POLITÉCNICO DE SANTARÉM
UIIPS – IMPACT SCIENCE

11 - 1 | 2023

CIBERSEGURANÇA: A PERSPETIVA DOS PROFISSIONAIS DE SAÚDE

Cibersecurity: A healthcare professional's perpective

Cecília Teresa Pinto | Diogo Bessa | Sónia Merciano | Ana Narra | Ana Pereira | Mario Silva | Filipe Madeira

Versão eletrónica
URL: https://revistas.rcaap.pt/uiips/
ISSN: 2182-9608
Data de publicação: 18-07-2023 Páginas: 14

Editor
Revista UI_IPSantarém

Referência eletrónica
Pinto, C.; Bessa, D.; Marciano, S.; Narra, A.; Pereira, A.; Silva, M.; Madeira, F.; (2023). Cibersegurança na perspetiva dos profissionais de saúde do artigo. *Revista da UI_IPSantarém. 11*(1), e27712. https://doi.org/10.25746/ruiips.v11.i1.27712

revistauiips@ipsantarem.pt
Complexo Andaluz,
Apartado 279
2001-904 Santarém

Revista da UI_IPSantarém – Unidade de Investigação do Instituto Politécnico de Santarém,
Vol. 11, N. º 1, 2023, e27712, Santarém
ISSN: 2182-9608
https://revistas.rcaap.pt/uiips/

CIBERSEGURANÇA NA PERSPETIVA DOS PROFISSIONAIS DE SAÚDE

Cibersecurity: A healthcare professional's perspective

Cecília Teresa Pinto
Instituto Politécnico de Santarém, Portugal
10100398@esg.ipsantarem.pt

Diogo Bessa
Instituto Politécnico de Santarém, Portugal
210100396@esg.ipsantarem.pt

Sónia Merciano
Instituto Politécnico de Santarém, Portugal
210100043@esg.ipsantarem.pt

Ana Narra
Instituto Politécnico de Santarém, Portugal
210100047@esg.ipsantarem.pt

Ana Pereira
Instituto Politécnico de Santarém, Portugal
210100054@esg.ipsantarem.pt

Mário Silva
Instituto Politécnico de Santarém, Portugal
mario.silva@essaude.ipsantarem.pt | 0000-0002-2434-4356 | 6115-2632-EFBE

Filipe Madeira
CIAC/ Pólo de Literacia Digital e Inclusão Social, Instituto Politécnico de Santarém, Portugal
filipe.madeira@esg.ipsantarem.pt | 0000-0002-2227-7006 | DE1F-7FEE-FBA5

RESUMO

Este estudo tem como principal objetivo perceber a capacitação dos profissionais de saúde em relação à cibersegurança e prevenção de ciberataques nas instituições onde estes exercem funções. O estudo consiste em aplicar uma escala de resposta tipo *Likert* previamente validada e publicada, para avaliar as atitudes em relação à cibersegurança em ambiente empresarial (*ATC-IB*), com o objetivo de obter dados sobre diversos indicadores como a cibersegurança e a gestão de risco de ciberataques na perspetiva dos profissionais de saúde, o questionário foi submetido através da plataforma digital Google Forms®, a distribuição do questionário foi *online* em redes sociais e grupos do *WhatsApp* que exercem a sua profissão no setor público, privado e social em Portugal. Trata-se de um estudo observacional, quantitativo, transversal e descritivo sobre atitudes em relação à cibersegurança nos seus locais de trabalho. Foi criada uma base de dados em programa *Microsoft Office Excel* ® e para a análise estatística descritiva e exploratória dos dados foi usado a linguagem de programação R e o *plug-in EZR*. Na amostra em estudo foram incluídos 82 profissionais de saúde e foram excluídos 8 por uma questão estatística. Respondentes por género: 76% mulheres e 24% homens. Divididos por 4 grupos profissionais: enfermeiros; médicos; técnicos superiores de diagnóstico e terapêutica (TSDT); e gestores. A média de idades é de 38,12 anos com um desvio padrão de 12.38. A área de abrangência situa-se maioritariamente na região de Lisboa e Vale do Tejo com representação de 94,4%; a região norte com 4,4% e a região do Alentejo com 1,1% de respondentes. 72% exercem funções no setor público; 25% no setor privado; e 3% no setor social. Grau académico e habilitações literárias está distribuído por: 2% é doutorado; 32% possui o grau de mestre; 60% é licenciado. Conclui-se que existem algumas diferenças ao nível de conhecimento de cibersegurança, nomeadamente na faixa etária 18-30 anos e as restantes idades, tal como entre géneros no mesmo item (de não saber a quem recorrer se existisse um ciberataque), esta dificuldade apresenta-se mais evidente em idades acima dos 31 anos e no género feminino. E ainda entre géneros acresce-se uma diferença estatisticamente significativa no item (de ganhar do ponto de vista financeiro com os ciberataques), conclui-se que o género feminino tem a perceção de que o dinheiro não é apenas e único fator motivador dos ciberataques. Entre classes profissionais verificou-se diferenças entre os enfermeiros e os TSDT para 1 item, os enfermeiros dão mais importância aos boletins informativos governamentais em relação ao cibercrime que os TSDT; e um item entre enfermeiros e gestores, sendo que os gestores têm mais conhecimento sobre quem é o responsável por proteger a instituição de saúde das ciberameaças, que os enfermeiros. Globalmente a escala *ATC-IB* nas três variáveis (géneros, faixas etárias e classes profissionais) não foram encontradas grandes diferenças, de um modo geral existe capacitação dos profissionais de saúde em relação à cibersegurança e prevenção de ciberataques no contexto ambiente de trabalho.

