	28	50,0	50,0	50,0
	por semestre	7	12,5	12,5	62,5
	por trimestre	4	7,1	7,1	69,6
	por mês	5	8,9	8,9	78,6
	por quinzena	3	5,4	5,4	83,9
	por semana	6	10,7	10,7	94,6
	Diariamente	3	5,4	5,4	100,0
	Total	56	100,0	100,0	

11- Verifica regularmente as actualizações de software do smartphone/tablet/portátil/PC..

		Frequência	%	% válida	% acumulativa
Válido	Nunca	7	12,5	12,5	12,5
	por semestre	10	17,9	17,9	30,4
	por trimestre	7	12,5	12,5	42,9
	por mês	10	17,9	17,9	60,7
	por quinzena	8	14,3	14,3	75,0
	por semana	5	8,9	8,9	83,9
	Diariamente	9	16,1	16,1	100,0
	Total	56	100,0	100,0	

12- Descarrega conteúdos digitais (música, filmes, jogos, etc...) de fontes não fidedignas.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	36	64,3	64,3	64,3
	por semestre	6	10,7	10,7	75,0
	por trimestre	4	7,1	7,1	82,1
	por mês	5	8,9	8,9	91,1
	por quinzena	3	5,4	5,4	96,4
	por semana	1	1,8	1,8	98,2
	Diariamente	1	1,8	1,8	100,0
	Total	56	100,0	100,0	

13-Partilha a sua localização nas redes sociais. (Fotos, local de trabalho...)

		Frequência	%	% válida	% acumulativa
Válido	Nunca	25	44,6	44,6	44,6
	por semestre	13	23,2	23,2	67,9
	por trimestre	6	10,7	10,7	78,6
	por mês	5	8,9	8,9	87,5
	por quinzena	4	7,1	7,1	94,6
	por semana	1	1,8	1,8	96,4
	Diariamente	2	3,6	3,6	100,0
	Total	56	100,0	100,0	

14- Aceita solicitações de amizade em redes sociais porque reconhece fotos.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	23	41,1	41,1	41,1
	por semestre	7	12,5	12,5	53,6
	por trimestre	7	12,5	12,5	66,1
	por mês	7	12,5	12,5	78,6
	por quinzena	4	7,1	7,1	85,7
	por semana	4	7,1	7,1	92,9
	Diariamente	4	7,1	7,1	100,0
	Total	56	100,0	100,0	

15- Carrega em links de email não solicitados de uma fonte desconhecida.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	50	89,3	89,3	89,3
	por semestre	3	5,4	5,4	94,6
	por trimestre	2	3,6	3,6	98,2
	por mês	1	1,8	1,8	100,0
	Total	56	100,0	100,0	

16- Envia informação pessoal a estranhos pela Internet. (contactos nas redes sociais, dá números de telefone ou email para obter códigos de download ou prémios, etc..)

		Frequência	%	% válida	% acumulativa
Válido	Nunca	51	91,1	91,1	91,1
	por semestre	3	5,4	5,4	96,4
	por trimestre	1	1,8	1,8	98,2
	por mês	1	1,8	1,8	100,0
	Total	56	100,0	100,0	

17-Carrega em links de email enviados por amigos próximos ou de colegas de trabalho.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	13	23,2	23,2	23,2
	por semestre	14	25,0	25,0	48,2
	por trimestre	5	8,9	8,9	57,1
	por mês	15	26,8	26,8	83,9
	por quinzena	4	7,1	7,1	91,1
	por semana	4	7,1	7,1	98,2
	Diariamente	1	1,8	1,8	100,0
	Total	56	100,0	100,0	

18-Verifica atualizações para qualquer antivírus que tenha instalado.

		Frequência	%	% válida	% acumulativa
Válido	Nunca	5	8,9	8,9	8,9
	por semestre	6	10,7	10,7	19,6
	por trimestre	6	10,7	10,7	30,4
	por mês	9	16,1	16,1	46,4
	por quinzena	9	16,1	16,1	62,5
	por semana	5	8,9	8,9	71,4
	Diariamente	16	28,6	28,6	100,0
	Total	56	100,0	100,0	

19- Descarrega informação e material de websites para o

		Frequência	%	% válida	% acumulativa
Válido	Nunca	40	71,4	71,4	71,4
	por semestre	7	12,5	12,5	83,9
	por trimestre	2	3,6	3,6	87,5
	por mês	3	5,4	5,4	92,9
	por quinzena	4	7,1	7,1	100,0
	Total	56	100,0	100,0	

20-Guarda informação da empresa no dispositivo eletrónico

		Frequência	%	% válida	% acumulativa
Válido	Nunca	37	66,1	66,1	66,1
	por semestre	9	16,1	16,1	82,1
	por mês	5	8,9	8,9	91,1
	por quinzena	4	7,1	7,1	98,2
	Diariamente	1	1,8	1,8	100,0
	Total	56	100,0	100,0	

4.7.2 ATC-IB - Resumo por item

Para ter uma perceção global das atitudes para cibersegurança dos profissionais de saúde apresenta-se de seguida a distribuição dos itens em frequências e percentagens do questionário *ATC-IB* (Tabela 5.3 a 5.5).

Tabela 4.3 Resumo dos itens 1 ao 8 da ATC-IB em frequências e percentagem.

1- Penso que a administração tem a responsabilidade de assegurar que a instituição de saúde esteja protegida contra o cibercrime.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	41	73,2	73,2	73,2
	Concordo.	15	26,8	26,8	100,0
	Total	56	100,0	100,0	

2- Estou ciente do meu papel em manter a instituição protegida de potenciais ciberameaças

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	1	1,8	1,8	1,8
	Concordo.	2	3,6	3,6	5,4
	Discordo.	15	26,8	26,8	32,1
	Discordo totalmente	38	67,9	67,9	100,0
	Total	56	100,0	100,0	

3- Penso que todos na instituição têm um papel a desempenhar na proteção contra as ciberameaças.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	41	73,2	73,2	73,2
	Concordo.	15	26,8	26,8	100,0
	Total	56	100,0	100,0	

4- É difícil saber como posso proteger a instituição do cibercrime.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	9	16,1	16,1	16,1
	Concordo.	27	48,2	48,2	64,3
	Discordo.	19	33,9	33,9	98,2
	Discordo totalmente	1	1,8	1,8	100,0
	Total	56	100,0	100,0	

5- Não tenho as competências necessárias para proteger a instituição do cibercrime.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	13	23,2	23,2	23,2
	Concordo.	23	41,1	41,1	64,3
	Discordo.	18	32,1	32,1	96,4
	Discordo totalmente	2	3,6	3,6	100,0
	Total	56	100,0	100,0	

6- Não creio que a segurança informática seja uma prioridade na minha instituição.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	7	12,5	12,5	12,5
	Concordo.	5	8,9	8,9	21,4
	Discordo.	25	44,6	44,6	66,1
	Discordo totalmente	19	33,9	33,9	100,0
	Total	56	100,0	100,0	

7-Os sistemas de informação oferecem toda a proteção que uma instituição necessita.

		Frequência	%	% válida	% acumulativa
Válido	Concordo.	10	17,9	17,9	17,9
	Discordo.	40	71,4	71,4	89,3
	Discordo totalmente	6	10,7	10,7	100,0
	Total	56	100,0	100,0	

8- Creio que denunciar o cibercrime é uma perda de tempo.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	1	1,8	1,8	1,8
	Concordo.	3	5,4	5,4	7,1
	Discordo.	29	51,8	51,8	58,9
	Discordo totalmente	23	41,1	41,1	100,0
	Total	56	100,0	100,0	

Tabela 4.4 Resumo dos itens 9 ao 18 da ATC-IB em frequências e percentagem.

9- A Autoridade não tem meios para combater o cibercrime de forma eficaz.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	6	10,7	10,7	10,7
	Concordo.	27	48,2	48,2	58,9
	Discordo.	21	37,5	37,5	96,4
	Discordo totalmente	2	3,6	3,6	100,0
	Total	56	100,0	100,0	

10- Creio que os hackers e cibercriminosos são mais talentosos do que as pessoas que nos deviam proteger.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	9	16,1	16,1	16,1
	Concordo.	29	51,8	51,8	67,9
	Discordo.	14	25,0	25,0	92,9
	Discordo totalmente	4	7,1	7,1	100,0
	Total	56	100,0	100,0	

11- Os boletins informativos governamentais em relação ao cibercrime não são relevantes para a instituição de saúde.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	2	3,6	3,6	3,6
	Concordo.	11	19,6	19,6	23,2
	Discordo.	36	64,3	64,3	87,5
	Discordo totalmente	7	12,5	12,5	100,0
	Total	56	100,0	100,0	

12- A Autoridade está demasiado ocupada para se preocupar com o cibercrime.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	3	5,4	5,4	5,4
	Concordo.	20	35,7	35,7	41,1
	Discordo.	26	46,4	46,4	87,5
	Discordo totalmente	7	12,5	12,5	100,0
	Total	56	100,0	100,0	

13- Receio que, se denunciar um ciberataque à Autoridade, isso vá prejudicar a minha reputação interna.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	2	3,6	3,6	3,6
	Concordo.	7	12,5	12,5	16,1
	Discordo.	32	57,1	57,1	73,2
	Discordo totalmente	15	26,8	26,8	100,0
	Total	56	100,0	100,0	

14- Penso que deverá ser feito mais para comunicar os riscos do cibercrime aos profissionais.

		Frequência	%	% válida	% acumulativa
Válido	Concordo.	1	1,8	1,8	1,8
	Discordo.	30	53,6	53,6	55,4
	Discordo totalmente	25	44,6	44,6	100,0
	Total	56	100,0	100,0	

15- Estou a par da política de uso informático da instituição de saúde, e tento manter-me atualizado

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	3	5,4	5,4	5,4
	Concordo.	22	39,3	39,3	44,6
	Discordo.	27	48,2	48,2	92,9
	Discordo totalmente	4	7,1	7,1	100,0
	Total	56	100,0	100,0	

16- Se ocorrer um ciberataque, não saberei como denunciá-lo.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	5	8,9	8,9	8,9
	Concordo.	31	55,4	55,4	64,3
	Discordo.	20	35,7	35,7	100,0
	Total	56	100,0	100,0	

17- Não acho que é minha responsabilidade denunciar um ciberataque contra a instituição de saúde.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	2	3,6	3,6	3,6
	Concordo.	5	8,9	8,9	12,5
	Discordo.	34	60,7	60,7	73,2
	Discordo totalmente	15	26,8	26,8	100,0
	Total	56	100,0	100,0	

18- Não presto atenção ao material informativo da instituição sobre ameaças de cibercrime.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	1	1,8	1,8	1,8
	Concordo.	12	21,4	21,4	23,2
	Discordo.	39	69,6	69,6	92,9
	Discordo totalmente	4	7,1	7,1	100,0
	Total	56	100,0	100,0	

Tabela 4.5 Resumo dos itens 19 ao 25 da ATC-IB em frequências e percentagem.

