Instituto Superior de Gestão e Administração de Santarém

Mestrado em Engenharia de Tecnologias e Sistemas Web

Dissertação

Cibersegurança numa unidade hospitalar

Artur Botas,

22108574

Santarém

Ano 2023/2024

Instituto Superior de Gestão e Administração de Santarém

Mestrado em Engenharia de Tecnologias e Sistemas Web

Dissertação

Cibersegurança numa unidade hospitalar

Artur Botas

22108574

Dissertação submetida para satisfação parcial dos requisitos do grau de Mestre em Engenharia de Tecnologias e Sistemas Web sob a orientação do Prof. Marco Tereso e Coorientação do Prof. Doutor Ricardo Ângelo Rosa Vardasca

Santarém

Ano 2023/2024

"Nunca abdicar dos sonhos, por mais difíceis que pareçam,

por mais cansado que esteja, nunca deixar de tentar!"

AGRADECIMENTOS

A Deus pela maravilhosa família que me deu, à compreensão da minha esposa e dos meus filhos pela minha ausência e indisponibilidade que manifestei durante estes últimos tempos, ao facto da minha mãe e avó poderem testemunhar mais esta conquista na minha vida e por toda a ajuda que me deram ao longo da mesma. Infelizmente nem o meu pai nem avô, os meus grande pilares e exemplos tiveram a oportunidade de testemunhar esta etapa, é a lei da vida, mas acredito que seria com imenso prazer que o fariam se ainda estivessem nesta dimensão e para mim uma imensa satisfação.

Ao meu orientador, Prof. Marco Tereso, pela paciência, disponibilidade, colaboração e pela visão crítica e oportuna.

Ao Prof. Doutor Ricardo Ângelo Rosa Vardasca pela disponibilidade, colaboração e a ambos pela simplicidade, genuinidade, assim como pelo apoio e incentivo durante este percurso, pelos conhecimentos e sabedoria transmitida, pelo exemplo e profissionalismo.

Ao meu chefe, Dr. Pedro Miguel Vieira Teixeira, pela amizade, sinceridade, colaboração, disponibilidade e companheirismo.

Eternamente grato pelo apoio e pelo crescimento que este percurso proporcionou na minha vida.

RESUMO

Sendo a cibersegurança, um tema de extrema importância para o bom funcionamento de qualquer instituição e uma vez que os ataques são cada vez mais frequentes, nomeadamente hospitalares, foram enviados alguns e-mails de alerta sobre segurança e posteriormente simulados alguns ataques phishing, para todos os utilizadores da instituição visada. Foram registados os acessos numa base de dados SQL, dos utilizadores que selecionaram o link e os que colocaram credencias. Por questões de segurança os dados foram anonimizados, inclusive a instituição, https://eur-lex.europa.eu/eli/reg/2016/679/oj. Novamente foi enviada informação por e-mail a dar conhecimento do efetuado e do número de utilizadores que expuseram credenciais, assim como identificados os pontos que deveriam ter sido reconhecidos como não seguros. Na segunda campanha de phishing, a simulação foi mais dissimulada, o que originou um número substancialmente maior de utilizadores a serem vítimas da mesma. O trabalho efetuado foi produtivo, uma vez que serviu para despertar os utilizadores e a própria instituição sobre as vulnerabilidades e suas consequências.

Embora os resultados tenham sido preocupantes, o objetivo foi atingido, estas simulações foram de extrema importância para sensibilizar e despertar os utilizadores para estas situações e evitar que sejam vítimas das mesmas.

Palavras chave: phishing; cibersegurança; segurança na web; malware; segurança de informação.

ABSTRACT

Since cybersecurity is an extremely important topic for the proper functioning of any institution and since attacks are increasingly frequent, particularly in hospitals, some security alert emails were sent and later some phishing attacks were simulated, for all the users. Accesses were recorded in an SQL database, of users who selected the link and those who placed credentials. For security and privacy reasons, the data were anonymized, including the institution. Again, information was sent by e-mail informing what had been done and the number of users who had exposed credentials, as well as identifying the points that should have been recognized as unsafe.

In the second phishing campaign, the simulation was more covert, which resulted in a substantially greater number of users falling victim to it. The work carried out was productive, as it served to awaken users and the institution itself about vulnerabilities and their consequences.

The results were concerning, the objective was achieved, these simulations were extremely important to raise awareness and awaken users to these situations and prevent them from becoming victims.

Keywords: phishing; cybersecurity; web security; malware; information security

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

ÍNDICE DE GRÁFICOS

Lista de abreviaturas e Acrónimos

ACES Agrupamento de Centros de Saúde

CA Conselho de Administração

GTI Gestão de Tecnologias de Informação

GCI Gabinete de Comunicação e Imagem

HL7 (Health Level Seven) que é um conjunto de padrões internacionais para a troca de informações clínicas e administrativas entre sistemas de saúde

RGPD Regulamento Geral de Proteção de Dados

SB SmartBusiness – software de implementação de questionários e registos de dados (Techera)

SQL "Structured Query Language", ou "Linguagem de Consulta Estruturada"

SNS Serviço Nacional de Saúde

1. Introdução

Este trabalho foi realizado num hospital público, composto por diversos departamentos e serviços, como por exemplo, urgência, internamento, cirurgia, ortopedia, radiologia, patologia clínica laboratorial, anatomia patológica, consulta externa, psiquiatria, departamento da mulher e da criança, cuidados paliativos e domiciliários, entre outros. É gerido por um CA, com o auxílio de administradores hospitalares, diretores de departamento, serviço, coordenadores, chefias e vários colaboradores, cumprindo padrões rigorosos de qualidade e segurança de forma a garantir cuidados de saúde eficazes e adequados a todos os utentes, proporcionando simultaneamente condições de trabalho a todos os profissionais que dele fazem parte. A missão é proporcionar atendimento de saúde acessível, eficaz e de qualidade. Garantindo a segurança e o bem-estar de todos os pacientes através de profissionais altamente qualificados que garantem a excelência no atendimento médico. Tem como valores a promoção da saúde e bem-estar dos pacientes, o respeito e dignidade destes, a ética profissional, e o continuo investimento na inovação da prestação de serviços de saúde. A estratégia é proporcionar mais e melhores meios e serviços aos pacientes, através de projetos e programas para proporcionar melhores condições e satisfazer as necessidades dos pacientes, adquirindo e implementado novas tecnologias e abordagens. O objetivo é proporcionar um ambiente seguro e acolhedor, onde o paciente e os seus familiares se sintam confortáveis e cuidados. O intuito é melhorar a qualidade dos serviços prestados, melhorando a eficiência dos serviços hospitalares, reduzindo custos e simultaneamente incrementando a taxa de sucesso na recuperação dos pacientes, enaltecendo a reputação e eficácia da instituição hospitalar junto da comunidade.

1.1. Problema, Investigação

A facilidade de acesso à internet e a crescente dependência da tecnologia tornaram o mundo virtual num ambiente propício para a disseminação de ameaças virtuais, sendo estas cada vez mais perfecionistas e difíceis de detetar, uma entre muitas é o phishing que é utilizada por

cibercriminosos na obtenção de informações pessoais das vítimas, através de mensagens fraudulentas que imitam a aparência das fidedignas.

1.2. Motivação

O phishing, é um tipo de ameaça cada vez mais frequente e robusta, pode originar prejuízos financeiros avolumados e comprometer dados, quer privados, das próprias vítimas quer institucionais, por este motivo este tipo de ataques afeta não só os próprios, mas também as instituições, comprometendo o normal funcionamento das mesmas. Por mais mecanismo de segurança e proteções que se implementa numa instituição existe sempre uma vulnerabilidade que é extremamente difícil de controlar.

“"Os seres humanos são a parte mais vulnerável de qualquer sistema de segurança. Eles são os mais fáceis de enganar, manipular e controlar. Se você quiser invadir um sistema de segurança, não tente quebrar as proteções técnicas - em vez disso, ataque a pessoa que está atrás da proteção.” Mitnick, K. D., & Simon, W. L. (2003)

1.3. Finalidade e objetivos

Pelos mais diversos motivos é crucial minimizar esta vulnerabilidade, phishing.

“É importante treinar e educar os funcionários sobre as melhores práticas de segurança cibernética. Isso pode incluir treinamento em como detetar e evitar phishing, senhas seguras, segurança de dispositivos móveis e outros tópicos relevantes de segurança.” Wittkopp, J (2016)

É fundamental compreender como funcionam e quais as melhores práticas para prevenir e combater estas ameaças. O objetivo é aprofundar e compreender a exposição a este tipo de ataques, analisando o grau de maturidade dos funcionários de uma instituição hospitalar, para compreender qual o impacto e medidas de prevenção, com o intuito de contribuir para o desenvolvimento de estratégias mais efetivas de segurança da informação no ambiente digital, em particular neste sector.

1.4. Contributos

A escolha deste tema está diretamente relacionada com a sua eficácia. “"Phishing é um dos tipos de ataque cibernético melhor bem-sucedidos, explorando a natureza inerentemente vulnerável das pessoas para levá-las a revelar informações confidenciais. Os ataques de phishing estão em constante evolução, usando técnicas mais sofisticadas e personalizadas para tornar as mensagens mais convincentes e enganosas.” Jakobsson e Myers (2006)

Com base na introdução apresentada anteriormente, é importante assumir que utilizadores com maior conhecimento sobre phishing tendem a ser menos propensos a serem vítimas desses ataques.

Medidas de segurança adicionais, como autenticação de dois fatores, podem reduzir a eficácia dos ataques de phishing, no entanto nem sempre é linear a implementação deste sistema numa organização.

A eficácia dos ataques de phishing é influenciada pela aparência visual dos e-mails e sites fraudulentos, dai a importância do treino dos utilizadores na identificação de fatores e elementos que denunciem e evitem que os utilizadores sejam vítimas e consequentemente ponham em risco a instituição.

A quantidade e o tipo de informações solicitadas nos ataques de phishing podem variar de acordo com o perfil das vítimas, este tipo de ataque pode ser extremamente elaborado e ser inclusive direcionado ao tipo de utilizador alvo. A eficácia deste ataque é afetada pelo grau de personalização da mensagem enviada às vítimas. Utilizadores que têm maior confiança na sua capacidade de identificar e evitar ataques de phishing tendem a ser mais propensos a serem vítimas desses ataques devido a uma falsa sensação de segurança.

Inicialmente foram despoletados alguns alertas relacionados com ataques de malware com recurso ao e-mail e posteriormente campanha de phishing aos utilizadores, que eventualmente revelaram a deficiente preparação e a enorme vulnerabilidade que estes representam na segurança da organização.

As implicações teóricas deste estudo sobre ataques de phishing são diversas. Em primeiro lugar, a pesquisa pode contribuir para o avanço da compreensão teórica sobre o fenômeno do phishing e suas diferentes variantes, aprofundando o conhecimento sobre as táticas, técnicas e procedimentos utilizados pelos cibercriminosos. Desta forma a instituição tem conhecimento da reação e comportamento dos utilizadores, da forma como interagem, da sua preparação e de como se dispõem a combater estas vulnerabilidades. Quais os mecanismos que podem alavancar a vulnerabilidade ou a robustez dos utilizadores que influenciam a probabilidade de sucesso dos ataques de phishing, bem como os mecanismos que podem levar as pessoas a cair nesse tipo de fraude. É de extrema importância a proatividade para garantir a segurança de pacientes, dados e sistemas.