Palavras-chave: Cibersegurança, profissionais de saúde, ciberataque, capacitação

ABSTRACT

The present study aimed is to understand the training of health professionals in relation to cybersecurity and cyberattack prevention in the institutions where they work. The study consists of applying a previously validated and published Likert-type response scale to assess attitudes towards cybersecurity in a business environment (ATC-IB), with the purpose of obtaining data on several indicators such as cybersecurity and risk management of cyberattacks from the perspective of health professionals. This is an observational, quantitative, cross-sectional, and descriptive study on attitudes towards cybersecurity in their workplaces. A database was created in Microsoft Office Excel ® program and for descriptive and exploratory statistical analysis of the data, the R programming language and the EZR plug-in were used. In the sample under study 82 health professionals were included and 8 were excluded for a statistical question. Respondents by gender: 76% women and 24% men. Divided into 4 professional groups: nurses; physicians; senior technicians of diagnosis and therapy (TSDT); and managers. The average age is 38.12 years with a standard deviation of

12.38. The area covered is mostly located in the Lisbon and Tagus Valley region, with 94.4% of respondents; the Northern region with 4.4%, and the Alentejo region with 1.1% of respondents. 72% work in the public sector; 25% in the private sector; and 3% in the social sector. Academic degree and academic qualifications are distributed as follows: 2% have a PhD; 32% have a Master's degree; 60% have a degree. We conclude that there are some differences in terms of knowledge of cybersecurity, namely in the 18-30 age group and the remaining age groups, as well as between genders in the same item (not knowing who to turn to if there is a cyberattack). This difficulty is more evident in age groups over 31 and in the female gender. Also between genders, there is a statistically significant difference in the item (gaining from the financial point of view with cyberattacks), concluding that the female gender has the perception that money is not the only motivating factor of cyberattacks. Between professional classes, differences were found between nurses and SDWTs for one item: nurses give more importance to governmental newsletters regarding cybercrime than SDWTs; and one item between nurses and managers: managers have more knowledge about who is responsible for protecting the health institution from cyber threats than nurses. Overall the ATC-IB scale in the three variables (gender, age groups and professional classes) no major differences were found, in general there is training of health professionals in relation to cybersecurity and prevention of cyberattacks in the context of work environment.

Keywords: Cibersecurity, professional's healthcare, cyberattack, empowerment.

1 INTRODUÇÃO

Com a rápida digitalização dos processos nas organizações de saúde, principalmente nos últimos dois anos devido às restrições impostas pela pandemia COVID-19, a par com o aumento dos ciberataques nestas instituições, tornou-se emergente desenvolver estratégias ao nível da cibersegurança, para mitigar os danos económicos e intangíveis que estes tipos de ataques podem causar.

Estudo tem como principal objetivo perceber o *empowerment* dos profissionais de saúde em relação à cibersegurança e prevenção de ciberataques nas instituições onde estes exercem funções.

O conceito *empowerment* nas organizações, significa dar poder, motivação, capacitação e liderança aos trabalhadores para que eles desempenhem as suas funções com responsabilidade, eficiência e eficácia aumentando assim a sua autonomia, autoconfiança e motivação (Pinto, 2018).

Segundo a Organização Mundial de Saúde (2006), *empowerment* "pode ser um processo social, cultural, psicológico ou apresentar suas preocupações, conceber estratégias para envolvimento na tomada de decisões e alcançar ações políticas, sociais e culturais para atender a essas necessidades".

É preciso ter em conta que promover o *empowerment* dos profissionais de saúde faz sentido quando existe uma aposta na educação na saúde e na literacia digital, na formação e informação de todos os profissionais; sobretudo os que têm maior dificuldade, reforçando a ideia de que a inclusão digital deixou de ser apenas o uso de sistemas de informação é também a forma como a usamos e quais são as consequências do seu uso inconscientemente (Baashar et al., 2020; Cremer el al., 2022; Nifakos et al., 2021). Para que haja capacitação de todos os profissionais de saúde importa conceder essa autonomia o que implica investir na própria cibersegurança das instituições.

Importa compreender estes conceitos de tecnologia de informação, digitalização e de cibersegurança e como se relacionam entre si. As Tecnologias de Informação (TI's) e a digitalização, ou seja, a passagem dos dados físicos para o meio digital são processos que têm evoluído ao longo dos últimos anos nas instituições prestadoras de cuidados de saúde com mais expressão atualmente (Cremer et al., 2022; Nunes et al., 2021).

A transformação digital e a cibersegurança são duas dimensões que convergem entre si e exigem uma adaptação da cultura das organizações a par de uma estratégia interventiva. Se a produtividade dos profissionais for resultado do acesso constante a aplicações de *software* e introdução de dados, então a área de cibersegurança deve ser incorporada em todos os aspetos. É preciso assegurar que o acesso aos dados é feito de forma segura, independentemente do dispositivo ou localização de quem acede e que haja visibilidade sobre o que está a acontecer. É importante que todos entendam os fundamentos da cibersegurança em toda a sua dimensão, pois só assim será possível garantir que esta estará totalmente alinhada com a estratégia de gestão de risco cibernético (Bradley et al., 2020; Cremer et al., 2022; Gunasekeran et al., 2021; Moustafa et al., 2021; Nifakos et al., 2021)

A cibersegurança consiste "no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem" (Centro Nacional de Cibersegurança Portugal [CNCS], 2020).