19- Confio na minha capacidade de reconhecer sinais de um ciberataque.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	7	12,5	12,5	12,5
	Concordo.	27	48,2	48,2	60,7
	Discordo.	19	33,9	33,9	94,6
	Discordo totalmente	3	5,4	5,4	100,0
	Total	56	100,0	100,0	

20- Penso que a maior ameaça para os sistemas informáticos vem de pessoas de dentro da instituição de saúde.

		Frequência	%	% válida	% acumulativa
Válido	Concordo.	29	51,8	51,8	51,8
	Discordo.	17	30,4	30,4	82,1
	Discordo totalmente	10	17,9	17,9	100,0
	Total	56	100,0	100,0	

21- Sinto que qualquer pessoa da organização está em risco de manipulação por ciber "vigaristas e burlões"

		Frequência	%	% válida	% acumulativa
Válido	Concordo.	7	12,5	12,5	12,5
	Discordo.	36	64,3	64,3	76,8
	Discordo totalmente	13	23,2	23,2	100,0
	Total	56	100,0	100,0	

22- Penso que os cibercriminosos e hackers apenas atingem uma instituição de saúde quando têm muito a ganhar do ponto de vista financeiro.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	9	16,1	16,1	16,1
	Concordo.	14	25,0	25,0	41,1
	Discordo.	31	55,4	55,4	96,4
	Discordo totalmente	2	3,6	3,6	100,0
	Total	56	100,0	100,0	

23- Apenas as grandes empresas e organizações são alvo dos hackers e cibercriminosos.

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	1	1,8	1,8	1,8
	Concordo.	6	10,7	10,7	12,5
	Discordo.	38	67,9	67,9	80,4
	Discordo totalmente	11	19,6	19,6	100,0
	Total	56	100,0	100,0	

24- Apenas as instituições de saúde que recebem pagamentos por sistemas online estão em risco de serem vítimas de um ciberataque.

		Frequência	%	% válida	% acumulativa
Válido	Concordo.	2	3,6	3,6	3,6
	Discordo.	38	67,9	67,9	71,4
	Discordo totalmente	16	28,6	28,6	100,0
	Total	56	100,0	100,0	

25- Não sei quem é o responsável por proteger a instituição de saúde das ciberameaças

		Frequência	%	% válida	% acumulativa
Válido	Concordo totalmente.	8	14,3	14,3	14,3
	Concordo.	21	37,5	37,5	51,8
	Discordo.	22	39,3	39,3	91,1
	Discordo totalmente	5	8,9	8,9	100,0
	Total	56	100,0	100,0	

5 Discussão

O presente estudo teve como objetivo conhecer quais os comportamentos e as atitudes em relação à cibersegurança que os profissionais de saúde têm em função dos seus conhecimentos atuais.

Com base nas pesquisas realizadas, importa referir que se tratar de um estudo pioneiro em Portugal sobre a cibersegurança aplicado ao sector da saúde, sector esse, que evidência em Portugal tal como no resto do mundo, uma grande abrangência decorrente da multidimensionalidade, multiplicidade e diversidade de pessoas, processos e dos domínios relacionados, os quais dificultam os processos de caracterização desta pertinente temática.

Na pesquisa de literatura internacional efetuada encontram-se publicados alguns estudos sobre o factor humano da cibersegurança que relacionam a dependência tecnológica e a impulsividade dos utilizadores com as atitudes e com os comportamentos demostrados como forma de caracterizar a ameaça interna não intencional. Foram identificados três publicações com a utilização destas escalas especificas nos trabalhos realizados no Reino Unido por *Lee Hadlington* "*Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours"* de 2017 e o "*Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom" de 2018* e nos Estados Unidos América (*Texas*) por Aivazpour Z. & Rao VSC. "*Impulsivity and Risky Cybersecurity Behaviors: A Replication" de* 2018*.*

Todo o processo metodológico de tradução e validação do conteúdo dos questionários decorreu sem grandes dificuldades ou obstáculos entre todos os intervenientes no processo, no entanto há que salientar dois aspetos importantes:

I. Uma das traduções foi realizada por intervenientes em que a língua materna não era o inglês, apesar de uma das duas traduções efetuadas, ser de uma tradutora profissional. Assume que este facto pode induzir algum viés;
II. A aplicação do pré-teste decorreu numa plataforma digital diferente da aplicada, pela manifesta dificuldade em garantir a participação unitária dos inquiridos. Nesta fase foi salientada a desadequação da janela temporal da escala *RScB* à temática e ao que era inquirido, constituindo um ponto de algum viés.

A fiabilidade foi analisada sob o ponto de vista da consistência interna dos questionários através da determinação do α de Cronbach. Os valores encontrados para estes questionários são considerados indicadores de consistência interna razoável.

Para os 20 e 25 itens, o α de Cronbach foi respetivamente de 0,745 e de 0,723, o que se considera que o instrumento tem uma boa consistência interna, permitindo assim passar à etapa seguinte. Pelo exposto o instrumento apresenta características razoáveis para medir.

A forma mais prática de avaliar o valor de alfa é pela comparação do valor calculado com o valor preconizado por diferentes autores. Esta comparação é imprecisa devido às limitações estatísticas, nomeadamente a amostragem reduzida. Efetivamente é uma limitação deste estudo se tivermos em conta a taxa reduzida de participação: num universo de 1726 profissionais apenas 65 responderam aos questionários, o que se traduz numa taxa de participação de 3,8%. Esta fraca afluência pode ser explicada por vários motivos:

I. A participação nos questionários realizou-se dentro do portal digital da entidade de saúde, implicando ao profissional dispensar algum do seu precioso tempo.
II. As entidades de saúde, especialmente os hospitais constituem ambientes de trabalho particularmente stressantes, contendo características organizacionais geralmente associadas com o stress o que limita a participação;
III. Como se trata de um estudo em ambiente hospitalar e no sentido de evitar a participação múltipla do mesmo participante, bloqueou-se o ID de sessão de navegação por definição de um cookie próprio da plataforma digital dos questionários. Este procedimento é importante para manter a participação individualizada, no entanto, constituiu uma limitação à participação dado que, na entidade em estudo, os computadores são partilhados entre os diferentes profissionais;
IV. O período de participação no estudo ser reduzido (6 semanas), por razões logísticas inerentes à vertente académica. Ao contrário do estudo realizado por *L.Hadlington,* este não teve qualquer financiamento ou estímulo à participação.
V. Por fim, o intervalo temporal do estudo (dezembro 2018 a 15 janeiro 2019), altura das épocas festivas com muitos profissionais de férias condicionando a participação. Esta calendarização está intimamente ligada ao processo académico.

Este estudo, demonstrou existir uma correlação moderadamente negativa (r(56)=-0,414) entre escalas *RScB* e *ATC-IB*, valores em consonância com os dados apresentados por (*Hadlington, 2017*) de (r(515)=-0,300)(9). Relativamente à correlação entre os valores da escala *RScB* e da escala *ATC-IB* com a variável idades, não se observou a existência de uma correlação significativa.

A média obtida pelos profissionais de saúde do CHBM inquiridos para a escala *ATC-IB* que foi de (66,41±6,263), inversamente à média geral obtida da escala *RScB* foi de (31,59 ±14,211).

Na literatura consultada encontraram-se descritos valores de (60,19±7,31) para a métrica *ATC-IB* e de (27,72±14,81) para à métrica *RScB* (*Hadlington,2017*), contudo como se trata de uma temática em desenvolvimento, que privilegia a aplicação de questionários como forma de sondagem ou inquérito da realidade que se pretende investigar, é natural que estas escalas sejam ajustadas ao longo do tempo, dificultando a comparação por falta de mais estudos. A ausência de um *Gold standard*, tal como descrito por *Serge Egelman* (2015), sobre as atitudes e comportamentos em cibersegurança é uma limitação na comparação de resultados, que se mantem.

A população estudada na entidade pública de saúde foi maioritariamente feminina, 71% dos participantes, distribuídos por diferentes grupos profissionais e por diferentes faixas etárias sem predomínio.

Pode-se caracterizar, apesar da reduzida dimensão da amostra em estudo, os profissionais de saúde como indivíduos com comportamentos em cibersegurança globalmente positivos independentemente do género, faixas etárias e grupo profissional, denotando, contudo, algumas diferenças por faixa etárias [≤37] e [≥53] ao nível do uso da mesma palavra passe para diferentes *websites* com 48,2% dos participantes confirmarem a utilização da mesma palavra passe numa base diária ou semanal apenas 14,4% respondeu nunca usa a mesma palavra passe para diferentes *websites*. Trata-se de uma limitação humana, algo que se torna incomportável para os utilizadores, em particular os que trabalham em ambientes stressantes, onde todos os minutos contam, como é o caso dos profissionais de saúde, algo que será mitigado com a introdução MFA, em particular com utilizam dos dados biométricos.

O uso da *Wi-Fi* de acesso livre apresenta uma diferença por faixa etária interessante, já que as faixas etárias [44;52] e [≥53] com menor tendência para usarem o Wi-Fi de livre acesso comparativamente às restantes, algo que pode ser explicado pela relação com os grupos profissionais, a qual também apresenta diferenças entre os médicos e

enfermeiros relativamente aos Técnicos Superiores de Diagnostico e assistentes operacionais possivelmente devido a uma ligação ao poder económico, um ponto passível de futuros estudos, como o poder económico individual pode condicionar a relação com a segurança da informação. 19,6% dos inquiridos usa diariamente a *wi-fi* de livre acesso. O Utilizo da *pen drive* pessoal nos computadores da instituição observou-se que a grupo etário [44;52] apresenta um comportamento diferente dos restantes. Trata-se de um ponto relevante das entidades publicas de saúde a ausência de aplicações informáticas de gestão para além dos horários do pessoal, forçando muitos dos profissionais com cargos de gestão a recorrerem a estes sistemas de transporte de informação entre sistemas constituindo uma vulnerabilidade documentada, mas recorrente em virtude de ausências de opções credíveis face as necessidades.

Por fim, no item 19- Descarrega informação e material de *websites* para o computador de trabalho sem a preocupação da sua autenticidade, da *RScB* comparado com as faixas etárias, observou-se uma diferença estatística entre a faixa etária [≥53] relativamente às restantes faixas. Pode-se afirmar que os profissionais com idades superiores ou iguais a 53 anos não apresentam uma preocupação com autenticidade do material descarregado dos *websites*, constituindo uma vulnerabilidade importante que necessita aprofundamento.

Relativamente as atitudes em relação à cibersegurança em ambiente empresarial, a escala não apresenta diferenças significativas entre os entre grupos profissionais, faixa etárias e género quando se demostrar um claro elevado envolvimento dos profissionais com a segurança dos dados dos doentes, uma atitude positiva para a cibersegurança em ambiente hospitalar superior aos dados encontrados na literatura. Este facto constitui um achado significativo, face aos valores publicados por *Hadlington (2018).*

A analise por item da escala de *ATC-IB* por faixa etária não revelou diferenças estatísticas significativas.