Em termos práticos, o estudo pode ajudar indivíduos, organizações e autoridades a adotar medidas mais efetivas de prevenção e combate aos ataques de phishing. Por exemplo, os resultados da pesquisa podem fornecer subsídios para o desenvolvimento de políticas de segurança da informação mais eficientes, bem como para a elaboração de programas de consciencialização e treino dos utilizadores sobre os riscos do phishing e as melhores práticas para evitá-lo.

Ademais, o estudo pode trazer benefícios diretos para as vítimas de phishing, ao oferecer informações mais precisas sobre como reconhecer e evitar esses ataques, além de orientações sobre como agir em caso de terem suas informações pessoais ou financeiras comprometidas. Dessa forma, a pesquisa pode contribuir para reduzir os danos causados por essa prática criminosa e aumentar a segurança da informação no ambiente digital.

1.5. Finalidade

O problema que levou a implementar esta investigação acaba por ser a necessidade de saber responder às seguintes questões:

Qual a preparação dos utilizadores, qual a ameaça associada a estes para a instituição?

Qual a informação e preparação para este tipo de ameaças?

1.6. Estrutura do documento

Este documento é constituído por onze capítulos, seguido de bibliografia.

O primeiro capítulo, faz uma pequena abordagem à instituição, qual o problema de investigação proposto, assim como a motivação que me levou a implementar este estudo, qual a finalidade e o objetivo do mesmo e quais as questões base que pretendo esclarecer; o segundo capítulo, refere o método, iniciando uma abordagem e análise aos padrões de funcionários, ou seja, a tempo inteiro e prestadores. Estudei a caracterização da amostra, em função das idades, sexo, habilitações e grupos profissionais; no terceiro capítulo, achei por bem, despertar os utilizadores acerca do tema abordado, uma vez que seria novidade este tipo de interação como os mesmos; o quarto capítulo, explanei a calendarização do estudo, os timings e a sequência de implementação e execução do trabalho; o quinto e sexto capítulo referem-se à implementação das campanhas de phishing, no caso foram duas, dai a divisão em dois capítulos; o sétimo capítulo explica a implementação de um quis com o intuito de ajudar na preparação dos utilizadores para estes tipos de ataques; o oitavo capítulo, esclarece a forma como foi criado e enviado o inquérito de aceitação e abordagem da temática pelos utilizadores; no capítulo nono, estão explicados os resultados obtidos com a implementação das tarefas anteriormente identificadas; finalmente no décimo capítulo foram discutidos os resultados obtidos, terminando no décimo primeiro com as conclusões, seguido da bibliografia consultada na preparação e no desenrolar de todos este trabalho.

2. Revisão da literatura

O phishing é um dos tipos mais comuns de fraude online, e, portanto, tem sido amplamente estudado pela comunidade académica.

Outros trabalhos similares depararam-se com dificuldades, das quais não afetaram este, nomeadamente, o caso de estudo, Rizzoni et al. (2019) vários e-mails foram identificados pelo antivírus como spam, embora o universo de utilizadores tenha sido o triplo em comparação com este e o endereço de e-mail utilizado nas várias campanhas, mais especificamente três foi sempre o mesmo. O hospital em causa já tinha implementado na intranet um exercício de cybersegurança, pelo facto de estar envolvido num projeto europeu, PANACEA[1], sobre cibersegurança envolvendo um estudo sobre o fator técnico e humano na cibersegurança hospitalar. Neste caso o hospital onde vou realizar a campanha de fishing nunca fez este tipo de trabalho.

De acordo com Gordon et al. (2017), "os profissionais de saúde podem beneficiar de programas de treino de consciencialização sobre phishing que incluem testes práticos para identificar áreas de vulnerabilidade", no estudo de seis instituições de saúde que têm simuladores de phishing, desde 1 de agosto de 2011, outra realidade que nada tem que ver com a nossa mais de uma década depois. A amostra é cerca de 3 milhões de e-mails onde 14.2% clicou, cerca de 1 em cada 7 utilizadores clicou no link, no entanto não testaram a possibilidade dos utilizadores inserirem credenciais, só analisaram os cliques nos links. O facto de a campanha estar ativa 24h, também não me parece que faça sentido, uma vez que estamos a analisar utilizadores que trabalham por turnos e inclusive podem não estar presentes durante este período, optei por manter a campanha ativa durante uma semana, período este que podia contemplar toda a amostra, salvo raras exceções, tipo férias, baixas ou eventualmente formações.

[1] www.panacearesearch.eu

Alguns estudos foram mais pormenorizados, Priestman, (2019), além de e-mail analisaram tráfego de internet, no entanto, concluíram de igual forma a fragilidade dos utilizadores, que inclusive adicionaram fotos contendo dados profissional no seu perfil de Facebook.

Bikov, (2019, May 1) conclui que a necessidade de treino desenvolve a experiência prática que os utilizadores necessitam e as campanhas de phishing são essenciais para a evolução do conhecimento dos utilizadores

Gordon, (2019), implementaram 20 campanhas de phishing e mais de cinquenta por cento dos utilizadores foram vítimas. Estas campanhas foram aplicadas ao longo de 3 anos com periodicidades de dois a três meses e verificou-se diminuição do número de vítimas por campanha, o que valida a importância destes treinos.

São imensos os estudos que reforçam a necessidade de formação e treino dos utilizadores, como prática para diminuir a vulnerabilidade deste tipo de ataques.

MÉTODO

2.1. Funcionários a tempo inteiro e prestadores de serviço

É importante analisar a população alvo deste trabalho, que está dividida em dois grupos, os profissionais que trabalham a tempo inteiro e os prestadores de serviços que se deslocam pontualmente à instituição, os denominados tarefeiros, por exemplo os médicos radiologistas que ganham consoante os relatórios realizados e que prestam serviço alguns um dia por semana, outros quinzenalmente ou mensalmente mediante a necessidade e as especialidades. Outro exemplo são os médicos que fazem serviço de urgência, alguns provenientes de centros de saúde que acabam por fazer turnos na instituição, nestes casos chegam a estar meses ausentes da instituição. Na tabela 1 estão quantificados os referidos profissionais á data do estudo. Para uma melhor perceção entre o número de funcionário a tempo inteiro e os prestadores representei-os no gráfico 1.

Tabela 1 - Funcionários a tempo inteiro e prestadores de serviços

	Funcionários	Prestadores
Total	1734	161

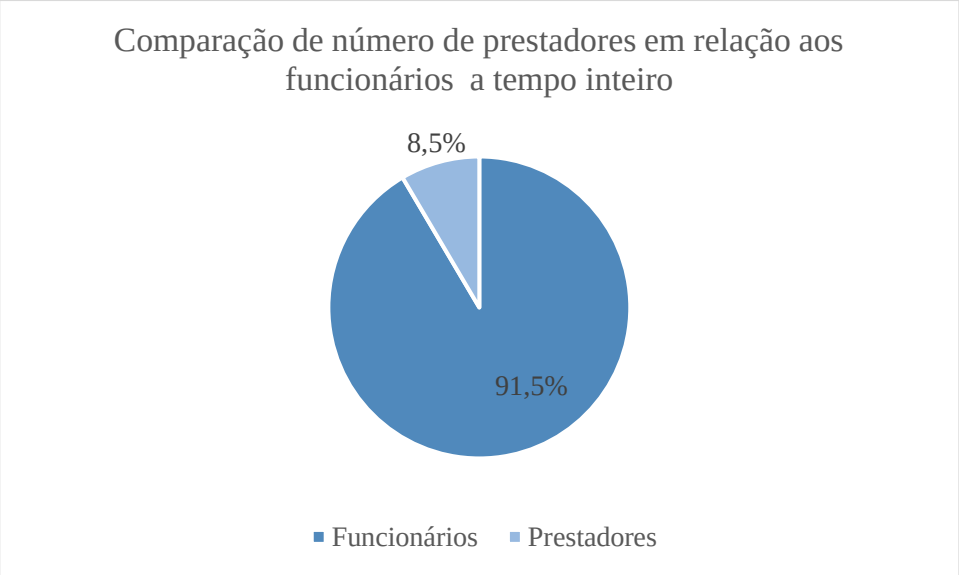


Gráfico 1 - Quantidade de prestadores em relação aos funcionários a tempo inteiro

2.3. Caracterização da amostra

2.3.1. Por forma a facilitar e a quantificar os funcionários em função dos dados demográficos construi com recurso ao PowerBI alguns filtros que ajudam a obter os dados pretendidos e a interpretação dos mesmos:

2.3.1.1. Anexo B
- Funcionários e Prestadores por sexo e idades

2.3.1.2. Anexo C
- Funcionários e Prestadores por sexo e idades, exemplo de idades compreendidas entre 33 e 43 anos

2.3.1.3. Anexo D
- Outra representação, mais global e menos interativa, sobre a distribuição de idades e sexo dos funcionários

2.3.1.4. Anexo E
- Árvore de decisão, mediante a escolha do sexo masculino ou feminino, é aplicado um filtro e posteriormente através da seleção do grupo profissional é apresentado o nível habilitacional, aplicando além dos mencionados outro filtro de idade

2.3.1.5. Anexo F
- Tabela relacional entre nível habilitacional e grupo profissional

2.3.1.6. Anexo G
- Tabela relacional entre grupo profissional e nível habilitacional

2.3.2. Idades

2.3.2.1. Funcionários

Em relação às idades dos funcionários da instituição optei por separá-los por décadas, na tabela 2 estão representados os funcionários que estão entre os 20, inclusive e ainda não atingiram os 30 anos:

Tabela 2 - Idades dos funcionários entre os 20 e 29 anos

	Funcionários							
Idade	22	23	24	25	26	27	28	29
Número de indivíduos	2	7	29	28	31	18	38	30

Na tabela 3 estão representados os funcionários que estão entre os 30, inclusive e ainda não atingiram os 40 anos:

Tabela 3 - Idades dos funcionários entre os 30 e 39 anos

	Funcionários									
Idade	30	31	32	33	34	35	36	37	38	39
Número de indivíduos	43	49	54	44	41	41	43	41	56	56

Na tabela 4 estão representados os funcionários que estão entre os 40, inclusive e ainda não atingiram os 50 anos:

Tabela 4 - Idades dos funcionários entre os 40 e 49 anos

	Funcionários									
Idade	40	41	42	43	44	45	46	47	48	49
Número de indivíduos	38	55	54	29	44	43	47	41	40	42

Na tabela 5 estão representados os funcionários que estão entre os 50, inclusive e ainda não atingiram os 60 anos:

Tabela 5 - Idades dos funcionários entre os 50 e 59 anos

	Funcionários									
Idade	50	51	52	53	54	55	56	57	58	59
Número de indivíduos	47	44	45	27	42	39	41	45	36	54

Na tabela 6 estão representados os funcionários que estão entre os 60, inclusive e ainda não atingiram os 70 anos:

Tabela 6 - Idades dos funcionários entre os 60 e 69 anos

	Funcionários									
Idade	60	61	62	63	64	65	66	67	68	69
Número de indivíduos	40	34	31	27	40	28	13	10	2	3

Na tabela 7 estão representados os funcionários que têm mais de 70 anos:

Tabela 7 – Idades dos funcionários entre os 70 e 79 anos

	Funcionários
Idade	71
Número de indivíduos	2

Recorrendo a uma representação gráfica global das idades de todos os funcionários, contrui o gráfico 2:

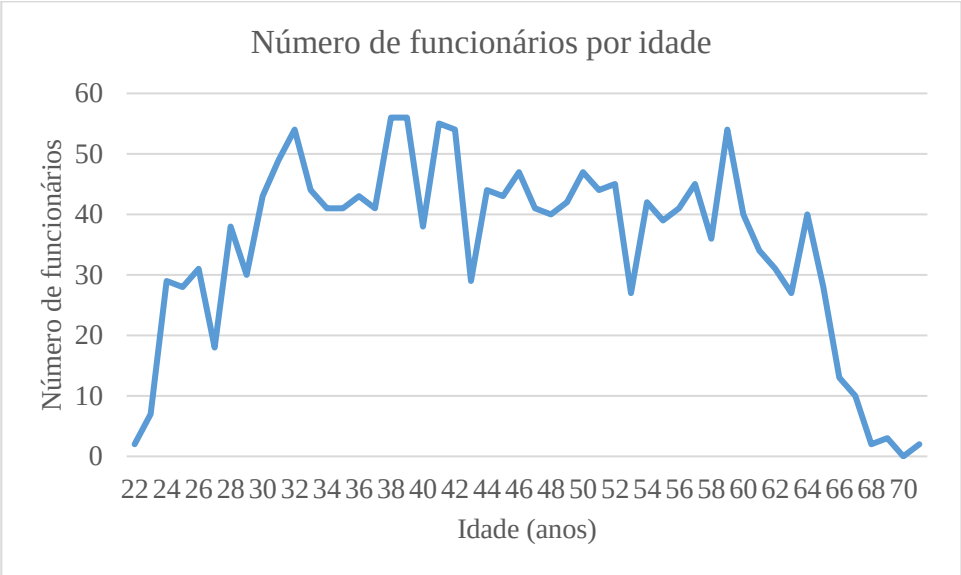


Gráfico 2 - Distribuição de funcionários por idade

Analisando as idades dos funcionários por classes, foi construída a tabela 8:

Tabela 8 - Idades de funcionários por classes

Idades	Número de funcionários
20 a 29	183
30 a 39	468
40 a 49	433
50 a 59	420
60 a 69	228
70 a 79	2

Baseado na tabela anterior foi elaborada a representação gráfica da mesma, obtendo o gráfico 3:

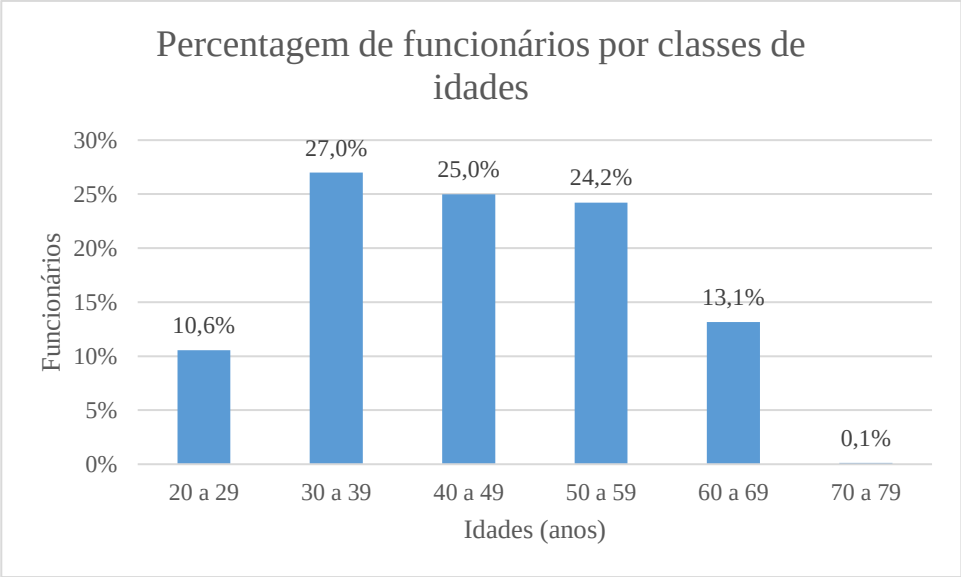


Gráfico 3- Funcionários distribuídos por classes de idades

Na tabela 9, está representada a média e a moda das idades dos funcionários efetidos na instituição estudada.

Tabela 9 – Média e moda das idades dos funcionários

Média	45
Moda	38

2.3.2.2. Prestadores

Analisando agora as idades dos prestadores da instituição, foi elaborada a tabela 10 que representa os prestadores que têm idade entre os 20, inclusive e que ainda não atingiram os 30 anos:

Tabela 10 - Idades dos prestadores entre os 20 e 29 anos

	Prestadores		
Idade	27	28	29
Número de indivíduos	3	2	1

Na tabela 11, estão representados os prestadores com idades compreendidas entre os 30 e ainda não atingiram os 40 anos.

Tabela 11 - Idades dos prestadores entre os 30 e 39 anos

	Prestadores									
Idade	30	31	32	33	34	35	36	37	38	39
Número de indivíduos	5	4	5	4	10	10	7	6	10	9

Na tabela 12, estão representados os prestadores que têm entre 40, inclusive e ainda não fizeram os 50 anos.

Tabela 12 - Idades dos prestadores entre os 40 e 49 anos

	Prestadores									
Idade	40	41	42	43	44	45	46	47	48	49
Número de indivíduos	8	8	7	3	2	5	3	6	3	1

Na tabela 13, estão representados os trabalhadores que já completaram 50, mas ainda não fizeram 60 anos:

Tabela 13 - Idades dos prestadores entre os 50 e 59 anos

	Prestadores									
Idade	50	51	52	53	54	55	56	57	58	59
Número de indivíduos	5	1	1	1	3	2	2	1	1	2

Na tabela 14, estão os prestadores com mais de 60 anos, inclusive e manos de 70 anos;

Tabela 14 - Idades dos prestadores entre os 60 e 69 anos

	Prestadores									
Idade	60	61	62	63	64	65	66	67	68	69
Número de indivíduos	1	2	0	2	1	4	2	2	2	1

Na tabela 15, estão todos os prestadores com mais de 70 anos de idade.

Tabela 15 - Idades dos prestadores entre os 70 e 79 anos

	Prestadores		
Idade	70	71	74
Número de indivíduos	1	1	1

Há semelhança do que foi feito anteriormente para os funcionários, foi elaborada a representação gráfica das idades dos prestadores no gráfico 4:

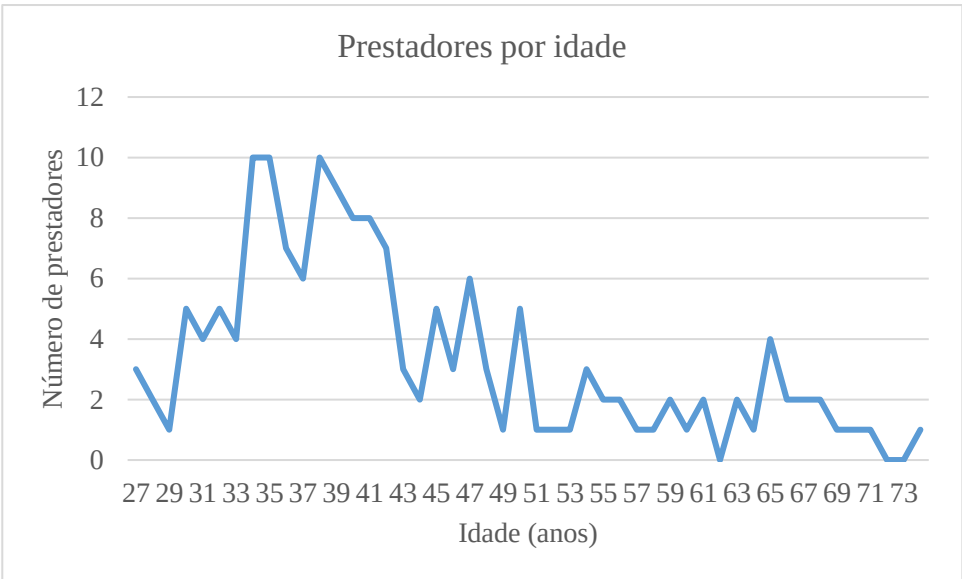


Gráfico 4 - Distribuição de prestadores por idade

Recorrendo a uma representação por classes das idades dos prestadores da instituição alvo de estudo obteve-se o gráfico 5:

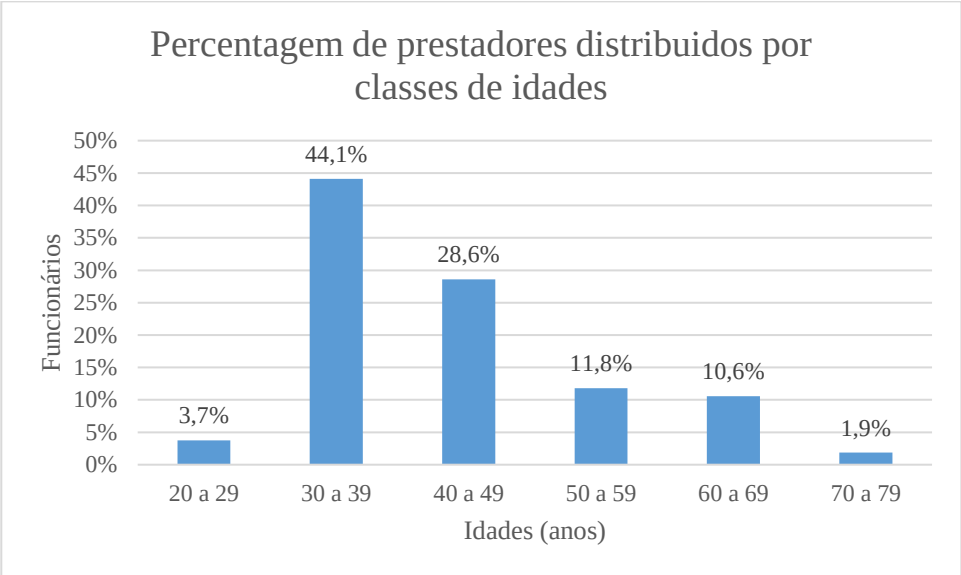


Gráfico 5 - Percentagem de prestadores por classes de idades

Na tabela 16, está representada a média e a moda das idades dos prestadores:

Tabela 16 – Média e moda das idades dos prestadores

Média	43
Moda	38

2.3.3.Sexo

No que respeita aos funcionários a tempo inteiro e aos prestadores, estão distribuídos por sexo da seguinte forma, consoante consta na tabela 17:

Tabela 17 – Distribuição de funcionários e prestadores por sexo

	Funcionários	Prestadores
Masculino	343	92
Feminino	1391	69

Para ter uma melhor precessão do sexo dos mesmos, foi elaborado o gráfico 6, onde é notória a predominância do sexo feminino nos funcionários a tempo inteiro:

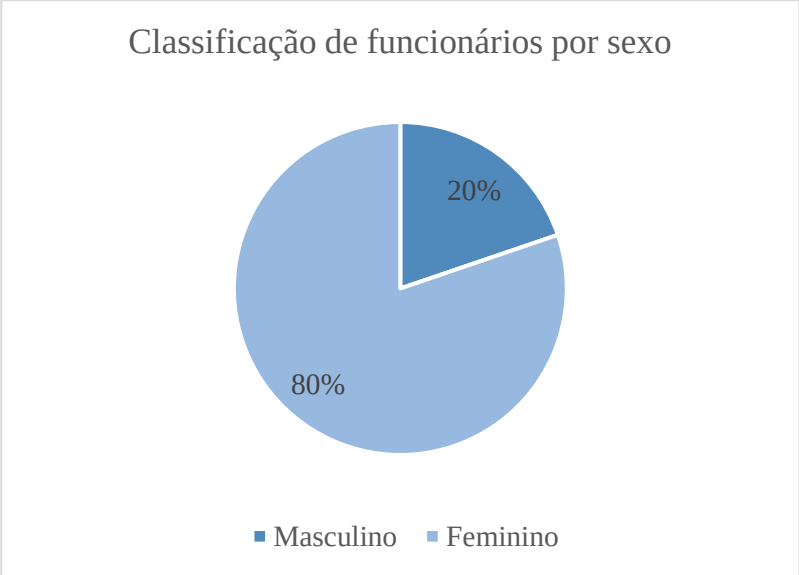


Gráfico 6 - Classificação de funcionários a tempo inteiro por sexo

O gráfico 7, representa a distribuição dos prestadores por sexo, curiosamente os prestadores de serviço estão mais equilibrados no que concerne à classificação por sexo em comparação com os funcionários a tempo inteiro:

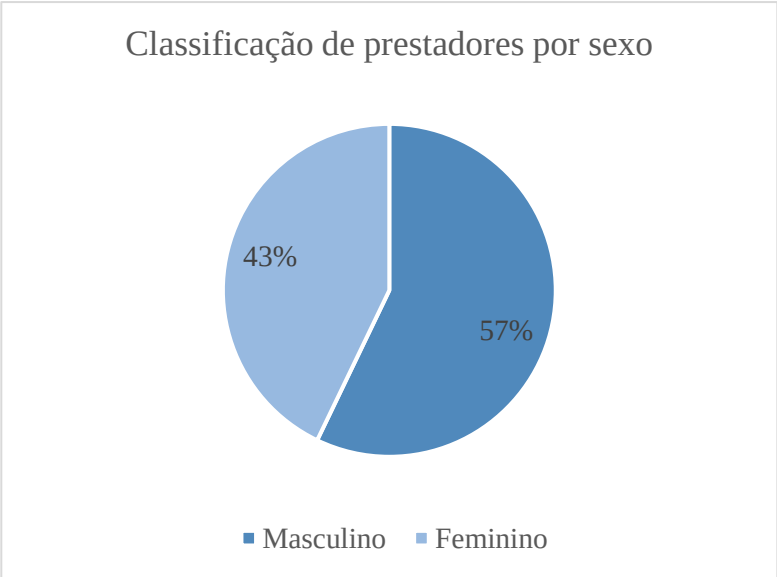


Gráfico 7- Classificação de prestadores por sexo

2.3.4.Habilitações Literárias

As habilitações escolares dos funcionários variam bastante, existem funcionários com menos do que a quarta classe e outros com doutoramento, em relação aos prestadores são um grupo mais homogéneo onde o grau mais baixo é a licenciatura.

2.3.4.1. Funcionários

As habilitações dos funcionários estão representadas na tabela 18, verificando-se que a esmagadora maioria são licenciados:

Tabela 18 - Habilitações dos funcionários

Habilitações	Funcionários
menos 4º ano	2
4º ano	27

5º ano	0
6º ano	78
7º ano	3
8º ano	4
9º ano	155
10º ano	5
11º ano	33
12º ano	249
Ensino Secundário Não Superior de Nível IV	9
Ensino Pós-Secundário Não Superior de Nível V	1
Curso Técnico Profissional	15
Bacharelato	148
Licenciatura	790
Pós-Licenciatura (Especialização)	38
Pós-Graduação	15
Mestrado	157
Doutoramento	5

Recorrendo á representação gráfica da tabela 18 foi elaborado o gráfico 8 e a distribuição fica:

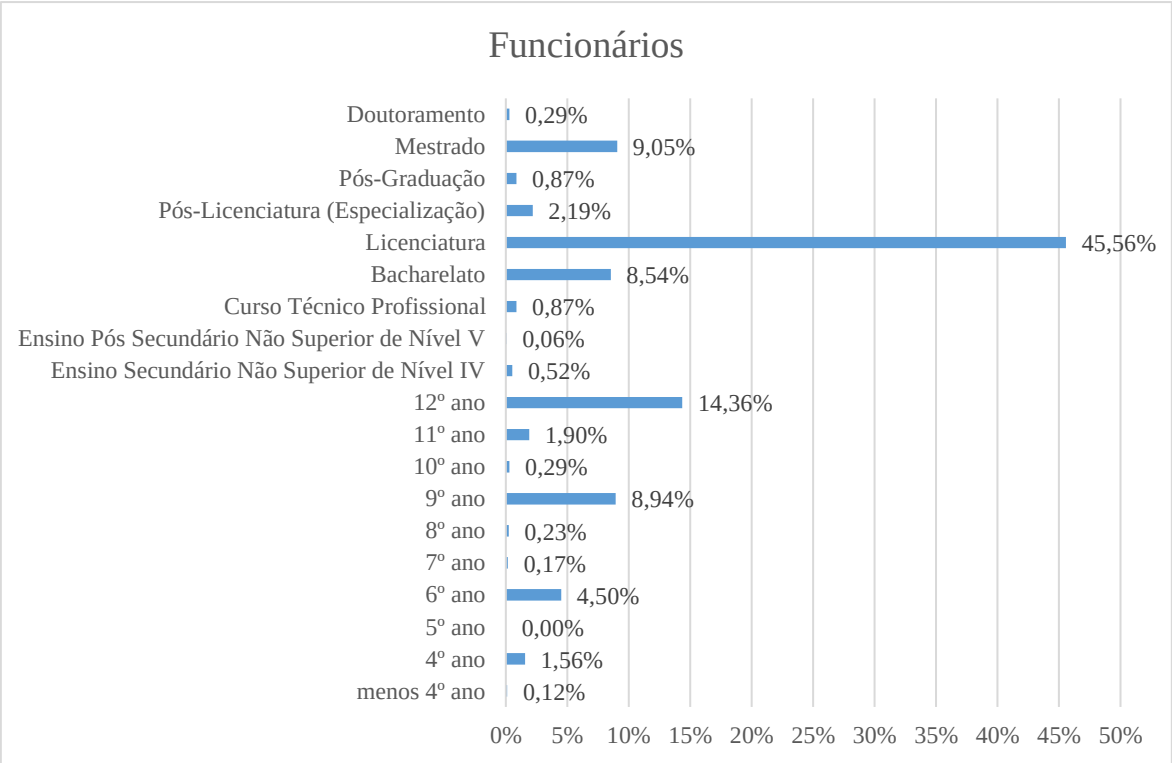


Gráfico 8- Percentagem de funcionários por habilitações

Tabela 19 - Habilitações por categoria profissional

	menos 4º ano	4º ano	6º ano	7º ano	8º ano	9º ano	10º ano	11º ano	12º ano	Ensino Secundário Não Superior de Nível IV	Ensino Pós-Secundário Não Superior de Nível V	Curso Técnico Profissional	Bacharelato	Licenciatura	Pós-Licenciatura (Especialização)	Pós-Graduação	Mestrado	Doutoramento	TOTAL PARCIAL
Administração Hospitalar														4					**4**
Assistente Operacional	2	27	78	3	4	139	4	17	171	9	1	9	2	11					**477**

Assistente Técnico						14	1	14	75			3	4	34		1	1		**147**
Conselho Fiscal														2				1	**3**
Pessoal de Enfermagem								2	1				114	465	35	6	16	1	**640**
Pessoal de Informática						1			1			3		2					**7**
Pessoal Dirigente													1	7			2	1	**11**
Pessoal em formação pré-carreira Médica														15	1		72	1	**89**
Pessoal em formação pré-carreira Farmacêutica														1			2		**3**

Pessoal Farmacêutico														9					**9**
Pessoal Médico														129	1	3	46		**179**
Pessoal Técnico Sup. de Diagnóstico e Terapêutica						1			1				27	84		3	14	1	**131**
Pessoal Técnico Superior de Saúde														3			1		**4**
Técnicos Superiores														24	1	2	3		**30**
TOTAL PARCIAL	**2**	**27**	**78**	**3**	**4**	**155**	**5**	**33**	**249**	**9**	**1**	**15**	**148**	**790**	**38**	**15**	**157**	**5**	**1734**

A tabela 19 foi introduzida no final como anexo A para facilitar a leitura da mesma.

Tabela 20 – Percentagem habilitações por categoria profissional

	menos 4º ano até 8 ano	9º ano	10º ano	11º ano	12º ano	Ensino Secundário Não Superior de Nível	Ensino Pós-Secundário Não	Curso Técnico Profissional	Bacharelato	Licenciatura	Pós-Licenciatura (Especialização)	Pós-Graduação	Mestrado	Doutoramento
Administração Hospitalar										0.5%				
Assistente Operacional	100%	89.7%	80.0%	51.5%	68.7%	100%	100%	60.0%	1.4%	1.4%				
Assistente Técnico		9.0%	20.0%	42.4%	30.1%			20.0%	2.7%	4.3%		6.7%	0.6%	
Conselho Fiscal										0.3%				20.0%
Pessoal de Enfermagem				6.1%	0.4%				77.0%	58.9%	92.1%	40.0%	10.2%	20.0%
Pessoal de Informática		0.6%			0.4%			20.0%		0.3%				
Pessoal Dirigente									0.7%	0.9%			1.3%	20.0%
Pessoal em formação pré-carreira Médica										1.9%	2.6%		45.9%	20.0%
Pessoal em formação pré-carreira Farmacêutica										0.1%			1.3%	
Pessoal Farmacêutico										1.1%				
Pessoal Médico										16.3%	2.6%	20.0%	29.3%	

Pessoal Técnico Sup. de Diagnóstico e Terapêutica		0.6%			0.4%				18.2%	10.6%		20.0%	8.9%	20.0%
Pessoal Técnico Superior de Saúde										0.4%			0.6%	
Técnicos Superiores										3.0%	2.6%	13.3%	1.9%	
TOTAL PARCIAL	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

A tabela 19, representa as habilitações literárias dos funcionários a tempo inteiro mediante a sua categoria profissional

Para facilitar a leitura optei por dividir as habilitações em duas tabelas, uma primeira, tabela 21 que inclui até 12º ano, inclusive e uma segunda, tabela 22, com habilitações superiores:

Tabela 21 - Percentagem de habilitações (em relação à totalidade dos funcionários) até ao 12º ano inclusive

	menos 4º ano	4º ano	5º ano	6º ano	7º ano	8º ano	9º ano	10º ano	11º ano	12º ano
Administração Hospitalar										
Assistente Operacional	0.12%	1.56%		4.50%	0.17%	0.23%	8.02%	0.23%	0.98%	9.86%
Assistente Técnico							0.81%	0.06%	0.81%	4.33%
Conselho Fiscal										
Pessoal de Enfermagem									0.12%	0.06%
Pessoal de Informática							0.06%			0.06%
Pessoal Dirigente										
Pessoal em formação pré-carreira Médica										
Pessoal em formação pré-carreira Farmacêutica										
Pessoal Farmacêutico										
Pessoal Médico										
Pessoal Técnico Sup. de Diagnóstico e Terapêutica							0.06%			0.06%
Pessoal Técnico Superior de Saúde										
Técnicos Superiores										
TOTAL PARCIAL	**0.12%**	**1.56%**	**0.00%**	**4.50%**	**0.17%**	**0.23%**	**8.94%**	**0.29%**	**1.90%**	**14.36%**

Tabela 22 - Percentagem de habilitações superiores ao 12º ano em relação à totalidade dos funcionários

	Ensino Secundário Não Superior de Nível IV	Ensino Pós-Secundário Não Superior de Nível V	Curso Técnico Profissional	Bacharelato	Licenciatura	Pós-Licenciatura (Especialização)	Pós-Graduação	Mestrado	Doutoramento
Administração Hospitalar					0.23%				
Assistente Operacional	0.52%	0.06%	0.52%	0.12%	0.63%				
Assistente Técnico			0.17%	0.23%	1.96%		0.06%	0.06%	
Conselho Fiscal					0.12%				0.06%
Pessoal de Enfermagem				6.57%	26.82%	2.02%	0.35%	0.92%	0.06%
Pessoal de Informática			0.17%		0.12%				
Pessoal Dirigente				0.06%	0.40%			0.12%	0.06%
Pessoal em formação pré-carreira Médica					0.87%	0.06%		4.15%	0.06%
Pessoal em formação pré-carreira Farmacêutica					0.06%			0.12%	
Pessoal Farmacêutico					0.52%				
Pessoal Médico					7.44%	0.06%	0.17%	2.65%	
Pessoal Técnico Sup. de Diagnóstico e Terapêutica				1.56%	4.84%		0.17%	0.81%	0.06%

Pessoal Técnico Superior de Saúde					0.17%			0.06%	
Técnicos Superiores					1.38%	0.06%	0.12%	0.17%	
TOTAL PARCIAL	**0.52%**	**0.06%**	**0.87%**	**8.54%**	**45.56%**	**2.19%**	**0.87%**	**9.05%**	**0.29%**

Se analisarmos a percentagem de funcionários que não tem formação superior, verificamos que representam um terço do total, como demonstrado na tabela 23:

Tabela 23 - Percentagem de formação não superior

	menos 4º ano	4º ano	5º ano	6º ano	7º ano	8º ano	9º ano	10º ano	11º ano	12º ano	Ensino Secundário Não Superior de Nível IV	Ensino Pós-Secundário Não Superior de Nível V	Curso Técnico Profissional
TOTAL PARCIAL	**0.12%**	**1.56%**	**0.00%**	**4.50%**	**0.17%**	**0.23%**	**8.94%**	**0.29%**	**1.90%**	**14.36%**	**0.52%**	**0.06%**	**0.87%**
Acumulado		1.67%	1.67%	6.17%	6.34%	6.57%	15.51%	15.80%	17.70%	32.06%	32.58%	32.64%	33.51%

Na tabela 24, facilmente se verifica que cerca de dois terços têm formação superior:

Tabela 24 - Percentagem de funcionários com formação superior

	Bacharelato	Licenciatura	Pós-Licenciatura (Especialização)	Pós-Graduação	Mestrado	Doutoramento
TOTAL PARCIAL	**8.54%**	**45.56%**	**2.19%**	**0.87%**	**9.05%**	**0.29%**
Acumulado		54.09%	56.29%	57.15%	66.21%	66.49%

No gráfico 9 é percetível o acumulado de habilitações dos funcionários:

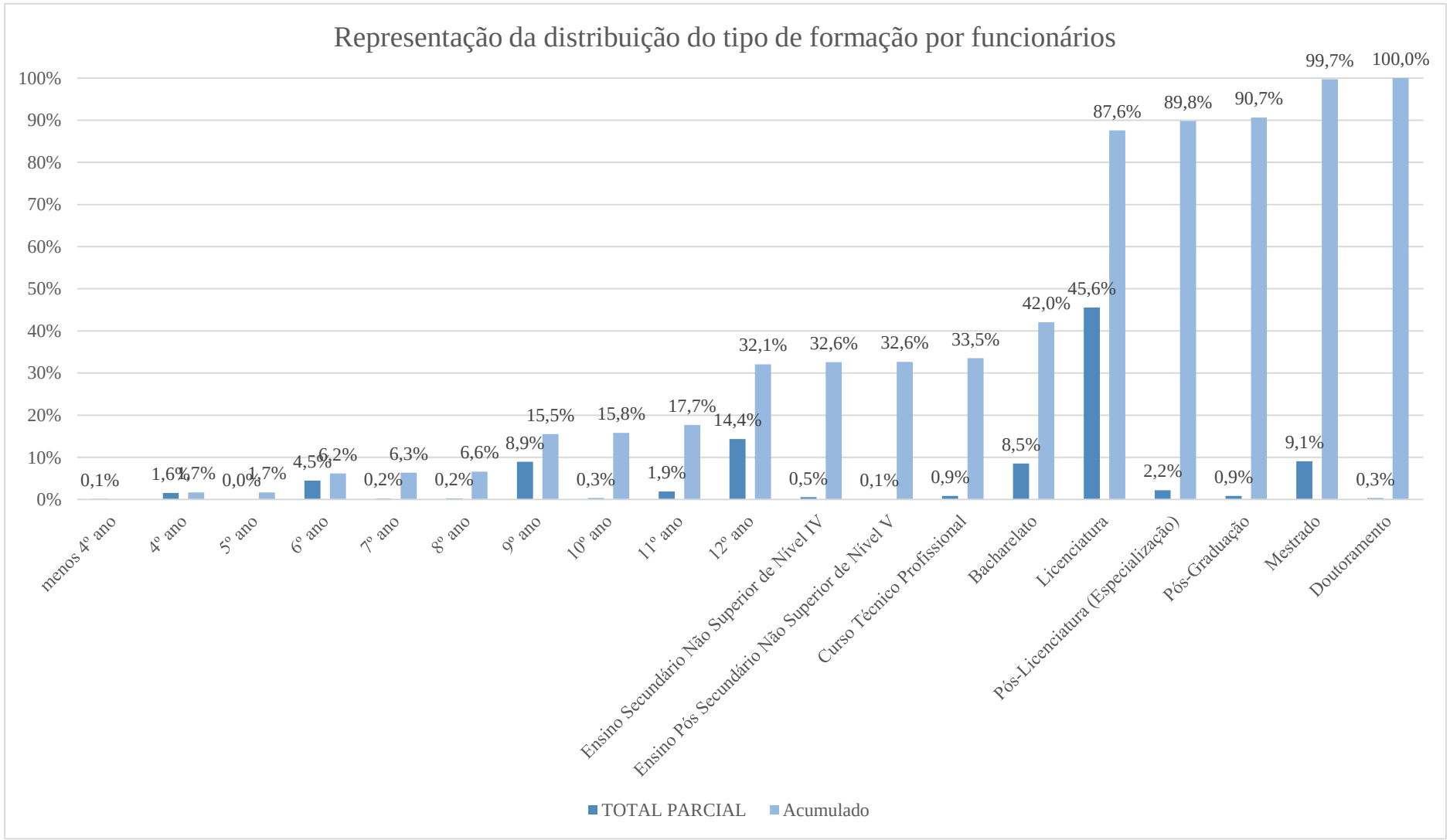


Gráfico 9 - Representação da distribuição de habilitações

As habilitações inferiores ao nono ano estão associadas aos assistentes operacionais.

Uma vez que a maior percentagem de habilitações são licenciaturas, optei por representar graficamente esta distribuição, gráfico 10, onde se verifica que grande parte é referente ao pessoal de enfermagem:

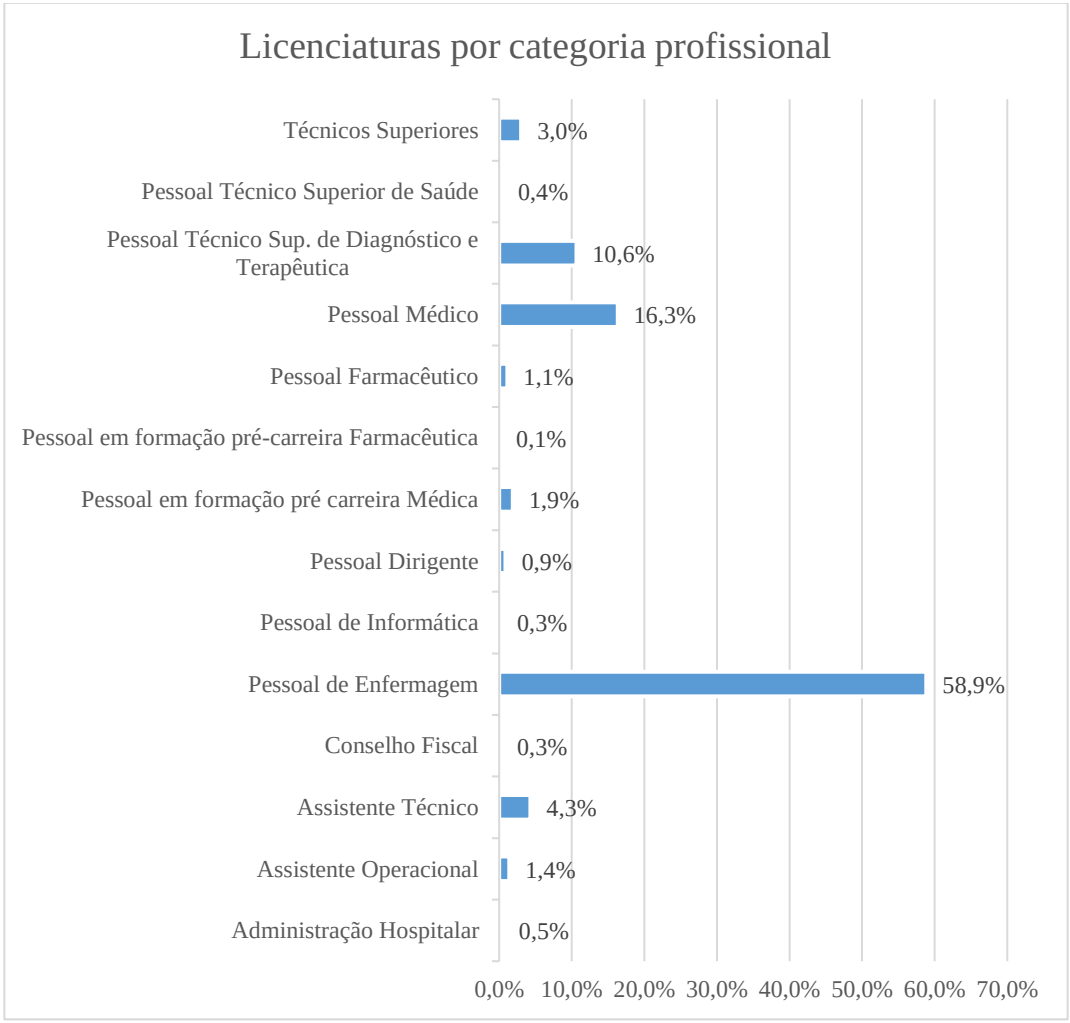


Gráfico 10 - Distribuição de licenciaturas por categoria profissional

2.3.4.2. Prestadores

As habilitações dos prestadores são maioritariamente licenciatura e mestrado como se pode verificar na tabela 25:

Tabela 25 - Habilitações dos prestadores

Habilitações	Prestadores de serviços
Licenciatura	83
Pós-Licenciatura (Especialização)	2
Mestrado	74
Doutoramento	2

Analisando graficamente, foi elaborado o gráfico 11:

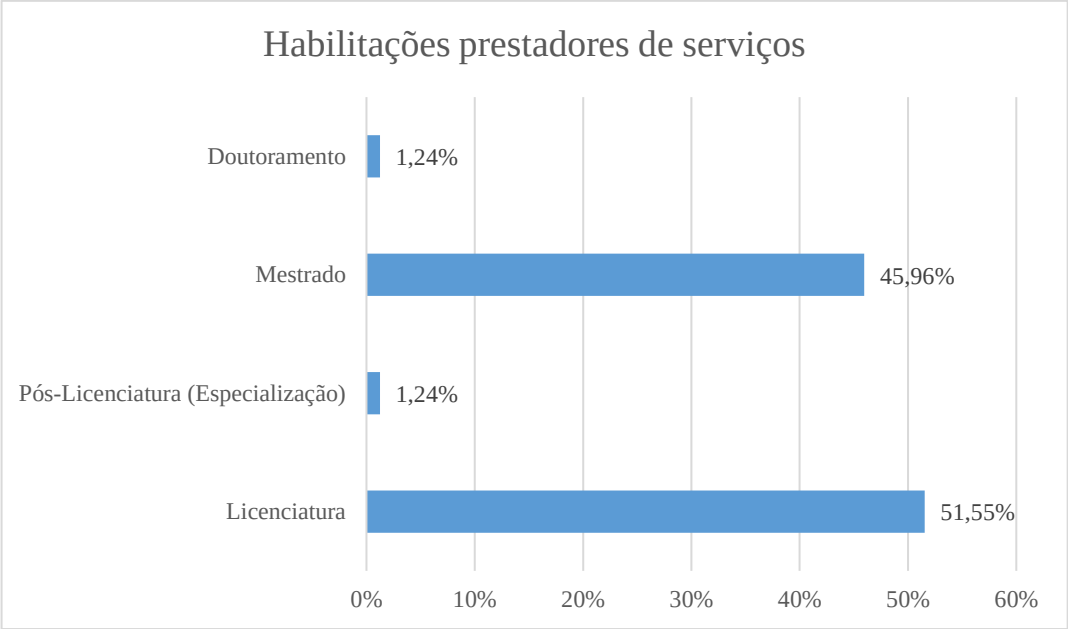


Gráfico 11 - Habilitações prestadores de serviços

2.3.5. Grupo profissional

2.3.5.1. Funcionários

Os funcionários estão inseridos nas seguintes categorias, consoante a tabela 26:

Tabela 26- Distribuição de funcionários por grupo profissional

Grupo Profissional	Funcionários	Prestadores
Administração Hospitalar	4	0
Assistente Operacional	477	0
Assistente Técnico	147	0
Conselho Fiscal	3	0
Pessoal de Enfermagem	640	0
Pessoal de Informática	7	0
Pessoal Dirigente	11	0
Pessoal em formação pré-carreira Médica	89	6
Pessoal em formação pré-carreira Farmacêutica	3	0
Pessoal Farmacêutico	9	0
Pessoal Médico	179	150
Pessoal Técnico Superior de Diagnóstico e Terapêutica	131	0
Pessoal Técnico Superior de Saúde	4	0
Técnicos Superiores	30	4
Outro Pessoal	0	1

Por forma a ter uma melhor precessão da distribuição dos funcionários por categoria profissional foi contruído o seguinte gráfico, gráfico 12, referente aos profissionais a tempo inteiro:

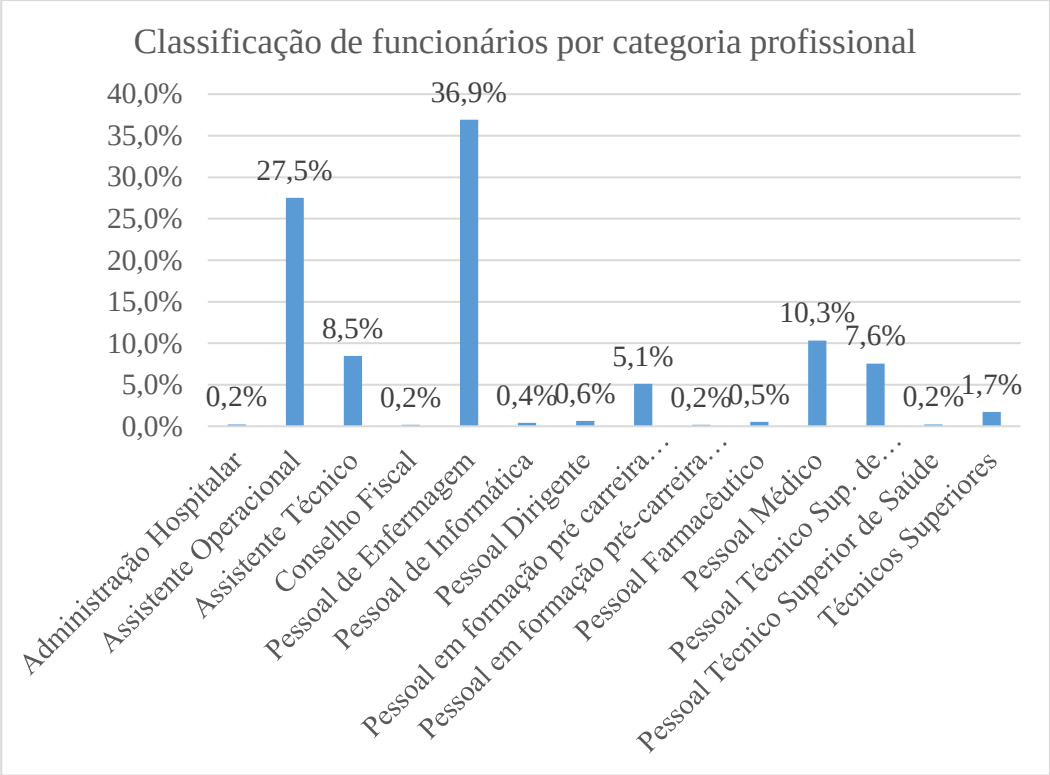


Gráfico 12 - Classificação de funcionários a tempo inteiro por categoria profissional

É percetível que a esmagadora maioria, nomeadamente 96%, se distribuem por 6 das 14 categorias existentes, como se demonstra na tabela 27.

Tabela 27 – Distribuição de 96% dos funcionários

Grupo Profissional	Funcionários
Assistente Operacional	477
Assistente Técnico	147
Pessoal de Enfermagem	640
Pessoal em formação pré-carreira Médica	89
Pessoal Médico	179
Pessoal Técnico Superiores de Diagnóstico e Terapêutica	131

Graficamente, gráfico 13,a distribuição dos 96% dos funcionários fica:

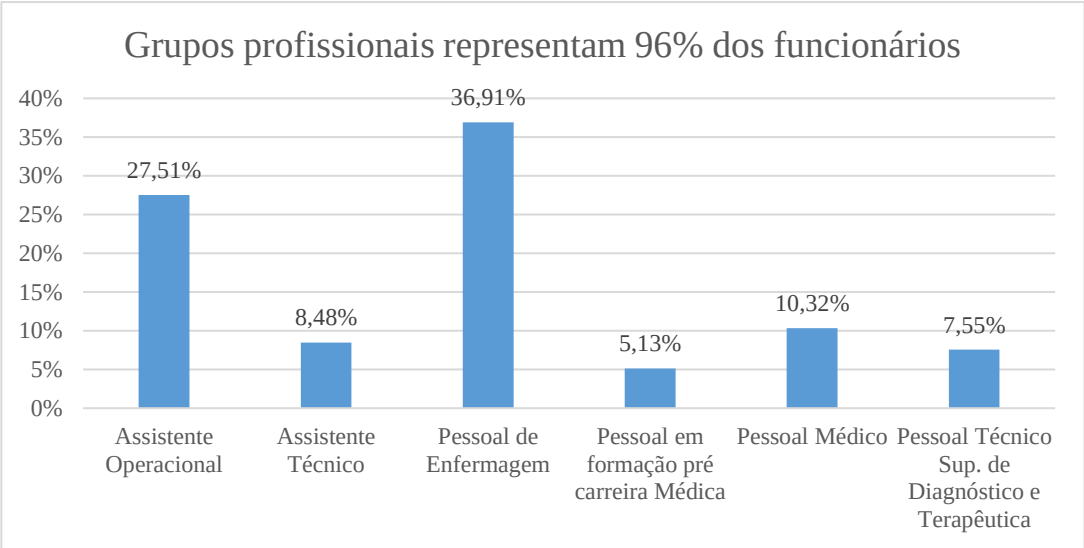


Gráfico 13 - Representação de 96% dos funcionários a tempo inteiro

Os restantes 4% dos funcionários estão distribuídos da seguinte forma, tabela 28:

Tabela 28 - Distribuição de 4% dos funcionários

Grupo Profissional	Funcionários
Administração Hospitalar	4
Conselho Fiscal	3
Pessoal de Informática	7
Pessoal Dirigente	11
Pessoal em formação pré-carreira Farmacêutica	3
Pessoal Farmacêutico	9
Pessoal Técnico Superior de Saúde	4
Técnicos Superiores	30

Graficamente a distribuição de 4% dos funcionários fica como está no gráfico 14:

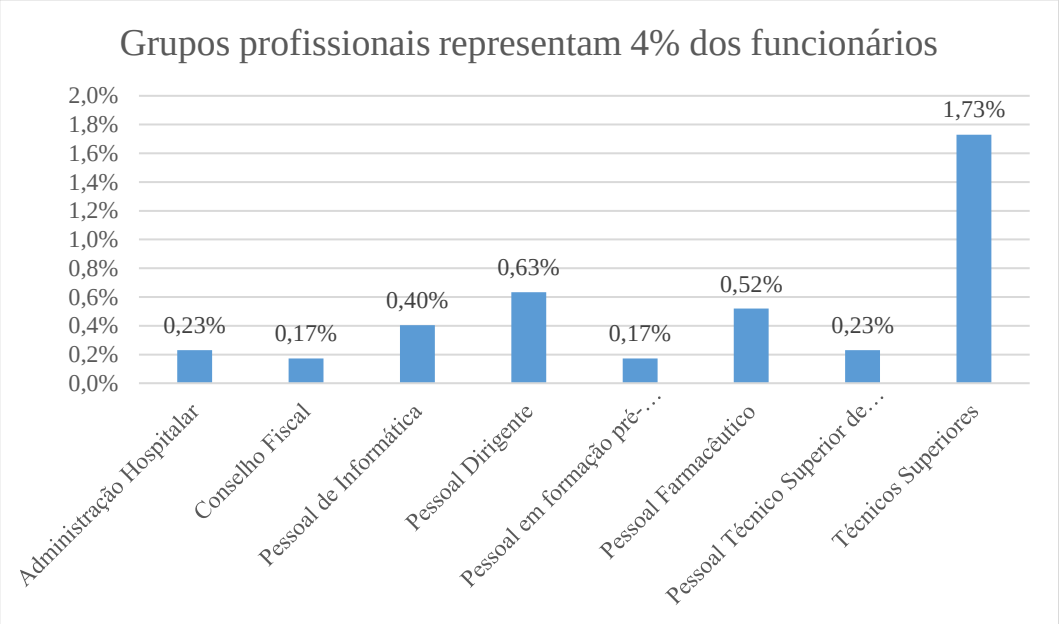


Gráfico 14- Representação de 4% dos funcionários a tempo inteiro

De salientar que embora o menor grupo pode ser o menos preocupante, uma vez que representa só 4% dos funcionários, mas é importante salientar que são estes quem possui mais permissões e acessos no sistema informático.