Por ciberameaça é definido pelo CNCS (2020) "Ciberameaça [ameaça]: "potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização", no âmbito do ciberespaço, (ISO/IEC 27032). É de salientar e de acordo com o Relatório Riscos & Conflitos do CNCS (2022), os tipos de ciberameaças mais relevantes em Portugal continuam a ser o *phishing* (é uma técnica de fraude *online* em que os cibercriminosos roubam informações pessoais); *ransomware* (é um software que bloqueia o computador); e a fraude/burla *online*. As organizações ao implementar programas de cibersegurança como medida preventiva podem se proteger ativamente deste tipo de ameaças.

Ao longo do tempo tem havido um esforço tanto a nível internacional como a nível nacional para criar políticas, diretrizes, normas e institutos numa tentativa de promover a prevenção dos mais diversos ataques informáticos (ciberataques) com o desenvolvimento de estruturas que dificultam este tipo de ataques, tais como o uso de *firewalls* (*software* que protege o computador da entrada e instalação de *software* maliciosos); outros tipos de estratégias é a alteração de *passwords* várias vezes por ano a formação dos profissionais de saúde em tecnologias de informação e segurança. Contudo, não são suficientes, pois os ciberataques continuam a acontecer, sendo o fator humano a maior barreira encontrada para a existência desta insegurança (Nifakos et al., 2021). Os colaboradores ao acederem a *links phishing* inocentemente, dão oportunidade a *hackers* (cibercriminosos) de copiarem dados sensíveis ou instalarem *Malware* (*software* que provoca danos), tornando assim, as instituições vulneráveis aos ciberataques (King et al., 2018; Moustafa et al., 2021; Nifakos et al., 2021; Nunes et al., 2021).

Para combater o risco cibernético, é necessário capacitar todos os *stakeholders* das organizações prestadoras de cuidados de saúde através de formação obrigatória e contínua de todo o espectro da segurança cibernética (ciberhigiene) e, assim, mitigar estes riscos (Cremer et al., 2022; Nifakos et al., 2021; Nunes et al., 2021).

A estrutura deste artigo será a seguinte: apresentação do problema de investigação, constante nesta secção; na secção seguinte apresenta-se a metodologia usada para desenvolver este trabalho; na terceira secção são apresentados os resultados do estudo; na penúltima secção é feita uma breve discussão e por fim, apresentam-se as principais conclusões e limitações resultantes deste trabalho de investigação.

2 MÉTODOS

2.1. Tipo de estudo

Trata-se de um estudo, observacional, quantitativo, transversal e descritivo sobre atitudes em relação à cibersegurança em instituições prestadoras de cuidados de saúde em Portugal.

A amostra é probabilística e enviesada, pois não é representativa de todos os profissionais de saúde existentes no país. Uma vez que os respondentes (94.5%) pertencem à região de Lisboa e Vale do

Tejo, 4,4% dos respondentes pertencem à região norte e 1,1% à região alentejana. A escolha das instituições de saúde foi realizada de forma probabilística.

O estudo centre-se em perceber a capacitação dos profissionais de saúde em relação à cibersegurança e prevenção de ciberataques. As métricas obtidas pela escala são comparadas com as métricas sociodemográficas e o grupo profissional, nomeadamente grupos etários, classes profissionais e género. Deste modo, foi formulada o seguinte objetivo geral: "Será que os profissionais de saúde possuem o conhecimento necessário para a prevenção de ciberataques na instituição onde exercem funções?", nesse sentido foi definido o seguinte objetivo específico: O género, a idade e a classe profissional é um fator de diferenciação em relação à literacia em cibersegurança

Tendo em consideração a questão de investigação e uma vez fundamentada na introdução e inserida no desenho de estudo, tornou-se essencial definir e caracterizar a população alvo, bem como estabelecer os critérios de seleção. Neste sentido, a unidade de análise para este estudo foram gestores e profissionais na área da saúde que estejam no ativo. O que determinou o número de inquiridos foi a disponibilidade dos profissionais para responder ao questionário no período em que decorreu o estudo.

2.2. Questionário sobre atitudes em relação à cibersegurança (*ATC-IB*)

A estrutura do questionário é constituída por dois grupos: a primeira parte consiste em questões sociodemográficas e a segunda é referente à escala *ATC-IB* - "*Attitudes towards cybersecurity and cybercrime in business*" (Hadlington, 2017) com 25 perguntas referentes à cibersegurança.

O questionário *ATC-IB* é composto por 25 itens, sendo estes avaliados segundo uma escala tipo *Likert* de 4 pontos assumindo valores de 1 a 4 correspondendo respetivamente a 1 = Discordo totalmente; 2 = Discordo; 3 = Concordo e 4 = Concordo totalmente. As perguntas 2, 14, 15, 19, 20 e 21, têm uma pontuação inversa (Hadlington, 2017). A soma das respostas tem um score que varia entre 25 e 100 pontos, sendo que uma pontuação mais baixa significa um fraco *engagement* e uma fraca consciência com o tema da cibersegurança e uma pontuação mais alta significa um forte *engagement* e uma forte consciência com o tema da cibersegurança (Hadlington, 2017).

2.3. Recursos digitais

O questionário foi disponibilizado durante um período de 10 dias, em junho de 2022, através de plataforma digital *Google Forms*® e foi divulgado através de redes sociais e grupos *WhatsApp*® entre gestores e profissionais na área da saúde que estão no ativo.