O estudo da distribuição por item da escala *ATC-IB* por grupo profissional foi efetuado com uma amostra de 52 elementos por existir grupos profissionais com dois ou menos indivíduos. A distribuição do item 7 da escala *ATC-IB* “Sistemas de informação oferecem toda a proteção que uma instituição necessita”, demostrou a existência de diferenças estatísticas entre o grupo profissional assistente operacional e a restantes classe profissionais, sendo que 60% dos inquiridos deste grupo profissional respondeu que concorda com a afirmação, que os sistemas de informação oferecem toda a proteção.

Por fim, na análise do item 12-“A Autoridade está demasiado ocupada para se preocupar com o cibercrime”, observou-se diferenças estatísticas entre o grupo profissional médicos e os enfermeiros e os assistentes operacionais, como todos os médicos discordar deste item.

Relativamente a análise por género as diferenças estatísticas nos itens: 6-“Não creio que a segurança informática seja uma prioridade na minha instituição” com o item 8-“Creio que denunciar o cibercrime é uma perda de tempo, algo que se encontra relacionado com as políticas de segurança da informação da entidade.

6 Conclusões

O presente estudo, realizado no âmbito do mestrado GATS tem como ambição desenvolver e acrescentar conhecimentos sobre os aspetos humanos relacionados com a segurança da informação em saúde, através da elaboração de uma radiografia atual em cibersegurança dos profissionais de saúde em ambiente hospital. É importante conhecer estes factores humanos porque os SIS precisam ser protegidos contra os atacantes externos, as ameaças internas e até mesmo contra os ataques de terceiros e concorrentes.

É imperativo num processo de gestão, avaliar inicialmente a realidade antes de delinear qualquer estratégia de mitigação de riscos associados à segurança do doente e aos seus dados, em particular a relacionada com a utilização de tecnologias em saúde desenvolvendo novas iniciativas para a melhoria continua da ciberresiliência e a capacidade de resposta às quebras de segurança.

Este estudo permitiu confirmar a correlação entre comportamentos arriscados em cibersegurança e atitudes em relação à cibersegurança em ambiente empresarial, tal como descrito na literatura, estabelecendo-se a ponte para a quantificação da consciencialização em cibersegurança, pelo modelo KAB.

Na globalidade não foram identificadas diferenças estatísticas significativas entre as médias de *RScB* e *ATC-IB* como os factores sociodemográficos estudados: Grupo profissional, faixa etária e género. Um ponto relevante do estudo é o facto dos profissionais de saúde evidenciarem uma média elevada na escala *ATC-IB*, compatível com uma atitude positiva em cibersegurança da saúde. Este facto relaciona-se com a envolvência demostrada pelos profissionais com a temática de segurança das tecnologias de saúde e dos respetivos dados gerados, evidenciando uma clara abertura para as mudanças necessárias para corrigir eventuais comportamentos de risco desde que devidamente orientados, formados e treinados.

A aplicação destes questionários a este grupo populacional revelou ser uma mais valia não só pela aplicação pioneira em Portugal despertando para a necessidade de novas investigações dentro desta temática, como também permitiu fazer o retrato importante do estado atual dos comportamentos e atitudes em relação à cibersegurança em entidades de saúde.

As capacidades e competências dos profissionais de saúde em matéria de cibersegurança, precisam de ser avaliadas do mesmo modo que a tecnologia o é, porque sistemas tecnologicamente evoluídos necessitam de pessoas com formação,

com conhecimentos suficientes para evitar falhas de segurança segundo as políticas de segurança estabelecidas salvaguardando os cidadãos que dependem dos serviços prestados.

A identificação de pontos divergentes e convergentes permite colmatar eventuais vulnerabilidades de formação e de treino facilitando a implementação das políticas de segurança da informação pela adquisição de um conjunto de competências relacionadas com os comportamentos seguros no ciberespaço e, desta forma, contribuir para a consciencialização em cibersegurança forte e coesa entre profissionais, tecnologias e políticas.

Contudo, dada a reduzida dimensão da amostra, observa-se a necessidade de proceder a novas investigações no sentido de confirmar a confiabilidade, convergência e veracidade da versão traduzida com o objetivo da sua utilização futura para obtenção de um *Gold standard* em comportamentos e atitudes em relação à cibersegurança.

A importância determinar um *Gold standard* que estabeleça a relação entre atitudes e comportamentos em cibersegurança é fundamental porque na nossa aparentes segurança descobrimos as nossas inseguranças e as nossos lacunas relativamente a segurança da informação e à utilização da tecnologia atual e futura.

7 Limitações

Tratou-se de um estudo integrado num projeto académico, com algumas limitações temporais, que de alguma forma condicionaram os resultados, em virtude da dimensão da amostra inquirida.

A dimensão reduzida da amostra obtida, contribuiu para que a maior limitação deste estudo seja a fraca adesão dos profissionais, facto que pode ser explicado pela desmotivação dos profissionais de saúde, comprometendo a sua aplicabilidade.

A utilização das escalas tem implícito um viés documentado que limita os resultados obtidos, em especial em ambiente hospitalar, que dada a sua especificidade podem condicionar as respostas e as conclusões.

A aplicabilidade dos itens Likert da escala RScB ao nível de concordância ou não de 7 pontos (0 = Nunca - 6 = Diariamente) com os comportamentos em cibersegurança, numa janela temporal ‘últimos seis meses’, não favorece o desenvolvimento da escala RScB, existindo alguns itens em que a resposta poderá eventualmente sofrer algumas tendências, que necessitam ser investigadas.

8 Bibliografia

1. Model HTAC, Assessments HT, Hta T, Model C, Hta T, Model C, et al. The HTA Core Model ® Guiding principles on use. 2011;2–4.
2. Van Roessel I, Reumann M, Brand A. Potentials and Challenges of the Health Data Cooperative Model. Public Health Genomics. 2018;20(6):321–31.
3. Flores M, Glusman G, Brogaard K, Price ND, Hood L. P4 medicine: how systems medicine will transform the healthcare sector and society. Per Med [*Internet*]. 2013 Aug 1;10(6):565–76. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4204402/pdf/nihms532619.pdf
4. SPMS. Especificação Técnica MySNS Carteira – Documentação [*Internet*]. 2018. Available from: https://spms.min-saude.pt/wp-content/uploads/2018/02/PICC_-MySNS-Carteira-Documentação_v16022018_2.pdf
5. kaspersky. Depois de um ano de WannaCry , o EternalBlue ainda é um vetor de infecção [*Internet*]. 2018 [cited 2018 Aug 30]. Available from: https://go.kaspersky.com/rs/802-IJN-240/images/10052018_PR_One
6. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas [*Internet*]. 2018;113(March):48–52. Available from: https://doi.org/10.1016/j.maturitas.2018.04.008
7. Ladika S. Health care, an easy target, needs to get its guard up. Manag Care [*Internet*]. 2016;25(12):31. Available from: http://www.ncbi.nlm.nih.gov/pubmed/28121559
8. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Vol. 25, Technology and Health Care. 2017. p. 1–10.
9. Hadlington L. Human factors in cybersecurity; examining the link between *Internet* addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon [*Internet*]. 2017;3(7):e00346. Available from: http://dx.doi.org/10.1016/j.heliyon.2017.e00346
10. Hadlington L. Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. Int J Cyber Criminol. 2018;12(1):269–81.

11. Santos AFC. O Cibercrime Desafios E Respostas Do Direito [*Internet*]. Universidade Autónoma de Lisboa; 2015. Available from: http://repositorio.ual.pt/handle/11144/2640

12. Antunes M, e Rodrigues B. Introdução à Cibersegurança. 1ª Edição. Lisboa: FCA - Editora Informática; 2018. 244 p.

13. Kim L. Cybersecurity awareness: Protecting data and patients. Nursing (Lond). 2017;47(6):65–7.

14. Imprensa ODE. Plano de cibersegurança da UE para proteger a *Internet* aberta , a liberdade e as oportunidades em linha. 2013;

15. James Scott. What the Health sector needs.pdf [*Internet*]. Institute for Critical Infrastructure Technology. [cited 2018 Oct 26]. Available from: https://icitech.org/what-the-health-sector-needs-to-know-about-cryptocurrency-technologies-blockchain-and-cryptojacking-attacks/

16. Stanciu V, Tinca A. Exploring cybercrime – realities and challenges. Account Manag Inf Syst [*Internet*]. 2017;16(4):610–32. Available from: http://dx.doi.org/10.24818/jamis.2017.04009

17. Savage K, Coogan P, Lau H. Information Resources [*Internet*]. Vol. 54, Research-Technology Management. Mountain View, CA 94043 USA; 2015. Report No.: 1.0. Available from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

18. Sittig D, Singh H. A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. Appl Clin Inform [*Internet*]. 2016 Apr 16;07(02):624–32. Available from: http://www.thieme-connect.de/DOI/DOI?10.4338/ACI-2016-04-SOA-0064

19. Collier R. NHS ransomware attack spreads worldwide. CMAJ. 2017;189(22):E786–7.

20. SPMS. RSE spms.pdf [*Internet*]. [cited 2018 Oct 31]. Available from: http://spms.min-saude.pt/product/area-cidadao/

21. Camões L de, Promoção A para a, Informação D da. Interoperabilidade Na Saúde.2013;Availablefrom:http://www.apdsi.pt/uploads/news/id719/Estudo_APDSI_Interoperabilidade_Saúde_completo.pdf

22. Oficial J, Do UE, Europeu P, Conselho DO, Europeu S. 4.4.2011. 2011;2009.

23. Agency EU, Framework C. OF UNION An EU framework for cybersecurity certification. 2017;

24. SPMS. Despacho sobre Cibersegurança da Saúde [*Internet*]. 2017. Available from: https://spms.min-saude.pt/2017/10/despacho-ciberseguranca-da-saude/

25. Rocha S, dos Santos AP, Garcia A, Durão E, de Jesus G, Gregório J, et al. Tecnologias de informação em saúde. 2017;

26. Commission E. State of the Union 2018 – Cybersecurity: Commission proposes to invest in stronger and pioneering cybersecurity capacity in the EU [*Internet*]. [cited 2019 Mar 3]. Available from: https://ec.europa.eu/digital-single-market/en/news/state-union-2018-cybersecurity-commission-proposes-invest-stronger-and-pioneering-cybersecurity

27. Saúde MDA. Despacho n 1400A 2015- 10 de fevereiro 2015 - plano nacional para a segurança dos doentes. 2016;(2):2–10.

28. Direcção Geral da Saúde. Plano nacional de saúde: revisão e extensão a 2020. Direcção Geral da Saúde. 2015;38.

29. Martins H, Domingues J. Os 10 Mandamentos da Cibersegurança [*Internet*]. Acta Medica Portuguesa. 2018 [cited 2019 Feb 1]. Available from: http://www.actamedicaportuguesa.com/student/index.php/2018/01/27/os-10-mandamentos-da-ciberseguranca/

30. Bonfanti ME. Enhancing Cybersecurity by Safeguarding Information Privacy. Proc 13th Int Conf Availability, Reliab Secur - ARES 2018 [*Internet*]. 2018;1–6. Available from: http://dl.acm.org/citation.cfm?doid=3230833.3233289

31. União Europeia. Regulamento Geral de Proteção de Dados. J Of da União Eur. 2016;156.

32. Lopes IM, Oliveira P. Aplicabilidade do Regulamento Geral sobre Proteção de Dados em Clínicas de Saúde. Iber J Inf Syst Technol. 2018;118–30.