2.3.5.2. Prestadores

Em relação aos prestadores de serviços, em comparação com os funcionários, nem chegam a 9% destes (8.5% mais precisamente), além de que devido à sua presença não ser diária possivelmente grande parte destes nem serão analisados no âmbito de intervenção deste trabalho. De qualquer forma a distribuição por grupo profissional é apresentada na tabela 29:

Tabela 29 - Distribuição de prestadores por grupo profissional

Grupo Profissional	Prestadores
Pessoal em formação pré-carreira Médica	6
Pessoal Médico	150
Técnicos Superiores	4
Outro Pessoal	1

No gráfico 15 é facilmente verificado que a esmagadora maioria se encaixa no Pessoal Médico:

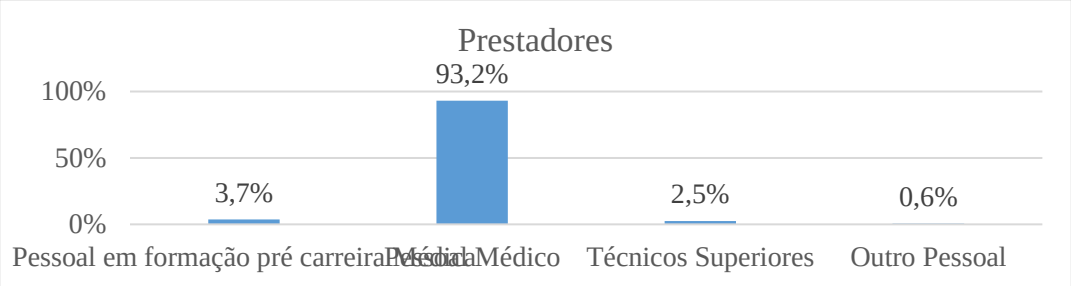


Gráfico 15 - Distribuição dos prestadores pelos grupos profissionais

A classe etária mais vulnerável foi entre 40 e 60 anos na primeira campanha, no entanto na segunda a classe foi entre 30 e 60 anos de idade.

Em termos de habilitações escolares a licenciatura foi efetivamente a mais destacada em vulnerabilidade, no entanto mais de 45 por cento dos funcionários têm esta formação e os funcionários com escolaridades inferiores ao 12 ano de escolaridade têm uma menor interação informática.

3. Preparação dos utilizadores para a análise pretendida

Uma vez que nunca tinha sido feito nada do sexo na instituição, foram enviados alguns e-mails com o intuído de sensibilizar sobre a questão de segurança e despertar os utilizadores para esta realidade.

Inicialmente foi abordada a questão do ransomware, uma vez que este malware utiliza como recurso o e-mail e já tinha sido alvo de ataque do WannaCry em tempos idos.

"Empresas e outras instituições em vários países, incluindo em Portugal, foram afetados por um vírus informático que inviabiliza a utilização de ficheiros e pede o pagamento de um valor para restabelecer o acesso. Em alguns casos, os computadores ficaram inoperacionais. Noutros, foram propositadamente desligados, para evitar mais danos." Pereia, J. P. (2017)

O ataque a instituições hospitalares é uma prática comum e no nosso Pais não é exceção, nem tão pouco coisa do passado, ou acontecimentos isolados. "Na última segunda-feira (25), o Hospital Garcia de Orta, em Lisboa, Portugal, sofreu um ataque cibernético que impactou todos os serviços da unidade hospitalar, exceto os atendimentos de urgência. A administração do hospital não deu muitos detalhes sobre o incidente, mas segundo o site de notícias CNN Portugal, houve um pedido de resgate por parte dos atacantes que provavelmente utilizaram um ransomware para o ataque. O Centro Nacional de Cibersegurança (CNCS) de Portugal está investigando o caso. De acordo com o portal SIC notícias, o hospital ainda não conseguiu restabelecido o funcionamento dos serviços e a unidade encontra-se com problemas para manter as consultas externas e exames.

Em paralelo a esse incidente, nesta última terça-feira (26), o Hospital do Litoral Alentejano, em Santiago do Cacém, também em Portugal, foi alvo de um ataque digital que acabou afetando a mais 5 outras unidades de saúde que pertencem ao mesmo complexo hospitalar: Alcácer do Sal, Grândola, Odemira, Santiago do Cacém e Sines. Todas as unidades tiveram dificuldade para manter o atendimento aos pacientes e houve a paralisação de alguns serviços." Camurça, F (2022)