2.4. Métodos estatísticos

Para a análise dos dados recorreu-se à estatística descritiva e exploratória para comparação de grupos independentes, de maneira a determinar se as diferenças entre eles são estatisticamente significativas (teste *Welch* e *Kruskal-Wallis*). Para verificação dos pressupostos de normalidade aplicaram-se os testes de *ShapiroWilk*. Foram usados o programa *Microsoft Office Excel*® e a linguagem de programação R (R *Core Team*, 2022) e o *plug-in* EZR (Kanda, Y., 2013). Relativamente à análise dos dados considerou-se o nível de significância de 5%.

A análise da consistência interna da escala foi calculada pelo investigador Nunes P., (2019) quando validou a mesma para a versão portuguesa: teve como resultado para índice alfa de *Cronbach*. de 0.72, fiabilidade apropriada para o estudo. Com um nível de significância de 5%

2.5. Procedimentos éticos e de confidencialidade

A recolha de dados respeita e assegura o cumprimento das regras do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia. Os dados recolhidos são anónimos, confidenciais, tratados informaticamente e armazenados em bases de dados específicas para o efeito. A participação no estudo foi voluntária e sujeita a aceitação dos propostos estabelecidos no consentimento informado. 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. A comissão de ética consultada respondeu decidir por unanimidade não haver cabimento a pronunciar-se sobre a emissão de um parecer

favorável ou desfavorável nos moldes que lhe compete e, desse modo, dar sentido favorável ao prosseguimento com o referido questionário.

3 RESULTADOS

3.1 Análise estatística de dados sociodemográficos

No decorrer do estudo, responderam ao questionário 90 profissionais na área da saúde. A amostra é constituída por 76% mulheres e 24% homens, divididos por 5 grupos profissionais: enfermeiros; médicos; técnicos superiores de diagnóstico e terapêutica (TSDT); gestores; e designação por "outras profissões na área de saúde: 1 assistente social, 1 psicólogo, 2 assistente dentista, 2 assistentes operacionais, 1 engenheiro informático, 1 farmacêutico" este último grupo foi excluído por motivos estatísticos, obtendo assim 82 respondentes. Em termos percentuais: enfermeiros (44%); TSDT (34%); médicos (11%); e gestores (11%).

A idade média dos respondentes incluídos no estudo é de 38,12 anos com um desvio padrão de 12.38. A mediana tem o valor de 36,38. Realizou-se a estratificação da variável idades de acordo com as seguintes faixas etárias: [18-30]; [31-45]; [46-60] e ≥ 60 anos, com a seguinte distribuição: n[18-30]=36%; n[31-45]=32%; n[46-60]=30% e ≥ 60= 2%.

A área de abrangência é maioritariamente da região de Lisboa e Vale do Tejo com 94,5% de respondentes, apenas 4,4% dos respondentes encontram-se na região norte e exercem funções em clínicas privadas e 1.1% dos respondentes pertence à região alentejana do país.

Grau académico: 2% possui o grau de doutorado; 32% mestrado; 60% licenciatura.

As instituições de saúde onde os respondentes exercem as suas funções, tem a seguinte distribuição: 64% dos respondentes exercem funções em unidades hospitalares; 19% em clínicas privadas (fisioterapia; hemodialise; hospitais privados; e em laboratórios de analises clínicas); 12% em unidades de cuidados de saúde primários e 5% em unidades de cuidados continuados. Os gestores representam 12% da amostra total e exercem funções nas diversas unidades de saúde acima referidas.

Distribuição de respondentes por setor de atividade: 72% exercem funções no setor público; 25% no setor privado; e 3% no setor social. 51% dos profissionais de saúde respondentes têm mais de 15 anos de exercício profissional.

3.2 Análise estatística da escala *ATC-IB* com os dados sociodemográficos

Realizado *Shapiro-Wilh test* em relação varável faixa etária não se verifica normalidade na distribuição (SW=0.86, p-*value*=0.00). Em relação à variável género, verifica-se distribuição normal (SW=0.52, p-*value*=6.63) o mesmo não se verifica nas variáveis classes profissionais em que existe violação na distribuição da normal (SW=0.80, p-*value*=0.00).

Relativamente aos itens da *ATC-IB* entre faixas etárias, procedeu-se à exploração das diferenças estatísticas por item, na determinação de eventuais diferenças. Para o efeito, recorreu-se ao teste de *Kruskal-Wallis* para amostras Independentes para cada item da respetiva escala por faixa etária. Verifica-se que existe diferenças estatisticamente significativas entre faixas etárias no item da 16 - "Se ocorrer um ciberataque, não saberei como denunciá-lo", como mostra a tabela 1.

Tabela 1

Resultados estatisticamente significativos por itens e por faixa etária

Item	**Faixa etária / p-*value***	**X^2 (3)**	**p-*value***
16	18-30: 31-46 / p-*value*= 0.03	9.46	0.02
	18-30: 46-60 / p-value= 0.03		

Para comparar os valores mediana da escala *ATC-IB* entre o género masculino e feminino, aplicou-se o teste *Welch* para duas amostras independentes, uma vez que se verifica os pressupostos de

normalidade na distribuição, mas não se verifica homocedástica, ou seja, não há variância (*Bartlett's K-squared* = 24.81, df = 1, p-*value* = 0.00), recorrendo-se ao teste de *Welch*.