33. SearchHealthIT. Cybersecurity in Healthcare : 5 Best Practices [*Internet*]. TechTarget. 2018. Available from: https://cdn.ttgtmedia.com/digitalguide/images/Misc/EA-Marketing/NetSeceguides/Cybersecurity-in-Healthcare.pdf

34. MCGUIRE A. WHAT THE HEALTH SECTOR NEEDS TO KNOW ABOUT CRYPTOCURRENCY TECHNOLOGIES, BLOCKCHAIN, AND CRYPTOJACKING ATTACKS [*Internet*]. IRISH TECH NEWS. 2018. Available from: https://irishtechnews.ie/what-the-health-sector-needs-to-know-about-cryptocurrency-technologies-blockchain-and-cryptojacking-attacks/

35. Microsoft, Marsh. By the Numbers: Global Cyber Risk Perception Survey. 2018;(February).

36. Ts IEC. TECHNICAL SPECIFICATION ISO / IEC TS Information technology — Security techniques — Guidelines for the assessment of information security. 2019;2019.

37. Rose R V, Kass JS. Mitigating Cybersecurity Risks. 2017;23(2):553–6.

38. Rui Rijo. Regime de Cibersegurança na Saúde : CINTESIS. 2018.

39. Nissim N, Yahalom R, Elovici Y. USB-based attacks. Comput Secur [*Internet*]. 2017;70:675–88. Available from: https://doi.org/10.1016/j.cose.2017.08.002

40. Saúde PAPDE, Nunes AM, Nunes AM. constitucional , no que se refere ao dever do de todos os cidadãos independentemente da sua saúde , a prevenção da doença , o diagnóstico , o país (Norte , Centro , Lisboa e Vale do Tejo , totalidade das prestações pela rede pública , o integradas no SNS. 2017;16–28.

41. SPSM. SPMS- Esclarecimentos cuidados primários.pdf [*Internet*]. spms. 2018 [cited 2018 Nov 27]. p. 3. Available from: http://spms.min-saude.pt/2018/11/esclarecimento/

42. Microsoft. Windows xp.pdf [*Internet*]. [cited 2018 Nov 28]. Available from: https://support.microsoft.com/pt-pt/help/14223/windows-xp-end-of-support

43. Collier R. NHS ransomware attack spreads worldwide. CMAJ. 2017;189(22):E786----E787.

44. ARSLVT. Hospitalização Domiciliária (UHD) [*Internet*]. www.arslvt.min-saude.pt. 2016. Available from: https://www.arslvt.min-saude.pt/frontoffice/pages/2?news_id=853

45. Nunes AM. Crise E Volume De Internações Hospitalares Em Portugal. Saúde em Redes [*Internet*]. 2017;3(3):264–72. Available from: http://revista.redeunida.org.br/ojs/index.php/rede-unida/article/view/909

46. Pope J. Ransomware: Minimizing the risks. Innov Clin Neurosci. 2016;13(11–12):37–40.

47. Gleitman H, Gross J, Reisberg D. Psicologia. 7th ed. Lisboa: Fundação Calouste Gulbenkian; 2007.

48. Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, Zwaans T. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Comput Secur [*Internet*]. 2017;66:40–51. Available from: http://dx.doi.org/10.1016/j.cose.2017.01.004

49. Cain AA, Edwards ME, Still JD. An exploratory study of cyber hygiene behaviors and knowledge. J Inf Secur Appl [*Internet*]. 2018;42:36–45. Available from: https://doi.org/10.1016/j.jisa.2018.08.002

50. Symantec Corporation. Good cyber hygiene.pdf [*Internet*]. 2019 [cited 2019 Feb 15]. Available from: https://us.norton.com/*internet*security-how-to-good-cyber-hygiene.html

51. Norton Symantec. Good cyber hygiene.pdf [*Internet*]. [cited 2018 Sep 10]. Available from: https://us.norton.com/*internet*security-how-to-good-cyber-hygiene.html

52. CNCS. Engenharia social [*Internet*]. [cited 2019 Mar 3]. Available from: https://www.cncs.gov.pt/engenharia-social/

53. Ayala L. Cybersecurity for Hospitals and Healthcare Facilities. Cybersecurity for Hospitals and Healthcare Facilities. 2016.

54. McAfee. What is Malware? [*Internet*]. [cited 2019 Jan 15]. Available from: https://www.mcafee.com/enterprise/pt-br/security-awareness/ransomware/what-is-malware.html

55. Marin HDF. Sistemas de informação em saúde : considerações gerais Health information system : general considerations. J Heath Informatics. 2010;2(1):20–4.

56. Pinto OEV, Prof P, Paulo D, Carreira A, Prof V, Filipe D, et al. GESTÃO DO RISCO E GARANTIA DA INFORMAÇÃO : A INFLUÊNCIA DO FATOR HUMANO E DA ÉTICA NA SEGURANÇA Dissertação para a obtenção do Grau de Mestre em Segurança da Informação e Direito no Ciberespaço Júri. 2016;

57. Pedro M. Introdução à BlockChain. 1ª. FCA - Editores Informáticos, editor. Lisboa: Lidel - Edições Técnicas; 2018. 160 p.

58. THE EUROPEAN COMMISSION. Commission Recommendation on a European Electronic Health Record exchange format [*Internet*]. Vol. 4. 2019 [cited 2019 Mar 3]. p. 8. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0243&from=EN

59. Andersson M, Streit B, Wehnert J. Joint Action to support the eHealth Network. 2017; Available from: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20170509_co05_en.pdf

60. Paper W. A Case Study for Blockchain in Healthcare : " MedRec " prototype for electronic health records and medical research data. 2016;

61. Journal I, Engineeringcomputer O, Issn S, No P. Health Care Virtual Environment System Reinforced by Hadoop and Cloud. 2016;5(5):1–7.

62. Sobradillo P, Pozo F, Agustí Á. Medicina P4: el futuro a la vuelta de la esquina. Arch Bronconeumol. 2010;47(1):35–40.

63. Kumari P, Lopez-Benitez M, Lee GM, Kim TS, Minhas AS. Wearable *Internet* of Things - From human activity tracking to clinical integration. Proc Annu Int Conf IEEE Eng Med Biol Soc EMBS. 2017;2361–4.

64. Insight ARDII. "Cidadão Ciberseguro" quer certificar conhecimentos sobre cibersegurança [*Internet*]. Media Next Professional Information Lda. 2019 [cited 2019 Feb 15]. Available from: https://www.itinsight.pt/news/seguranca/cidadao-ciberseguro-quer-certificar-conhecimentos-sobre-ciberseguranca

65. FCC. Projeto-nau [*Internet*]. FCT - Unidade de Computação Científica Nacional. [cited 2019 Mar 1]. Available from: https://www.fccn.pt/projeto-nau/

66. Aivazpour Z, Rao VSC. Impulsivity and Risky Cybersecurity Behaviors : A Replication. Proc Am Conf Inf Syst. 2018;(2017):1–9.

67. Sibley C, Duckitt J. Big-five personality, social worldviews, and ideological attitudes: Further tests of a dual process cognitive-motivational model. J Soc Psychol. 2009;149(5):545–61.

68. College HM, Cooper J, College T. Gleitman, Gross, Reisberg 2011. Psychology 8th.

69. Egelman S, Peer E. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). Proc ACM CHI'15 Conf Hum Factors Comput Syst [*Internet*]. 2015;1:2873–82. Available from: http://dx.doi.org/10.1145/2702123.2702249

70. ENISA. The new users ' guide : [*Internet*]. Information Security. 2010. Available from: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide

71. Öłütçü G, Testik ÖM, Chouseinoglou O. Analysis of personal information security behavior and awareness. Comput Secur. 2016;56:83–93.

72. Hadlington L. The "Human Factor" in Cybersecurity. In: Psychological and Behavioral Examinations in Cyber Security [*Internet*]. 2018. p. 46–63. Available from: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-4053-3.ch003

73. Statistics L. Cronbach's Alpha (α) using SPSS Statistics [*Internet*]. [cited 2019 Jan 23]. Available from: https://statistics.laerd.com/spss-tutorials/cronbachs-alpha-using-spss-statistics.php

74. Pimenta F, Leal I, Maroco J. Adaptação e estudo da escala de valor da saúde. Psicol Saúde Doenças [*Internet*]. 2009;10(2):217–25. Available from: http://www.scielo.oces.mctes.pt/scielo.php?pid=S1645-00862009000200006&script=sci_arttext

75. Vida CN de É para as C da. Integridade na Investigação Científica Recomendação [*Internet*]. Vol. 2, CNECV. Lisboa; 2018. Available from: http://www.cnecv.pt/admin/files/data/docs/1523888172_IntegridadeCNECV2018.pdf

76. Beaton DE, Bombardier C, Guillemin F, Ferraz MB. Guidelines for the process of cross-cultural adaptation of self-report measures. Spine (Phila Pa 1976) [*Internet*]. 2000 Dec 15;25(24):3186–91. Available from: https://pdfs.semanticscholar.org/3c7e/9d70a7062ba8dd018f22cb8cef8182b09432.pdf

77. Beaton, Dorcas; Bombardier, Claire; Guillemin, Francis; Ferraz MB. Recommendations for the Cross-Cultural Adaptation of the DASH & QuickDASH Outcome Measures. Inst Work Heal [*Internet*]. 2007;(August 2014):1–45. Available from: http://www.dash.iwh.on.ca/system/files/X-CulturalAdaptation-2007.pdf

78. Maroco J, Garcia-Marques T. Qual a fiabilidade do alfa de Cronbach? Questões antigas e soluções modernas? Laboratório Psicol [*Internet*]. 2013 Nov 17;4(1):65–90. Available from: http://publicacoes.ispa.pt/index.php/lp/article/viewFile/763/706.

9 Apêndices

9.1 Consentimento informado, esclarecido e livre.

CONSENTIMENTO INFORMADO, ESCLARECIDO E LIVRE PARA PARTICIPAÇÃO EM ESTUDOS DE INVESTIGAÇÃO.

Por favor, leia com atenção a seguinte informação. Se achar que algo está incorreto ou que não está claro, não hesite em solicitar mais informações.

Título do estudo: Cultura em Cibersegurança dos profissionais da Saúde em ambiente hospitalar

Enquadramento: Atitudes e comportamentos em cibersegurança ambiente empresarial

Explicação do estudo: A preocupações diárias dos profissionais de saúde são tratar as pessoas doentes, em custos, normas, regulamentos e procedimentos. Será que a segurança do doente diferente da cibersegurança em SIS? A perspetiva de cuidar do doente ao nível físico e psíquico também envolve a proteção e os cuidados com os seus dados pessoais, também numa perspetiva holística onde tudo se relaciona desde dos processos aos fármacos e a sua privacidade.

É importante que utilizador tenha conhecimento suficientes para evitar cliques em *links* em e-mails sem verificar o URL e utilizar de equipamentos de armazenamento em dispositivos sensíveis em especial no sector da saúde, onde a existe uma proliferação de equipamentos conectados *IoT*, biossensores e aplicações de registos eletrónicos interligadas em rede, uma panóplia de tecnologias mais as dezenas de smartphones conectados e com capacidade de explorar vulnerabilidades. A importância da quantificação das atitudes e comportamentos em ambiente empresarial dos profissionais da saúde é uma ferramenta importante para determinar a necessidade de formação na temática e despertar uma consciência coletiva essencial para a gestão de risco e para a segurança do doente e simultaneamente para o saudável funcionamento e reputação da instituição de saúde onde se inserem.

Condições e financiamento: Não existem condições especiais ou financiamento envolvido no desenvolvimento deste estudo.

Questionário: As respostas a estes questionários *online* são anónimas. O sistema não irá armazenar informação que permita associar as respostas a quem as enviou. Por esta razão, depois de concluir os questionários propostos, não poderá voltar a consultá-lo ou alterar as suas respostas. Obrigado pela sua participação.

Confidencialidade e anonimato: O autor deste estudo respeita e assegura o cumprimento das regras decorrentes da entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia.

Os dados recolhidos são anónimos, confidenciais, tratados informaticamente e armazenados em bases de dados específicas para o efeito.

Assume-se o compromisso de oferecer serviços de qualidade a todos os destinatários (partes interessadas).

O questionário tem como finalidade a recolha de informação que permita a investigação em cibersegurança na saúde e a mitigação dos riscos visem a melhoria contínua da qualidade dos serviços prestados e a resiliência.

Por favor, colabore

Informação Recolhida: idade, género e grupo profissional que será relacionada com a *Awareness* em cibersegurança.

Concorda com a proposta que lhe foi feita? SIM 

Contacto:

Paulo Lopes Nunes

Telemóvel: 936203247

E-mail: 6490@alunos.estesl.ipl.pt

9.2 Autorização do Autor

Gmail — Paulo Lopes Nunes <pmrsln@gmail.com>

[Redir: 6490@alunos.estesl.ipl.pt] Re: Request authorization.
1 mensagem

Lee Hadlington <lhadlington@dmu.ac.uk> 18 de fevereiro de 2019 às 10:21
Para: "6490@alunos.estesl.ipl.pt" <6490@alunos.estesl.ipl.pt>

Dear Paulo

I am more than happy for you to use these scales, and thank you for asking ! I would be interested in hearing about the results for the study as well - there is perhaps a better set of scales you could use for this, is it engagement in cybersecurity that you are interested in ?
Best

Lee

> On 7 Feb 2019, at 10:49, 6490@alunos.estesl.ipl.pt wrote:
>
> Good morning Professor Lee Hadlington.
>
> My name is Paulo Lopes Nunes, I'm a student in the Escola Superior de Tecnologia da Saúde de Lisboa (Lisbon School of Health Technology) - ESTeSL a public school, integrated into the Polytechnic Institute of Lisbon (IPL).
> Currently finishing the master`s in health technology Assessment. I would like to develop my thesis in the area of Cybersecurity in healthcare, specifically the cybersecurity-related to healthcare professionals.
> In this sense, I would like to request the Professor authorization to develop the translation and validation for Portuguese of the RSCB and ATC-IB scale for the health sector, as an important assessment tool for cybersecurity engagement and awareness.
>
> Sincerely,
>
> Paulo Nunes
>

9.3 Comissão de Ética CHBM

CHBM Centro Hospitalar Barreiro Montijo EPE

Concordo.
Ao CA
26/09/2018

Luís dos Santos Pinheiro
Diretor Clínico

Apreciado em Reunião do Conselho de Administração CHBM, E.P.E. de 28/09/2018 ACTA N.º 39

C.A. Autorizado

Pedro Lopes
Presidente do Conselho de Administração

Memorando // Nota interna n.º: **35/2018** Data: 21 / 09 / 2018

De: **Comissão de Ética para a Saúde**

Para: **Dr. Luís dos Santos Pinheiro – Director Clínico e Vogal Executivo do Conselho de Administração**

Assunto: **Estudo clínico para mestrado**

A 21/09/2018 reuniu a Comissão de Ética do Centro Hospitalar Barreiro Montijo, E.P.E. que analisou um pedido de autorização para aplicação de um questionário aos profissionais de saúde do Centro Hospitalar Barreiro Montijo, E.P.E., no âmbito de um trabalho intitulado "Cibersegurança em saúde: Avaliação das atitudes e comportamentos de cibersegurança dos profissionais da saúde em ambiente hospitalar" a realizar por Paulo Manuel Roque da Silva Lopes Nunes, técnico de análises clínicas e saúde pública no Serviço de Patologia Clínica deste Centro Hospitalar e aluno de mestrado da Escola Superior de Tecnologia da Saúde de Lisboa. Na documentação anexa ao pedido foram juntos o projecto com o questionário, curriculum vitae do proponente e da orientadora, e declaração de consentimento informado a utilizar no estudo. Através do preenchimento de um inquérito via on-line este estudo observacional quantitativo e transversal tem como objectivo primário avaliar as atitudes e comportamentos para a cibersegurança dos profissionais de saúde, em ambiente hospitalar. A Comissão de Ética delibera por unanimidade no sentido de nada ter a opor à realização deste estudo.

CEF
Dá-se conhecimento do parecer ao Requerente
3.10.2018.

(Elvira Camacho, Dr.ª)
(Presidente da CES)

1.10.2018

ENTRADA
Conselho de Administração
N.º 12529 24/09/2018
M Malato

9.4 Autorização ClaraSaúde

Autorização

A 12/10/2018 reuniu da Direção dos Grupo Clarasaúde que analisou um pedido de autorização para aplicação de um questionário aos profissionais que compõem o grupo, no âmbito de um trabalho intitulado "Cibersegurança em saúde: Avaliação das atitudes e comportamentos de cibersegurança dos profissionais da saúde em ambiente hospitalar" a realizar por Paulo Manuel Roque da Silva Lopes Nunes, técnico de análises clínicas e saúde pública e aluno de Mestrado GATS da Escola Superior de Tecnologia da Saúde de Lisboa.

Na documentação anexa ao pedido foram juntos o projeto com o questionário, curriculum vitae do proponente e da orientadora, e declaração de consentimento informado a utilizar no estudo. Através do preenchimento de um inquérito via on-line este estudo observacional quantitativo e transversal.

Por nada ter a opor à realização deste estudo, foi autorizado.

ClaraSaúde, Lda.
NIPC:508565146

(Carlos Clara, Dr.)

(CEO Clarasaúde)

9.5 Questionários Originais

Table 1. Scale Items for the Risky Cybersecurity Behaviours Scale (RScB).

	Item
1	Sharing passwords with friends and colleagues.
2	Using or creating passwords that are not very complicated (e.g. family name and date of birth).
3	Using the same password for multiple websites.
4	Using online storage systems to exchange and keep personal or sensitive information.
5	Entering payment information on websites that have no clear security information/certification
6	Using free-to-access public Wi-Fi
7	Relying on a trusted friend or colleague to advise you on aspects of online-security.
8	Downloading free anti-virus software from an unknown source.
9	Disabling the anti-virus on my work computer so that I can download information from websites.
10	Bringing in my own USB to work in order to transfer data onto it.
11*	Checking that software for your smartphone/tablet/laptop/PC is up-to-date.
12	Downloading digital media (music, films, games) from unlicensed sources
13	Sharing my current location on social media.
14	Accepting friend requests on social media because you recognise the photo.
15	Clicking on links contained in unsolicited emails from an unknown source.
16	Sending personal information to strangers over the Internet.
17	Clicking on links contained in an email from a trusted friend or work colleague.
18*	Checking for updates to any anti-virus software you have installed.
19	Downloading data and material from websites on my work computer without checking its authenticity.
20	Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop)

* Indicates reverse scored items.

Table 2. Scale items for the Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB).

	Item
1	I think that management have the responsibility to ensure a company is protected from cybercrime
2*	I am aware of my role in keeping the company protected from potential cybercriminals.
3	I believe everyone in the company has a role to play in protecting against threats from cybercriminals.
4	It is hard to know how I can help protect the organisation from cybercrime.
5	I don't have the right skills to be able to protect the organisation from cybercrime.
6	I do not feel that IT security is a priority within my organisation.
7	Computer systems provide all the protection a company needs.
8	I think that reporting cybercrime is a waste of time.
9	The Police lack the capacity to deal with cybercrime effectively.
10	I believe that cybercriminals are more advanced than the people who are supposed to be protecting us.
11	I think that information provided by the Government and Police on cybercrime is not relevant to businesses.^
12	I feel that the Police are far too busy to deal with cybercrime.^
13	I worry that if I report a cyberattack to the Police it might damage the reputation of the company
14*	I think more could be done to communicate the risks from cybercrime to individuals in the organisation.
15*	I am aware of the company's IT use policy and attempt to follow it.
16	I would not know how to report a cyberattack if one happened.
17	I don't think that reporting a cyberattack on the company is my responsibility.
18	I don't pay attention to company material about the threats from cybercrime.
19*	I am confident that I would be able to spot the signs of a cyberattack.
20*	I think the biggest threat for IT systems comes from people within the company.
21*	I feel that any individual within the company are at risk of manipulation from confidence tricksters.
22	I think that cybercriminals only target a company when there is a substantial financial gain.
23	I believe only large companies are targeted by hackers and cybercriminals.
24	I feel that only companies that take payments using online systems are at risk of being victims of cybercrime.^
25	I don't think I know who is responsible for protecting the company from cybercrime.

^Indicates items that were omitted from the final scale due to poor inter-item correlation.

* Indicates items that were reversed scored.

9.6 Questionários tradutora oficial-*RScB*

NOTÁRIA
Paloma Rito

NOTARIADO PORTUGUÊS

CARTÓRIO NOTARIAL DE PALOMA RITO

Rua José Saramago, Lote 26, R/C Esq.