Procedeu-se à exploração das diferenças estatísticas por item da escala de atitudes, na determinação de eventuais diferenças, verifica-se que existe diferenças estatisticamente significativas entre género, no item da 16 - "Se ocorrer um ciberataque, não saberei como denunciá-lo" e no item 22 - "Penso que os cibercriminosos e *hackers* apenas atingem uma instituição de saúde quando têm muito a ganhar do ponto de vista financeiro", como mostra na tabela 2.

Tabela 2

Resultados estatisticamente significativos por itens e por género

Item	**Género**	**média**	**Desvio-padrão**	**T. *Welch***	**p-*value***
16	feminino	2.80	0.84	t=24.8 dt=1 p-*value*=0.00	0.02
	masculino	2.26	0.87		
22	feminino	2.41	0.76	t = -2.06, df = 23.31, p-*value* =0.04	0.04
	masculino	2.94	0.94		

Procedeu-se ainda à exploração das diferenças estatísticas por item da escala de atitudes, na determinação de eventuais diferenças entre classes profissionais. Para o efeito, recorreu-se ao teste de *Kruskal-Wallis* para amostras independentes para cada item da respetiva escala por grupo profissional, uma vez que não se verifica os pressupostos de distribuição normal na variável classes profissionais. Foram verificadas diferenças estatisticamente significativas nos valores medianos das pontuações entre as classes profissionais, nos seguintes itens: (11) "Os boletins informativos governamentais em relação ao cibercrime não são relevantes para a instituição de saúde onde colaboro"; (25) "Sei quem é o responsável por proteger a instituição de saúde (onde trabalho/colaboro) das ciberameaças", resultados apresentados na tabela 3.

Tabela 3

Resultados estatisticamente significativos por itens e por classe profissional

Item	**Classe Profissional / p-*value***	**X^2 (3)**	**p-*value***
11	Enfermeiro-TSDT / p-*value*= 0.04	7.54	0.04
25	Enfermeiro-Gestor / p-*value*= 0.01	10.80	0.01

A escala *ATC-IB* tem uma pontuação entre 25 a 100 pontos (soma das respostas por item), sendo que uma pontuação mais baixa significa um comportamento mais arriscado em relação ao tema cibersegurança e uma pontuação mais elevadas indicam uma forte consciência em cibersegurança. Os valores obtidos na amostra em estudo variaram entre 26 e 88 com uma média de 61,7 e com um desvio-padrão de 8.2. A média das pontuações da escala é de 62,5 pontos, os respondentes encontram-se dentro desse valor médio.

4 DISCUSSÃO 8

Foi realizada uma análise com o teste *Kruskal-Wallis* para comparar as medianas da escala entre as classes profissionais e entre faixas etárias e não foram encontradas diferenças significativas (X^2 (3) =5.44, p-*value*=0.14); para comparar as pontuações medianas de género da escala, foi utilizado um teste *Welch*, e também não foram encontradas diferenças significativas (t = -1.59, df = 30.33, p-*value* = 0.12). Tal é confirmado no estudo efetuado por Nunes et al., (2021) verificam que os itens da *ATC-IB* quanto às faixas etárias que não existem diferenças estatisticamente significativas. O

grau académico dos respondentes que no mínimo é a licenciatura também deverá ser um fator influenciador.

Foi também realizada uma análise individual de itens para comparar entre faixas etárias, entre grupos profissionais e entre o género.

Considerando as faixas etárias e género, foi encontrada diferença estatisticamente significativa no item 16 “Se ocorrer um ciberataque, não saberei como denunciá-lo” entre o intervalo de idades 18-30 e o intervalo entre os 31 aos 60 anos. Na faixa etária dos 18-30 anos (36% do total da amostra) 11% sabe como pode denunciar; dos 25% que não sabe como denunciar, 18% são do sexo feminino e 7% do sexo masculino. Na faixa etária dos 31-60 anos (68% dos respondentes encontram-se nesta faixa etária), 12% sabe como denunciar um cibercrime e 56% não sabe como denunciar, dos quais: 38% são mulheres e 18% são homens. Conclui-se que em ambas as faixas etárias são as mulheres que possuem menos informação sobre este item. Essas diferenças são mais evidentes na faixa etária dos 31-60 anos, com uma diferença de 20% entre sexos. Enquanto na faixa etária 18-30 anos a diferença entre géneros é de 11%.

Ao comparar as medianas para cada item em relação ao género, verificou-se que existem diferenças estatisticamente significativas no item 22 “Penso que os cibercriminosos e *hackers* apenas atingem uma instituição de saúde quando têm muito a ganhar do ponto de vista financeiro”. Do total da amostra 76% são do género feminino e destas: 63% discordam que os cibercriminosos apenas atingem a instituição quando ganham financeiramente, enquanto 5% concordam com esta afirmação. Dos 24% respondentes do sexo masculino: 16.4% concordam e 8.6.% discordam da afirmação. Conclui-se que o género feminino tem uma perceção de que o dinheiro não é apenas e único fator motivador dos ciberataques, também podem existir outros interesses como o roubo de dados pessoais e dados sensíveis dos doentes e com eles todos os riscos que lhes estão inerentes.

Considerando as diferenças entre classes profissionais foram encontradas diferenças estatisticamente significativas no item 11 “Os boletins informativos governamentais em relação ao cibercrime não são relevantes para a instituição de saúde onde colaboro”: da totalidade de enfermeiros respondentes 79% discordam e 21% concordam, que os boletins informativos não sejam uma mais valia nas instituições onde exercem a sua profissão, enquanto para o total dos TSDT 40% concordam e 60% discordam, ou seja existe uma diferença de 19% nas respostas entre as duas classes profissionais. Sendo os enfermeiros na sua maioria (quase 80%) que discordam desta afirmação. Enquanto, que os TSDT não apresentam valores tão discrepantes (60/40%) entre o discordo/concordo respetivamente.

No item 25 “Sei quem é o responsável por proteger a instituição de saúde (onde trabalho/colaboro) das ciberameaças” existe diferenças estatisticamente significativas entre a classe profissional de enfermagem e o gestor. 72% dos enfermeiros e 22% dos gestores não sabem quem é o responsável por proteger a organização; enquanto 78% dos gestores e apenas 28% dos enfermeiros sabe quem é o responsável. Este resultado poderá ser explicado uma vez que os enfermeiros estão ligados à parte assistencial, enquanto para os gestores, inerente ao exercício das suas funções têm um conhecimento mais abrangente dos órgãos e departamentos da instituição onde trabalham.

95% pensa qua é da obrigação das administrações serem responsáveis pela proteção da instituição contra o cibercrime. E 7% pensa que as instituições de saúde que recebem pagamentos por sistemas online é que estão em risco de serem vítimas de um ciberataque. 83% tem a noção que qualquer instituição pode ser vítima de um ciberataque independentemente do seu tamanho.

65% dos respondentes diz ter consciência do seu papel para manter a instituição protegida de potenciais ciberameaças e 93% pensa que todos têm um papel a desempenhar nessa proteção, contudo 60% pense que é difícil de saber como o pode fazer. E apenas 32% diz ter as competências necessárias.

93% acredita que deva denunciar um cibercrime e que tem essa responsabilidade, mas 54% não sabe como fazê-lo. 78% dá atenção devida à informação dada pela instituição sobre ameaças de cibercrime.

Quanto à escala *ATC-IB* e a sua pontuação entre 25 a 100 pontos, a amostra em estudo obteve uma média de 61,7 pontos com um desvio-padrão de 8.2. Indicando uma consciência mediana em

relação à cibersegurança. Não muito diferente da pontuação média do estudo de Nunes et al., (2021) que foi de 66.4 (+/- 6.3).

O fator humano é uma das maiores preocupações das organizações pois é indicado como o elo mais fraco no contexto da cibersegurança organizacional, por ser um alvo fácil de atingir pelos cibercriminosos e, por isso, a vítima mais comum dos ciberataques. (Gonçalves, 2019)

"Os profissionais de saúde são treinados e qualificados para prestar cuidados de saúde, muitas vezes sujeitos a altos níveis de *stress* devido à sobrecarga de trabalho e responsabilidades. Na sua rotina diária eles trabalham como uma equipa, (...) e há uma tendência natural de confiar naqueles ao seu redor", sendo prática comum nos hospitais "compartilhar um computador de mesa para uma equipa" (Nunes et al., 2021, p. 174). É de extrema relevância que todas as organizações se preocupem com a cibersegurança pois "os incidentes não discriminam organizações", ou seja, as vulnerabilidades são exploradas em organizações de grandes e pequenas dimensões, independentemente da indústria onde se inserem (Baptista, 2019; Proofprint, 2019).

Nesse sentido, apesar de as organizações de maior dimensão parecerem mais atraentes para os cibercriminosos, as organizações de menores dimensões acabam por ser mais lucrativas devido à falta de preparação que apresentam (Gonçalves; Proofprint, 2019). Deste modo, nos últimos anos registou-se um aumento constante de ataques contra organizações de pequenas dimensões (Gonçalves, 2019).

Nifakos et. al (2021) refere a necessidade de desenvolver estratégias para que os profissionais de saúde desempenhem um papel central na mitigação dos riscos cibernéticos.

5 CONCLUSÃO

Considerando a questão de investigação e os objetivos enunciadas, bem como a análise dos resultados, pode-se verificar que existem algumas diferenças ao nível de conhecimento de cibersegurança, nomeadamente na faixa etária 18-30 anos e as restantes idades, tal como entre géneros no mesmo item (de não saber a quem recorrer se existisse um ciberataque), sendo a dificuldade mais evidente em idades acima dos 31 anos e no género feminino. E ainda entre géneros, acresce-se uma diferença estatisticamente significativa no item de ganhar do ponto de vista financeiro com os ciberataques, conclui-se que o género feminino tem a perceção de que o dinheiro não é apenas e único fator motivador dos ciberataques. Entre classes profissionais verificou-se diferenças entre os enfermeiros e os TSDT para item "Os boletins informativos governamentais em relação ao cibercrime não são relevantes para a instituição de saúde onde colaboro" 79% dos enfermeiros discordam e 40% dos TSDT concordam com esta afirmação. Entre enfermeiros e gestores item "Sei quem é o responsável por proteger a instituição de saúde (onde trabalho/colaboro) das ciberameaças", 78% dos gestores sabe quem é o responsável e somente 28% dos enfermeiros diz saber quem é.
Globalmente a escala *ATC-IB* tanto para géneros, faixas etárias como entre classes profissionais não foram encontradas muitas diferenças, ou seja, de um modo geral existe capacitação dos profissionais de saúde em relação à cibersegurança e prevenção de ciberataques no contexto ambiente de trabalho. A formação de nível superior dos respondentes e a crescente preocupação e sensibilização com este tema no setor da saúde, poderá ser a justificação dos resultados obtidos. Mas ainda há muito a fazer nesta área, a implementação de formação contínua *on job* é imperativo para mitigar o risco de ciberataques futuros.