Pinhal Novo - Palmela

NOTÁRIA PALOMA RITO

_____Certifico que, na data de hoje, em Pinhal Novo, concelho de Palmela, no Cartório Notarial de Paloma Rito, sito na Rua José Saramago Lote 26, r/c Esq, perante mim, **Noelma Tatiana da Silva Sebastião**, colaboradora do referido Cartório, devidamente autorizada pela Notária, Paloma da Paz Costa Lavrador Rito nos termos do Art.º 8º do DL 26/2004, de 4/02, com a nova redação dada pelo DL n.º 15/2011, de 25 de Janeiro, autorização essa publicada no site da Ordem dos Notários em 08/01/2018 com o n.º de registo 317/7, compareceu como outorgante: _____

_____**Maria Cristina Mestre Silvestre**, casada, natural da freguesia de Relíquias, concelho da Odemira, residente na Rua de Angola, n.º 20, R/C Esquerdo, Pinhal Novo, Palmela, cuja identidade verifiquei pela exibição do cartão de cidadão n.º 05658353 2 ZY5, válido até 02/03/2028 emitido pela República Portuguesa, a qual me declarou, sob compromisso de honra, que a tradução para a língua Portuguesa do documento em anexo escrito em língua inglesa, que é uma mera ***FOTOCÓPIA NÃO CERTIFICADA COM MERO VALOR DE INFORMAÇÃO*** ***da tabela 1 emitido através da página http://dx.doi.org/10.1016/j.heliyon.2017.e00346,*** reproduz fiel e corretamente o original anexo – **que é uma mera fotocópia** - tradução essa pela qual me declarou assumir inteira e completa responsabilidade. _____

_____Pinhal Novo, onze de março de dois mil e dezanove. _____

A Tradutora:

_____

(*Maria Cristina Mestre Silvestre*)

Rua José Saramago, n.º 26, r/c esquerdo, 2955-027 Pinhal Novo, Palmela,
email: info@cn-pinhalnovo.com Telf.: 212360666 Fax:212360667, Telemóvel:918596255

NOTÁRIA
Paloma Rito

A colaboradora:

(*Noelma Tatiana da Silva Sebastião*)

Conta registada sob o nº 82 Fatura nº 33308

Table 1. Scale Items for the Risky Cybersecurity Behaviours Scale (RScB).

	Item
1	Sharing passwords with friends and colleagues.
2	Using or creating passwords that are not very complicated (e.g. family name and date of birth).
3	Using the same password for multiple websites.
4	Using online storage systems to exchange and keep personal or sensitive information.
5	Entering payment information on websites that have no clear security information/certification
6	Using free-to-access public Wi-Fi
7	Relying on a trusted friend or colleague to advise you on aspects of online-security.
8	Downloading free anti-virus software from an unknown source.
9	Disabling the anti-virus on my work computer so that I can download information from websites.
10	Bringing in my own USB to work in order to transfer data onto it.
11*	Checking that software for your smartphone/tablet/laptop/PC is up-to-date.
12	Downloading digital media (music, films, games) from unlicensed sources
13	Sharing my current location on social media.
14	Accepting friend requests on social media because you recognise the photo.
15	Clicking on links contained in unsolicited emails from an unknown source.
16	Sending personal information to strangers over the Internet.
17	Clicking on links contained in an email from a trusted friend or work colleague.
18*	Checking for updates to any anti-virus software you have installed.
19	Downloading data and material from websites on my work computer without checking its authenticity.
20	Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop)

*Indicates reverse scored items.

Tabela 1: Itens para a Escala de Comportamentos de Cibersegurança Arriscados (Risky Cybersecurity Behaviours Scale, RScB em inglês)

	Item
1	Partilhar palavras-passe com amigos e colegas.
2	Usar ou criar palavras-passe pouco complicadas (por ex., apelido e data de nascimento).
3	Usar a mesma palavra-passe para sites diferentes.
4	Usar sistemas de armazenagem online para partilhar ou guardar informação pessoal e sensível.
5	Inserir informação de pagamento em sites que não têm informação/certificação de segurança clara
6	Usar Wi-Fi de livre acesso público
7	Confiar num amigo ou colega próximo para conselhos em aspectos de segurança online.
8	Descarregar anti-vírus gratuito de uma fonte desconhecida.
9	Desactivar o anti-vírus no meu computador de trabalho para que possa descarregar informação de sites.
10	Trazer a minha própria pen para o trabalho a fim de transferir informação para ela.
11*	Verificar que o software do meu smartphone/tablet/portátil/PC está actualizado.
12	Descarregar conteúdos digitais (música, filmes, jogos) de fontes não-licenciadas
13	Partilhar a minha localização actual em redes sociais.
14	Aceitar solicitações de amizade em redes sociais porque reconheço a foto.
15	Carregar em links de emails não solicitados de uma fonte desconhecida.
16	Enviar informação pessoal a estranhos pela Internet.
17	Carregar em links de emails de amigos próximos ou de um colega de trabalho.
18*	Procurar actualizações para qualquer anti-vírus que tenha instalado.
19	Descarregar informação e material de sites para o meu computador de trabalho sem verificar a sua autenticidade.
20	Guardar informação da empresa no meu dispositivo electrónico pessoal (por ex., smartphone/tablet/portátil)

* Indica itens com pontuação inversa.

1 http://dx.doi.org/10.1016/j.heliyon.2017.e00346

A tradutora

9.7 Questionários Tradutora oficial *ATC-IB*

NOTÁRIA
Paloma Rito

NOTARIADO PORTUGUÊS

CARTÓRIO NOTARIAL DE PALOMA RITO

Rua José Saramago, Lote 26, R/C Esq.

Pinhal Novo - Palmela

NOTÁRIA PALOMA RITO

_____Certifico que, na data de hoje, em Pinhal Novo, concelho de Palmela, no Cartório Notarial de Paloma Rito, sito na Rua José Saramago Lote 26, r/c Esq, perante mim, **Noelma Tatiana da Silva Sebastião**, colaboradora do referido Cartório, devidamente autorizada pela Notária, Paloma da Paz Costa Lavrador Rito nos termos do Art.º 8º do DL 26/2004, de 4/02, com a nova redação dada pelo DL n.º 15/2011, de 25 de Janeiro, autorização essa publicada no site da Ordem dos Notários em 08/01/2018 com o n.º de registo 317/7, compareceu como outorgante: _____

_____**Maria Cristina Mestre Silvestre**, casada, natural da freguesia de Relíquias, concelho da Odemira, residente na Rua de Angola, n.º 20, R/C Esquerdo, Pinhal Novo, Palmela, cuja identidade verifiquei pela exibição do cartão de cidadão n.º 05658353 2 ZY5, válido até 02/03/2028 emitido pela República Portuguesa, a qual me declarou, sob compromisso de honra, que a tradução para a língua Portuguesa do documento em anexo escrito em língua inglesa, que é uma mera ***FOTOCÓPIA NÃO CERTIFICADA COM MERO VALOR DE INFORMAÇÃO*** ***da tabela 2 emitido através da página http://dx.doi.org/10.1016/j.heliyon.2017.e00346,*** reproduz fiel e corretamente o original anexo – **que é uma mera fotocópia** - tradução essa pela qual me declarou assumir inteira e completa responsabilidade. _____

_____Pinhal Novo, onze de março de dois mil e dezanove. _____

A Tradutora:

_____

(*Maria Cristina Mestre Silvestre*)

Rua José Saramago, n.º 26, r/c esquerdo, 2955-027 Pinhal Novo, Palmela,
email: info@cn-pinhalnovo.com Telf.: 212360666 Fax:212360667, Telemóvel:918596255

NOTÁRIA
Paloma Rito

A colaboradora:

(*Noelma Tatiana da Silva Sebastião*)

Conta registada sob o nº 83 Fatura n.º 32308/8

Rua José Saramago, n.º 26, r/c esquerdo, 2955-027 Pinhal Novo, Palmela,
email: info@cn-pinhalnovo.com Telf.: 212360666 Fax:212360667, Telemóvel:918596255

Table 2. Scale items for the Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB).

	Item
1	I think that management have the responsibility to ensure a company is protected from cybercrime
2*	I am aware of my role in keeping the company protected from potential cybercriminals.
3	I believe everyone in the company has a role to play in protecting against threats from cybercriminals.
4	It is hard to know how I can help protect the organisation from cybercrime.
5	I don't have the right skills to be able to protect the organisation from cybercrime.
6	I do not feel that IT security is a priority within my organisation.
7	Computer systems provide all the protection a company needs.
8	I think that reporting cybercrime is a waste of time.
9	The Police lack the capacity to deal with cybercrime effectively.
10	I believe that cybercriminals are more advanced than the people who are supposed to be protecting us.
11	I think that information provided by the Government and Police on cybercrime is not relevant to businesses.^
12	I feel that the Police are far too busy to deal with cybercrime.^
13	I worry that if I report a cyberattack to the Police it might damage the reputation of the company
14*	I think more could be done to communicate the risks from cybercrime to individuals in the organisation.
15*	I am aware of the company's IT use policy and attempt to follow it.
16	I would not know how to report a cyberattack if one happened.
17	I don't think that reporting a cyberattack on the company is my responsibility.
18	I don't pay attention to company material about the threats from cybercrime.
19*	I am confident that I would be able to spot the signs of a cyberattack.
20*	I think the biggest threat for IT systems comes from people within the company.
21*	I feel that any individual within the company are at risk of manipulation from confidence tricksters.
22	I think that cybercriminals only target a company when there is a substantial financial gain.
23	I believe only large companies are targeted by hackers and cybercriminals.
24	I feel that only companies that take payments using online systems are at risk of being victims of cybercrime.^
25	I don't think I know who is responsible for protecting the company from cybercrime.

^Indicates items that were omitted from the final scale due to poor inter-item correlation.
* Indicates items that were reversed scor

http://dx.doi.org/10.1016/j.heliyon.2017.e00346

Tabela 2: Itens do Questionário sobre Atitudes em Relação à Cibersegurança e Cibercrime (Attitudes towards Cybersecurity and Cybercrime Questionnaire, ATC-IB em inglês)

	Item
1	Penso que a administração tem a responsabilidade de assegurar que a empresa esteja protegida de cibercrime
2*	Estou ciente do meu papel em manter a companhia protegida de potenciais cibercriminosos.
3	Penso que todos na empresa têm um papel a desempenhar na protecção contra ameaças de cibercriminosos.
4	É difícil saber como posso proteger a organização do cibercrime.
5	Não tenho as competências necessárias para proteger a organização do cibercrime.
6	Não creio que a segurança informática seja uma prioridade na minha organização.
7	Os sistemas de computador oferecem toda a protecção que uma companhia precisa.
8	Creio que denunciar cibercrimes é uma perda de tempo.
9	A Polícia não tem meios para combater o cibercrime de forma eficaz.
10	Creio que os cibercriminosos são mais avançados do que as pessoas que nos deviam proteger.
11	Penso que a informação do Governo e da Polícia em relação ao cibercrime não tem importância para as empresas.^
12	Penso que a Polícia está demasiado ocupada para se preocupar com o cibercrime.^
13	Receio que, se denunciar um ciberataque à Polícia, isso vá prejudicar a reputação da empresa
14*	Penso que deve ser feito mais para comunicar os riscos de cibercrime às pessoas na organização.
15*	Estou a par da política de uso informático da empresa, e tento segui-la.
16	Se ocorrer um ciberataque, não saberei como denunciá-lo.
17	Não acho que é da minha responsabilidade denunciar um ciberataque contra a empresa.
18	Não presto atenção ao material da empresa sobre ameaças de cibercrime.
19*	Confio na minha capacidade de reconhecer sinais de um ciberataque.
20*	Penso que a maior ameaça para os sistemas informáticos vem de pessoas de dentro da empresa.
21*	Sinto que qualquer pessoa na empresa está em risco de manipulação por vigaristas.
22	Penso que os cibercriminosos apenas atingem uma empresa quando têm muito a ganhar do ponto de vista financeiro.
23	Penso que apenas as grandes empresas são atingidas por hackers e cibercriminosos.
24	Penso que apenas empresas que recebem pagamentos por sistemas online estão em risco de serem vítimas de cibercrime.^
25	Acho que não sei quem é responsável por proteger a companhia do cibercrime.