As limitações identificadas ao longo deste estudo prendem-se com o intervalo de tempo disponível para realização das várias etapas do estudo, o que conduziu a uma amostra de dimensão reduzida. A área geográfica dos inquiridos onde exercem a sua profissão foi maioritariamente na região Lisboa e vale do tejo, o que dificultou a sua extrapolação para a restante população nacional, uma vez que num universo de 58739 médicos e de 80238 enfermeiros existentes no país (INE, 2021). Não foi possível a recolha de dados em relação às outras profissões, pelas mesmas não se encontrarem disponíveis, por essa razão não foi possível realizar essa extrapolação.

Recomenda-se assim a realização de novos estudos na temática, no sentido de perceber quais as

estratégias que poderão ser implementadas para potenciar o *empowerment* dos profissionais de saúde em questões de cibersegurança.

6 REFERÊNCIAS

APA (2020). *The Publication Manual of the American Psychological Association, Seventh Edition is the official source for APA Style*. https://www.apastyle.org/

Baashar, Y., Hitham Alhussian, H., Patel, A., Alkawsi, G., Alzahrani, A. I., Alfarraj, O., & Hayder, G. (2020). *Customer relationship management systems (CRMS) in the healthcare environment: A systematic literature review*. PubMed. Retrieved Junho 22, 2022, from https://pubmed.ncbi.nlm.nih.gov/34170994/

Baptista, I. M. A. (2019). *Dissertação · Mestrado Bolonha em Segurança de Informação e Direito no Ciberespaço*. Dissertação · Mestrado Bolonha em Segurança de Informação e Direito no Ciberespaço. Retrieved Junho 27, 2022, from https://fenix.tecnico.ulisboa.pt/cursos/msidc/dissertacao/1409728525632070

Bradley, D. C., Maria, A. R., Cabello, I. R., Villanueva, G., Fønhus, M. S., Glenton, C., Glenton, C., Lewin, S., Henschke, N., Buckley, B. S., Melhl, G. L., Tamrat, T., & Shepperd, S. (2020). *Mobile technologies to support healthcare provider to healthcare provider communication and management of care*. PubMed. Retrieved Junho 20, 2022, from https://pubmed.ncbi.nlm.nih.gov/32813281/

Carmo, H., & Ferreira, M. M. (1998). *Metodologia da Investigação: guia para auto-aprendizagem*. Universidade Aberta.

CNCS: Centro Nacional de Cibersegurança Português. (2022). *Relatório Riscos e Conflitos em Cibersegurança*. Centro Nacional de Cibersegurança. Retrieved Junho 15, 2022, from https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs15m.pdf

CNCS: Centro Nacional de Cibersegurança Portugal. (2020). *CIBERSEGURANÇA EM PORTUGAL*. Centro Nacional de Cibersegurança. Retrieved Junho 30, 2022, from https://www.cncs.gov.pt/docs/relatorio-sociedade2020-observatoriociberseguranca-cncs-1.pdf

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Martin Mullins, M., Murphy, F., & Materne, S. (2022). *Cyber risk and cybersecurity: a systematic review of data availability*. PubMed. Retrieved Junho 21, 2022, from https://pubmed.ncbi.nlm.nih.gov/35194352/

Diário da República, 1.ª série. (2019). *Lei n.º 58/2019 Regulamento Geral sobre a Proteção de Dados – DGERT*. DGERT. Nº151 pág. 3. Retrieved Junho 21, 2022, from https://www.dgert.gov.pt/regulamento-geral-sobre-a-protecao-de-dados

Gonçalves, R. S. (2019). *Repositório da Universidade de Lisboa: O fator humano da cibersegurança nas organizações*. UTL Repository. Retrieved Junho 30, 2022, from https://www.repository.utl.pt/handle/10400.5/19248

Gunasekeran, D. V., Tseng, R. M. W. W. T., Tham, Y.-C. T., & Wong, T. Y. W. (2021). *Applications of digital health for public health responses to COVID-19: a systematic scoping review of artificial intelligence, telehealth and related technologies*. PubMed. Retrieved Junho 23, 2022, from https://pubmed.ncbi.nlm.nih.gov/33637833/ 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

Hadlington L., (2017). *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon*. 2017;3(7):e00346. http://dx.doi.org/10.1016/j.heliyon.2017.e00346

Hellemann, N. (2021). *SoSafe Cyber Security Awareness*. An Analysis of the European Cyberthreat Landscape. Retrieved Junho 30, 2022, from https://lp.sosafe.de/hubfs/SoSafe%20%20Human%20Risk%20Review%202021%20%20EN.pdf?__hstc=106398849.e258a00999b2355d7856ff3839bf88d0.1656070830516.1656070783

INE: Instituto Nacional de Estatística (2021). *Censos 2021 - Dados de saúde*. Disponível em https://www.ine.pt/xportal/xmain?xpgid=ine_tema&xpid=INE&tema_cod=1117

Kanda, Y., (2013). "*Investigation of the freely available easy.to.use software EZR for medical Statistics*." Bone Marrow Transplantation. https://www.nature.com/articles/bmt2012244.pdf.

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). *Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment*. NCBI. Retrieved Junho 21, 2022, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5807417/

Ministério da Saúde - Serviço Nacional Saúde. (2019). *Guia de Boas Práticas e Regras para sítios web SNS/MS CIBERSEGURANÇA*. SPMS. Retrieved Junho 25, 2022, from https://www.spms.min-saude.pt/wp-content/uploads/2019/11/Guia-de-Boas-Pra%CC%81ticas-e-Regras-para-sites.pdf

Moore, E. C., Tolley, C. L., Bates, D. W., & Slight, S. P. (2020). *A systematic review of the impact of health information technology on nurses' time*. PubMed. Retrieved Junho 23, 2022, from https://pubmed.ncbi.nlm.nih.gov/32159770/

Moustafa, A. A., Bello, A., & Maurushat, A. (2021, Junho 18). *The Role of User Behaviour in Improving Cyber Security Management*. PubMed. Retrieved June 20, 2022, from https://pubmed.ncbi.nlm.nih.gov/34220596/

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). *Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review*. PubMed. Retrieved Junho 18, 2022, from https://pubmed.ncbi.nlm.nih.gov/34372354/

Nunes, P., Antunes, M., & Sila, C. (2021). *Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions*. PDF. Retrieved Junho 21, 2022, from https://iconline.ipleiria.pt/handle/10400.8/6096

Pinto, M., (2018). *Empowerment: entenda o que é e como aplicar! Guia do empreenderdor*. Disponível em https://www.guiaempreendedor.com/guia/empowerment-entenda-o-que-e-e-como-aplicar

Proofpoint Report. (2019). *Human Factor Report*. gtd-pfpt-us-r-human-factor-2019_0.pdf. Retrieved Junho 21, 2022, from https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-r-human-factor-2019_0.pdf

R Core Team, (2022). *R: A languase and environment for statiscal computing. R Foundation for Statiscal Computing*, Vienna, Austria. URL https://www.R-project.org/.

World Health Organization. (2006). *What is the evidence on effectiveness of empowerment to improve health?* WHO/Europe. Retrieved Julho 2, 2022, from https://www.euro.who.int/__data/assets/pdf_file/0010/74656/E88086.pdf

7 ANEXOS

Questionário

Dados sociodemográficos

1. Tomei conhecimento da informação relativa ao objetivo do estudo, bem como à confidencialidade dos dados (incluindo a sua codificação) e à sua utilização exclusiva para trabalhos futuros de investigação aplicada.
2. Indique a sua idade
3. No presente, exerço funções ou cargos em entidades das áreas da saúde como gestor elou profissional de saúde
4. Indique o seu sexo
5. Indique o seu nível de escolaridade
6. Indique a sua nacionalidade (portuguesa, ...)
7. Indique o distrito onde trabalha (Santarém, ...)
8. Indique a localidade onde trabalha (Santarém, ...)
9. Indique a localidade onde reside (Santarém, ...)
10. Indique a sua profissão/cargo que exerce atualmente
11. Indique o número de anos na profissão de gestor e/ou profissional de saúde
12. Indique o número de anos em que está no cargo que ocupa atualmente
13. Indique a natureza de entidade da área da saúde onde trabalha
14. Indique o tipo da entidade da área da saúde onde trabalha Exos: estabelecimento hospitalar, agrupamento de centros de saúde, clínica, consultório, laboratório,
15. Indique o serviço onde trabalha

Indicadores sobre cibersegurança

1. Penso que a administração tem a responsabilidade de assegurar que a instituição de saúde esteja protegida contra o cibercrime
2. Estou ciente do meu papel em manter a instituição protegida de potenciais ciberameaças
3. Penso que todos na instituição têm um papel a desempenhar na proteção contra as ciberameaças
4. É difícil saber como posso proteger a instituição do cibercrime
5. Tenho as competências necessárias para proteger a instituição do cibercrime
6. A segurança informática é uma prioridade na minha instituição
7. Os sistemas de informação oferecem toda a proteção que uma instituição necessita
8. Creio que denunciar o cibercrime é uma perda de tempo
9. Autoridade Nacional em matéria de cibersegurança nacional (Centro Nacional de Cibersegurança - CNCS) não tem meios para combater o cibercrime de forma eficaz
10. Creio que os hackers e cibercriminosos são mais talentosos do que as pessoas que nos deviam proteger
11. Os boletins informativos governamentais em relação ao cibercrime não são relevantes para a instituição de saúde onde colaboro
12. O Centro Nacional de Cibersegurança - CNCS, está demasiado ocupado e não se preocupa devidamente com o cibercrime
13. Receio que, se denunciar um ciberataque ao Centro Nacional de Cibersegurança - CNCS, isso vá prejudicar a minha reputação interna
14. Penso que deverá ser feito mais para comunicar os riscos do cibercrime aos profissionais e gestores
15. Estou a par da política de uso informático da instituição de saúde, e tento manter-me atualizado
16. Se ocorrer um ciberataque, não saberei como denunciá-lo

17. É minha responsabilidade denunciar um ciberataque contra a instituição de saúde
18. Tenho atenção ao material informativo da instituição 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 instituição de saúde
21. Sinto que qualquer pessoa da organização está em risco de manipulação por ciber "vigaristas e burlões"
22. Penso que os cibercriminosos e *hackers* apenas atingem uma instituição de saúde quando têm muito a ganhar do ponto de vista financeiro
23. Apenas as grandes empresas e organizações são alvo dos *hackers* e cibercriminosos
24. Apenas as instituições de saúde que recebem pagamentos por sistemas online estão em risco de serem vítimas de um ciberataque
25. Sei quem é o responsável por proteger a instituição de saúde (onde trabalho/colaboro) das ciberameaças