^Indica itens que foram omitidos na escala final devido a uma pobre correlação inter-itens.
* Indica itens que tiveram a pontuação inversa

http://dx.doi.org/10.1016/j.heliyon.2017.e00346

A tradutora

9.8 Questionários traduzidos

Questionários

Scale Items for the Risky Cybersecurity Behaviours Scale (RScB).

1 Compartilhando senhas com amigos e colegas.

2 Usar ou criar senhas que não sejam muito complicadas (por exemplo, nome de família e data de nascimento).

3 Usando a mesma senha para vários sites.

4 Utilizar sistemas de armazenamento online para trocar e manter informações pessoais ou confidenciais.

5 Inserindo informações de pagamento em sites que não possuem informações / certificação de segurança claras

6 Usando Wi-Fi público de acesso gratuito

7 Confiar em um amigo ou colega de confiança para aconselhá-lo sobre aspetos da segurança on-line.

8 Download de software antivírus gratuito de uma fonte desconhecida.

9 Desativando o antivírus no meu computador de trabalho para que eu possa baixar informações de sites.

10 Trazendo meu próprio USB para trabalhar para transferir dados para ele.

11 * Verificar se o software do seu smartphone / tablet / laptop / PC está atualizado.

12 Download de mídia digital (músicas, filmes, jogos) de fontes não licenciadas

13 Compartilhando minha localização atual nas mídias sociais.

14 Aceitar solicitações de amizade nas mídias sociais porque você reconhece a foto.

15 Clicando nos links contidos em emails não solicitados de uma fonte desconhecida.

16 Envio de informações pessoais a estranhos pela Internet.

17 Clicar nos links contidos em um email de um amigo ou colega de trabalho confiável.

18 * Verificando atualizações de qualquer software antivírus que tenha instalado.

19 Download de dados e materiais de sites no meu computador de trabalho sem verificar sua autenticidade.

20 Armazenar informações da empresa no meu dispositivo eletrônico pessoal (por exemplo, smartphone / tablet / laptop)

Scale items for the Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB).

1 Acho que a Administração tem a responsabilidade de garantir que uma empresa seja protegida contra cibercrime

2 * Estou ciente do meu papel em manter a empresa protegida contra potenciais cibercriminosos.

3 Acredito que todos na empresa têm um papel a desempenhar na proteção contra ameaças de criminosos cibernéticos.

4 É difícil saber como posso ajudar a proteger a organização contra o cibercrime.

5 Não tenho as habilidades certas para poder proteger a organização do cibercrime.

6 Não sinto que a segurança de TI seja uma prioridade dentro da minha organização.

7 Sistemas de computador fornecem toda a proteção que uma empresa precisa.

8 Eu acho que denunciar o cibercrime é uma perda de tempo.

9 A polícia não tem capacidade para lidar eficazmente com o cibercrime.

10 Eu acredito que os cibercriminosos são mais avançados do que as pessoas que deveriam estar nos protegendo.

11 Eu acho que as informações fornecidas pelo governo e pela polícia sobre cibercrime não são relevantes para as empresas.

12 Eu sinto que a polícia está ocupada demais para lidar com o cibercrime.

Preocupa-me que, se eu denunciar um ciberataque à Polícia, possa prejudicar a reputação da empresa

14 * Acho que mais poderia ser feito para comunicar os riscos do cibercrime aos indivíduos da organização.

15 * Estou ciente da política de uso de TI da empresa e tento acompanhá-la.

16 Eu não saberia como denunciar um ataque cibernético se um acontecesse.

17 Não acho que denunciar um ataque cibernético à empresa seja minha responsabilidade.

18 Eu não presto atenção ao material da empresa sobre as ameaças do cibercrime.

19 * Estou confiante de que conseguiria identificar os sinais de um ataque cibernético.

20 * Acho que a maior ameaça para os sistemas de TI vem de pessoas dentro da empresa.

21 * Eu sinto que qualquer indivíduo dentro da empresa está em risco de manipulação de trapaceiros de confiança.

22 Eu acho que os cibercriminosos só visam uma empresa quando há um ganho financeiro substancial.

23 Acredito que apenas grandes empresas são alvo de hackers e cibercriminosos.

24 Eu sinto que apenas empresas que aceitam pagamentos usando sistemas on-line correm o risco de serem vítimas de cibercrime.

25 Eu não acho que sei quem é responsável por proteger a empresa do cibercrime.

9.9 Questionários Retraduzidos

Questionnaires

Scale Items for the Risky Cybersecurity Behaviours Scale (RScB).

1 Sharing passwords with friends and colleagues.

2 Use or create passwords that are not too complicated (e.g. family name and date of birth).

3 Using the same password for multiple sites.

4 Use online storage systems to exchange and keep personal or confidential information.

5 Entering payment information on sites that do not have clear security information / certification.

6 Using public Wi-Fi for free access

7 Trust a trusted friend or colleague to advise you on aspects of online safety.

8 Download free antivirus software from an unknown source.

9 Disabling antivirus software on my work computer so that I can download information from websites.

10 Bringing my own USB to work to transfer data to it.

11 Check if your smartphone / tablet / laptop / PC software is up-to-date.

12 Download digital media (music, movies, games) from unlicensed sources

13 Sharing my current location on social media.

14 Accept friend requests on social media because you recognize the photo.

15 Clicking on links contained in unsolicited email from an unknown source.

16 Sending personal information to strangers over the Internet.

17 Clicking on the links contained in an email from a trusted friend or co-worker.

18 Checking for updates to any antivirus software you have installed.

19 Downloading data and materials from websites to my work computer without verifying their authenticity.

20 Store company information on my personal electronic device (e.g. smartphone / tablet / laptop).

Scale items for the Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB).

1 I think Management has a responsibility to ensure that a company is protected against cybercrime.

2 I am aware of my role in keeping the company safe from potential cybercriminals.

3 I believe that everyone in the company has a role to play in protecting against threats from cybercriminals.

4 It's hard to know how I can help protect the organization from cybercrime.

5 I don't have the right skills to protect the organization from cybercrime.

6 I don't feel that IT security is a priority within my organization.

7 Computer systems provide all the protection an organization needs.

8 I think reporting cybercrime is a waste of time.

9 Police do not have the capacity to deal effectively with cybercrime.

10 I believe cybercriminals are more advanced than the people who should be protecting us.

11 I think the information provided by government and police about cybercrime is not relevant to business.

12 I feel that the police are too busy to deal with cybercrime.

I am concerned that if I report a cyberattack to the police, it could damage the company's reputation.

14 I think more could be done to communicate the risks of cybercrime to individuals in the organization.

15 I am aware of the company's IT use policy and try to follow it.

16 I wouldn't know how to report a ~~cyber attack~~ if one happened.

17 I don't think reporting a cyberattack to the company is my responsibility.

18 I don't pay attention to the company's material on cybercrime threats.

19 I am confident that I could identify the signs of a cyberattack.

20 I think the biggest threat to IT systems comes from people within the organization.

~~21 I~~ feel that any individual within the company is at risk of manipulation by trusted scammers.

22 I think cybercriminals only target a company when there is a substantial financial gain.

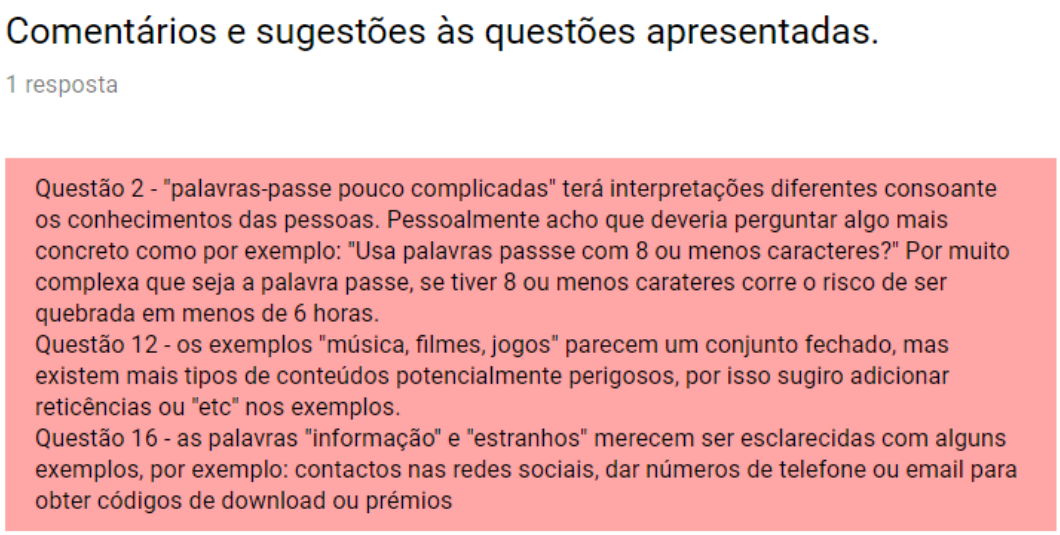
23 I believe that only large companies are targeted by hackers and cybercriminals.

24 I feel that only companies that accept payments using online systems are at risk of falling victim to cybercrime.

25 I don't think I know who is responsible for protecting the company from cybercrime.

9.10 Painel de peritos

Comentários dos peritos de IPLeiria



Comentários e sugestões às questões apresentadas.

1 resposta

Questão 2 - "palavras-passe pouco complicadas" terá interpretações diferentes consoante os conhecimentos das pessoas. Pessoalmente acho que deveria perguntar algo mais concreto como por exemplo: "Usa palavras passse com 8 ou menos caracteres?" Por muito complexa que seja a palavra passe, se tiver 8 ou menos carateres corre o risco de ser quebrada em menos de 6 horas.
Questão 12 - os exemplos "música, filmes, jogos" parecem um conjunto fechado, mas existem mais tipos de conteúdos potencialmente perigosos, por isso sugiro adicionar reticências ou "etc" nos exemplos.
Questão 16 - as palavras "informação" e "estranhos" merecem ser esclarecidas com alguns exemplos, por exemplo: contactos nas redes sociais, dar números de telefone ou email para obter códigos de download ou prémios

Comentários.

2 respostas

Algumas perguntas levarão, porventura, aos inquiridos a responder de forma a não se "incriminar". Exemplos:

2 - Usa ou cria palavras-passe pouco complicadas, por exemplo (apelido, data de nascimento, 1234).

==> a tendência é o utilizador responder que não, dado o termo "pouco complicadas". A pergunta não poderia ser ao contrário?

"Usa ou cria palavras-passe complexas, com oito ou mais caracteres, não usando apelidos, datas de nascimento ou sequências do género 123456

(iria é fugir ao inquérito original)

4 - Usa sistemas de armazenamento online para partilhar ou guardar informação pessoal e sensível.
==> (dar exemplos: google Drive? Dropbox? etc.)

5 - Insere informação de pagamento em websites que não têm informação/certificação de segurança explícita.
=> "certificação de segurança explícita". Será plenamente entendida pelos destinatários?

5 - Insere informação de pagamento em websites que não têm informação/certificação de segurança explícita.
=> "certificação de segurança explícita". Será plenamente entendida pelos destinatários?

7 - Confia num amigo ou colega próximo para conselhos em aspetos de segurança online.
E se o amigo for um informático? :)

Continuação de bom trabalho.

No geral o questionário parece bem traduzido e estruturado. No entanto, existem conceitos básicos para um informático que podem ser mal interpretados por pessoas de outras áreas. Por isso as perguntas devem ser o mais objetivas possível.

O perito/data

3 respostas

P. (não costumo partilhar dados online)

Miguel Frade

P

9.11 Questionário Definitivo aplicado.

Cibersegurança dos profissionais de saúde em ambiente hospitalar

Enquadramento

O presente estudo científico é realizado no âmbito do Mestrado em Gestão e Avaliação de Tecnologias em Saúde (GATS) lecionado pela Escola Superior de Tecnologia da Saúde de Lisboa (ESTEsL) integrada no Instituto Politécnico de Lisboa (IPL), com do Instituto Politécnico de Leiria (IPLeiria), com o objetivo de quantificar a percepção em cibersegurança e cibercrime através da avaliação das atitudes e dos comportamentos dos profissionais nos SIS em ambiente hospitalar. Validação para português e adaptação à área da saúde dos questionários sobre os Comportamentos arriscados em Cibersegurança *Risky cybersecurity behaviours scale (RScB)* e o de Atitudes em Relação à Cibersegurança e Cibercrime em empresas *Attitudes towards cybersecurity and cybercrime* in business' (*ATC-IB*) validadas por *Lee Hadlington* (2017) baseados no trabalho de *Serge Egelman* e *Eyal Peer* (2015) para o desenvolvimento de uma escala de medição da segurança, intenções e comportamentos.

Informação Recolhida:

Idade, género e grupo profissional.

Confidencialidade e anonimato:

O autor deste estudo respeita e assegura o cumprimento das regras decorrentes da entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia.

Os dados recolhidos são anónimos, confidenciais, tratados informaticamente e armazenados em bases de dados específicas para o efeito.

O sistema não irá armazenar informação que permita associar as respostas a quem as enviou. Por esta razão, depois de concluir os questionários propostos, não poderá voltar a consultá-los ou alterar as suas respostas.

Se achar que algo está incorreto ou que não está suficientemente claro, não

hesite em solicitar mais informações para:

6490@alunos.estesl.ipl.pt

Concorda em participar no estudo? *

- ◯ sim
- ◯ não

Dados Pessoais

Idade (Anos) *

Sexo *

- ◯ Feminino
- ◯ Masculino

Grupo profissional *

- ◯ Dirigente Superior
- ◯ Técnico Superior
- ◯ Informático
- ◯ Assistente Técnico, Técnico de nível intermédio, Pessoal Administrativo,
- ◯ Assistente Operacional
- ◯ Médico
- ◯ Enfermeiro
- ◯ Técnico Superior de Diagnóstico e Terapêutica
- ◯ Técnico Superior de Saúde
- ◯ Outras
- ◯ Questionário sobre os comportamentos de risco em Cibersegurança (*RScB*)

É fundamental que responda às questões de forma honesta para que a classificação obtida traduza efetivamente as suas atitudes e os seus comportamentos reais na utilização dos sistemas e tecnologias de informação e comunicação.

A sua opinião é uma ferramenta essencial para a avaliação do nível de consciencialização dos profissionais na instituição de saúde, relativamente à adoção de boas práticas de cibersegurança.

Seleccione a opção que melhor se adapta à frequência com que nos últimos 6 meses:

0- Nunca; 1 - 1 a 2 vezes por semestre; 2 -1 a 2 vezes por trimestre; 3 - 1 a 2 vezes por mês; 4 - 1 a 2 vezes por quinzena; 5 - 1 a 2 vezes por semana; 6 - Diariamente

1- Partilha palavras-passe com colegas *

	0	1	2	3	4	5	6	
Nunca	◯	◯	◯	◯	◯	◯	◯	Diariamente

2- Usa ou cria palavras-passe pouco complicadas (ex: data de nascimento, apelido, etc..) *

	0	1	2	3	4	5	6	
Nunca	◯	◯	◯	◯	◯	◯	◯	

3-Usa a mesma palavra-passe para diferentes websites.

	0	1	2	3	4	5	6	
Nunca	◯	◯	◯	◯	◯	◯	◯	Diariamente

4- Usa sistemas de armazenamento *online* para partilhar ou guardar informação pessoal e sensível(google drive, dropbox, onedrive, etc..). *

	0	1	2	3	4	5	6	
Nunca	◯	◯	◯	◯	◯	◯	◯	Diariamente

5 - Insere informação de pagamento em websites sem a informação/certificação de segurança explícita. *

	0	1	2	3	4	5	6	
Nunca	◯	◯	◯	◯	◯	◯	◯	Diariamente

6-Usa Wi-Fi de livre acesso público. *

0	1	2	3	4	5	6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

7-Confia num amigo ou colega próximo para conselhos em aspetos de segurança *online*. *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

8-Descarrega antivírus gratuitos de fontes desconhecidas. *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

9-Desativa o antivírus do computador de trabalho para que possa descarregar informação de websites. *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

10-Utiliza a pen drive pessoal com a finalidade de transferir informação nos computadores da instituição.

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯

11- Verifica regularmente as actualizações de *software* do smartphone/tablet/portátil/PC.. *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

12- Descarrega conteúdos digitais (música, filmes, jogos, etc...) de fontes não fidedignas. *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

13-Partilha a sua localização nas redes sociais. (Fotos, local de trabalho...) *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

14- Aceita solicitações de amizade em redes sociais porque reconhece fotos. *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

15- Carrega em *links* de *email* não solicitados de uma fonte desconhecida. *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

16- Envia informação pessoal a estranhos pela *Internet* (contactos nas redes sociais, dá números de telefone ou *email* para obter códigos de download ou prémios, etc..) .* *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

17-Carrega em *links* de *email* enviados por amigos próximos ou de colegas de trabalho. *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

18-Verifica atualizações para quaisquer antivírus que tenha instalado. *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯

19- Descarrega informação e material de websites para o computador de trabalho sem a preocupação da sua autenticidade. *

0 1 2 3 4 5 6

Nunca ◯ ◯ ◯ ◯ ◯ ◯ ◯ Diariamente

20-Guarda informação da empresa no dispositivo eletrónico pessoal (por ex., smartphone/tablet/portátil) *

	0	1	2	3	4	5	6	
Nunca	◯	◯	◯	◯	◯	◯	◯	Diariamente

Questionário sobre Atitudes em Relação à Cibersegurança e Cibercrime em empresas (ATC-

IB)

É fundamental que responda às questões de forma honesta para que a classificação obtida traduza efetivamente as suas atitudes e os seus comportamentos reais na utilização dos sistemas e tecnologias de informação e comunicação.

A sua opinião é uma ferramenta essencial para a avaliação do nível de consciencialização dos profissionais na instituição de saúde, relativamente à adoção de boas práticas de cibersegurança.

Seleccione a opção que melhor se adapta à sua experiência nos últimos 6 meses

1- Penso que a administração tem a responsabilidade de assegurar que a instituição de saúde esteja protegida contra o cibercrime. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

2- Estou ciente do meu papel em manter a instituição protegida de potenciais ciberameaças *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

3- Penso que todos na instituição têm um papel a desempenhar na proteção contra as ciberameaças. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente

4- É difícil saber como posso proteger a instituição do cibercrime. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente

5- Não tenho as competências necessárias para proteger a instituição do cibercrime. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente

6- Não creio que a segurança informática seja uma prioridade na minha instituição. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente

7-Os sistemas de informação oferecem toda a proteção que uma instituição necessita. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente

8- Creio que denunciar o cibercrime é uma perda de tempo. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente

9- A Autoridade não tem meios para combater o cibercrime de forma eficaz *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

10- Creio que os *hackers* e cibercriminosos são mais talentosos do que as pessoas que nos deviam proteger. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

11- Os boletins informativos governamentais em relação ao cibercrime não são relevantes para a instituição de saúde. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

12- A Autoridade está demasiado ocupada para se preocupar com o cibercrime. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

13- Receio que, se denunciar um ciberataque à Autoridade, isso vá prejudicar a minha reputação interna. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

14- Penso que deverá ser feito mais para comunicar os riscos do cibercrime aos profissionais. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

15- Estou a par da política de uso informático da instituição de saúde, e tento manter-me atualizado *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

16- Se ocorrer um ciberataque, não saberei como denunciá-lo. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

17- Não acho que é minha responsabilidade denunciar um ciberataque contra a instituição de saúde. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

18- Não presto atenção ao material informativo da instituição sobre ameaças de cibercrime. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

19- Confio na minha capacidade de reconhecer sinais de um ciberataque. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

20- Penso que a maior ameaça para os sistemas informáticos vem de pessoas de dentro da instituição de saúde. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

21- Sinto que qualquer pessoa da organização está em risco de manipulação por ciber "vigaristas e burlões" *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

22- Penso que os cibercriminosos e *hackers* apenas atingem uma instituição de saúde quando têm muito a ganhar do ponto de vista financeiro. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

23- Apenas as grandes empresas e organizações são alvo dos *hackers* e cibercriminosos. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

24- Apenas as instituições de saúde que recebem pagamentos por sistemas *online* estão em risco de serem vítimas de um ciberataque. *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

25- Não sei quem é o responsável por proteger a instituição de saúde das ciberameaças *

◯ Concordo totalmente.

◯ Concordo.

◯ Discordo.

◯ Discordo totalmente

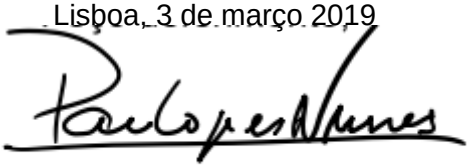
» Redirection to final page of *Online* Pesquisa (alterar)

9.12 Declaração da inexistência de conflito de Interesses

Declaração da inexistência de conflito de interesses

Eu, Paulo Manuel Roque da Silva Lopes Nunes licenciado em Análises Clínicas e Saúde Pública pela Escola Superior de Tecnologia da Saúde de Lisboa (ESTeSL), com o Cartão de Cidadão nº 09039273 6ZY2, válido até 03/06/2019, atualmente a frequentar o Mestrado em Gestão e Avaliação de Tecnologias em Saúde, na Escola Superior de Tecnologias da Saúde de Lisboa (ESTeSL) do Instituto Politécnico de Lisboa, em parceria com a Escola Superior de Saúde da Universidade do Algarve (UALG ESS), declaro a inexistência de potenciais conflitos de interesse na realização da Dissertação de Mestrado, com o título provisório "**Avaliação das atitudes e comportamentos de cibersegurança dos profissionais da saúde em ambiente hospitalar**".

Lisboa, 3 de março 2019



Paulo Lopes Nunes