4. Calendarização da tarefa

4.1. Inicialmente programada

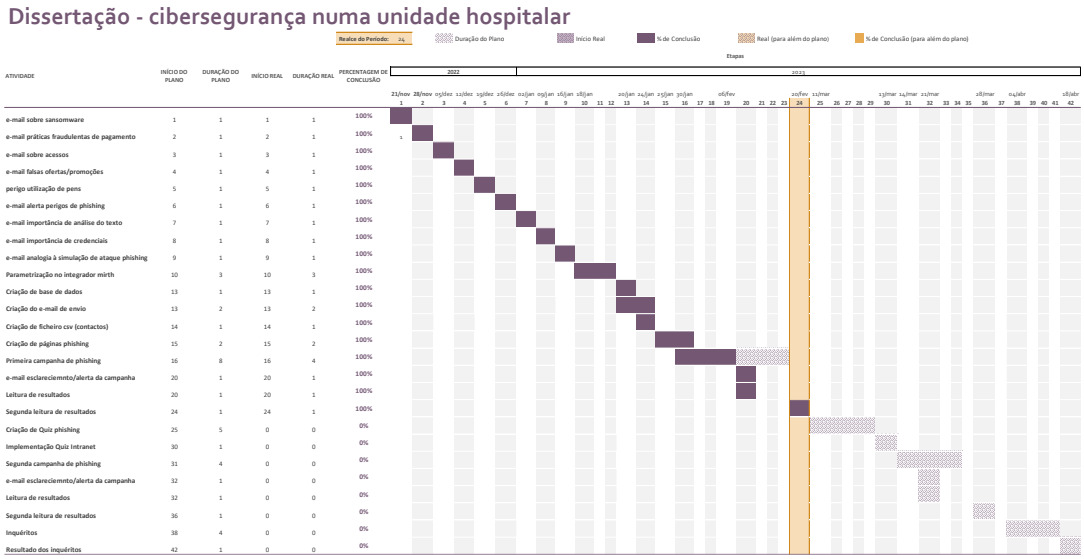


Figura 1 - calendarização de tarefas

4.2. Efetivamente implementada

4.2.1. Primeira campanha de phishing

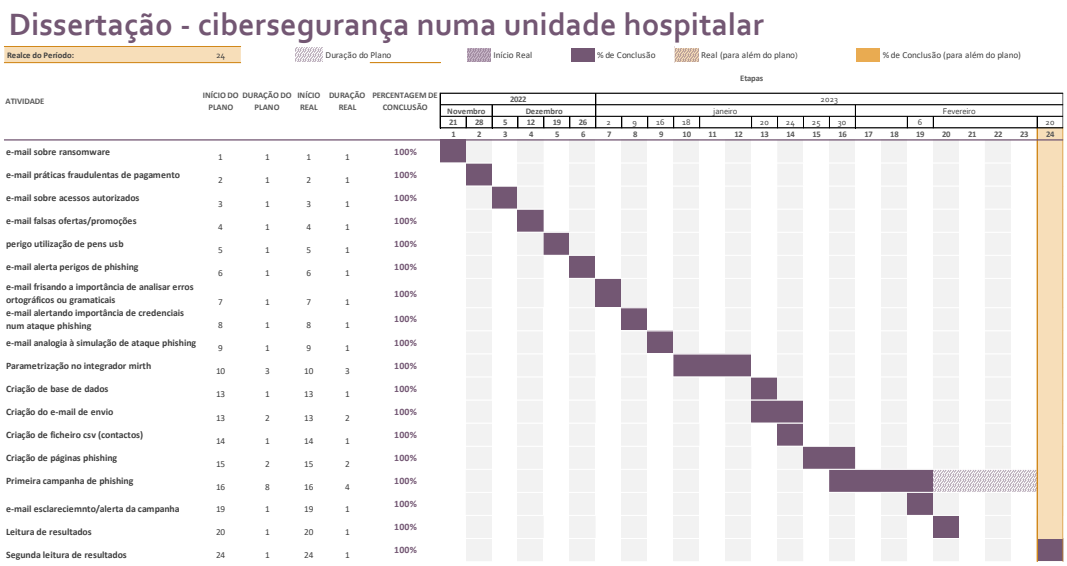


Figura 2- Calendarização da primeira campanha de phishing

4.2.2.Segunda campanha de phishing

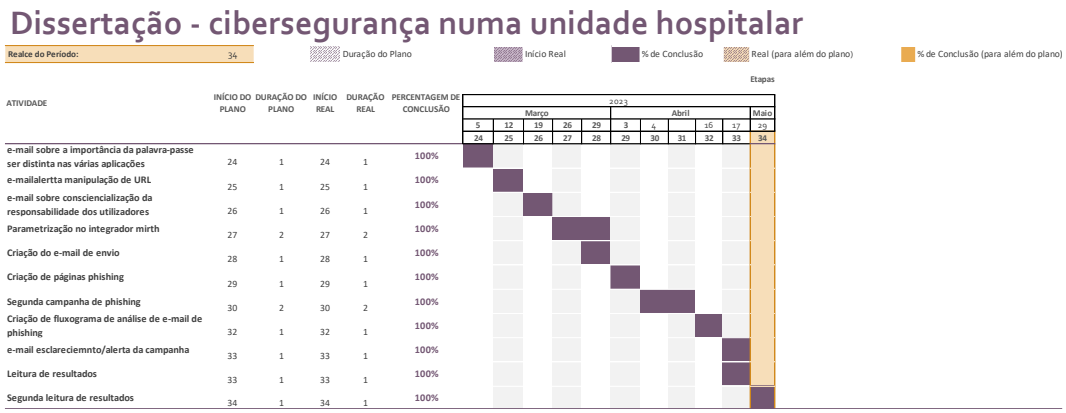


Figura 3 - Calendarização da segunda campanha de phishing

4.2.3.Quiz

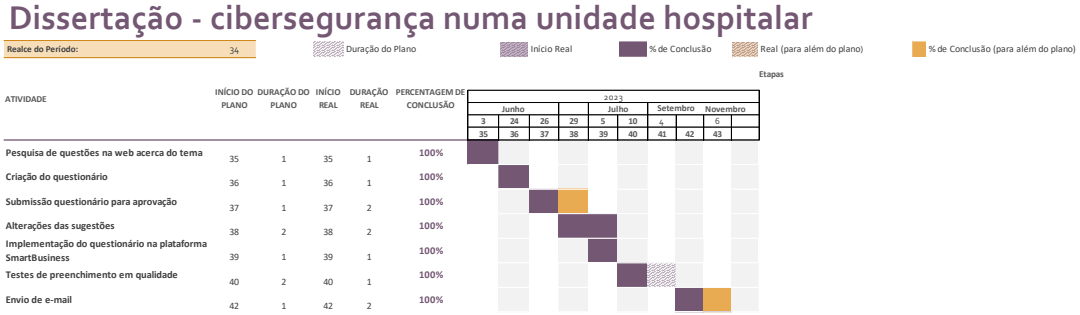


Figura 4- Calendarização do Quiz

4.2.4.Inquéritos

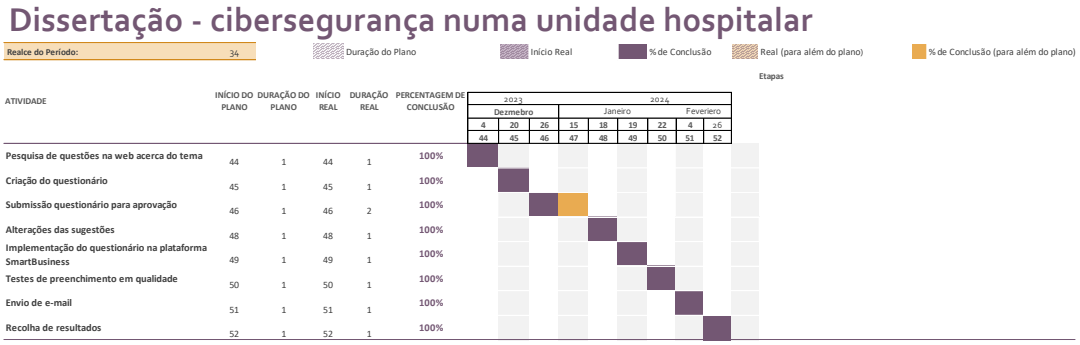


Figura 5- Calendarização do inquérito

5. Primeira campanha de phishing

5.1. Envio de e-mail de alerta sobre segurança

Foram enviados e-mails semanais, exemplo figura 6, com agendamento aos domingos, a todos os utilizadores alertando dos perigos maliciosos, com o objetivo de sensibilização sobre o tema.

Figura 6 - e-mail enviado alertando sobre um dos grandes perigos na internet ransomware

Outra forma de fraude e risco de sites maliciosos pode ser iniciada por companhas on-line, em conversa com alguns utilizadores da instituição alguns reportaram que tinham sido vítimas deste tipo de esquemas, que devido a preços aliciantes, quer em artigos de marca ou oferta de férias já tinham sido burlados, não obstante existe o perigo de utilizarem o e-mail institucional e eventualmente a mesma password utilizada na instituição para registo nestes sites. Neste sentido foram enviados os seguintes e-mails. Na figura 7, o e-mail alertava sobre pr´ticas fraudulentas de pagamentos

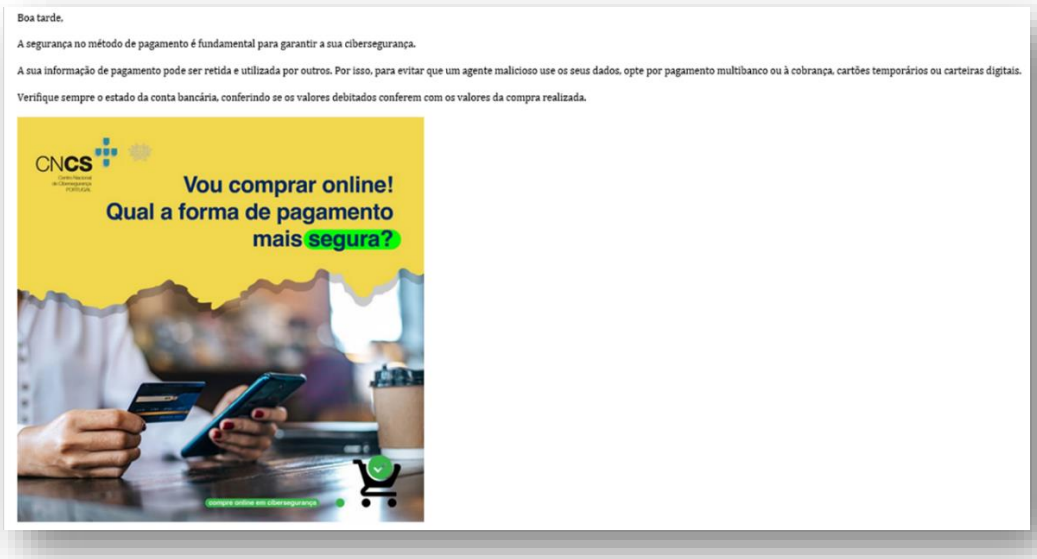


Figura 7 - e-mail alertando sobre práticas fraudulentas de pagamentos

A figura 8, alerta acerca das autorizações para acesso e instalações:

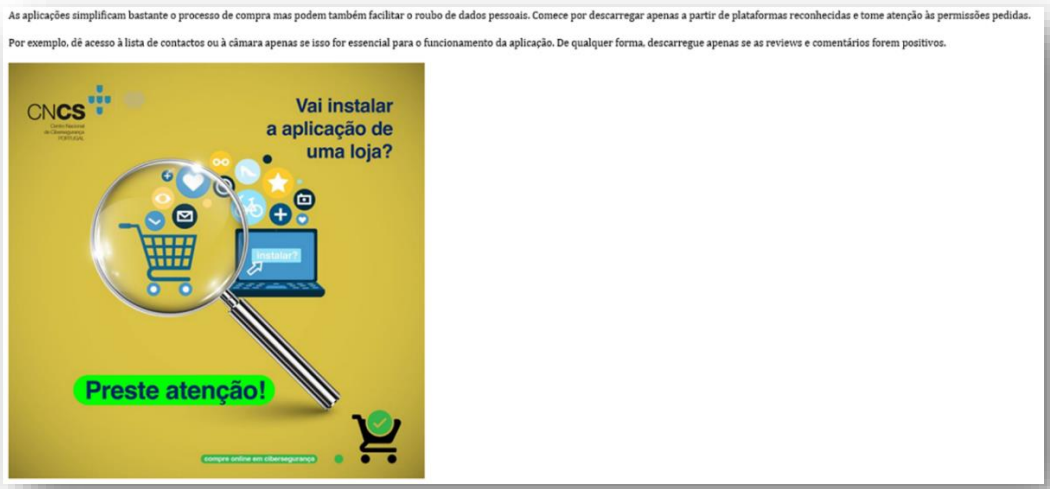


Figura 8 - e-mail acerca de acesso autorizados

A figura 9 alertava acerca de falsas ofertas ou promoções, que como será observado neste trabalho foi um dos recursos utilizados numa campanha de phishing

Figura 9 - email alertando para falsas ofertas ou promoções

Outra ameaça que está diretamente relacionada com vulnerabilidade por parte dos utilizadores é a utilização de dispositivos periféricos, nomeadamente pens que ao serem introduzidas nos equipamentos da instituição podem dar origem a ataques iniciados por estes meios. A figura 10, representa o e-mail enviado que teve o intuito de sensibilizar neste sentido.

Figura 10 - e-mail alertando para o perigo de utilização de pens usb

Após esta série de e-mail que foram enviados para todos os utilizadores com o intuito de despertar e sensibilizar os perigos numa ação ou reação menos refletida por parte dos destes optei por ser mais cirúrgico e enviar um e-mail que vai ao encontro dos cuidados a ter num ataque phishing, que será despoletado algum tempo depois deste e-mail, figura 11:

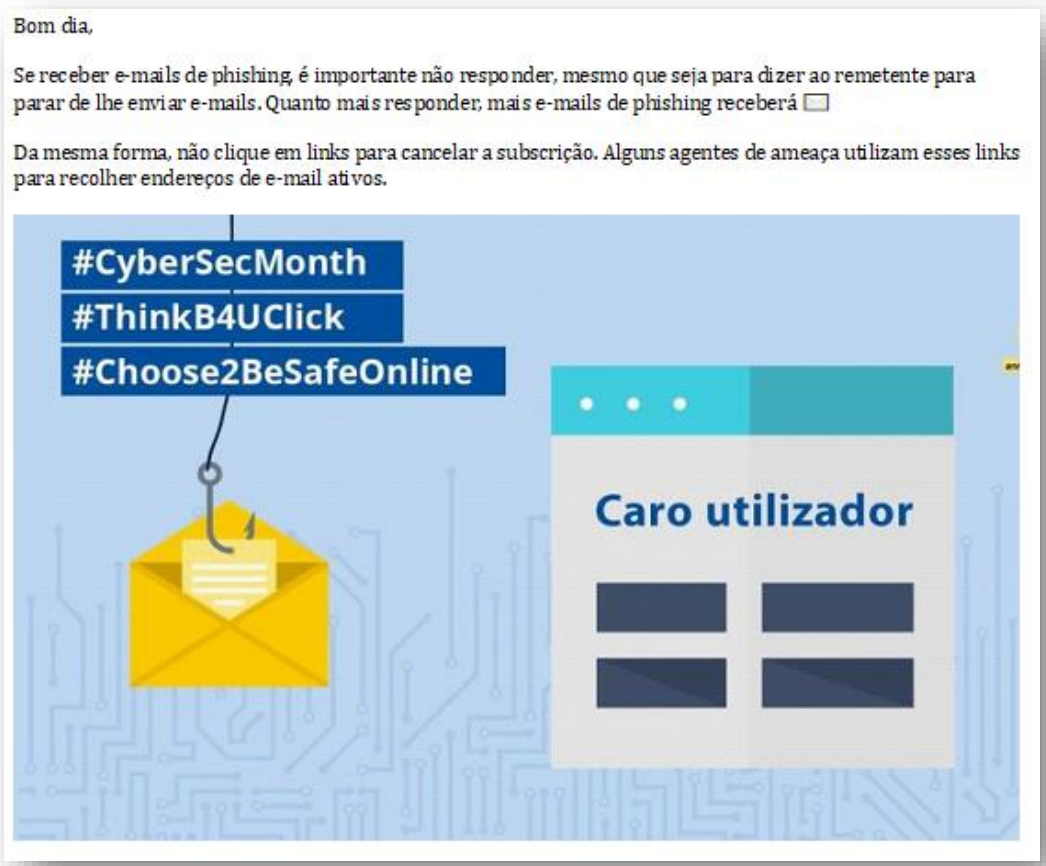


Figura 11 - e-mail alertar dos perigos do phishing

No ataque de simulação de phishing são introduzidos propositadamente erros ortográficos e previamente é enviado este e-mail, figura 12, a frisar a importância desta análise nos endereços de e-mail recebidos, assim como no corpo do e-mail e nos links ou anexos deste.

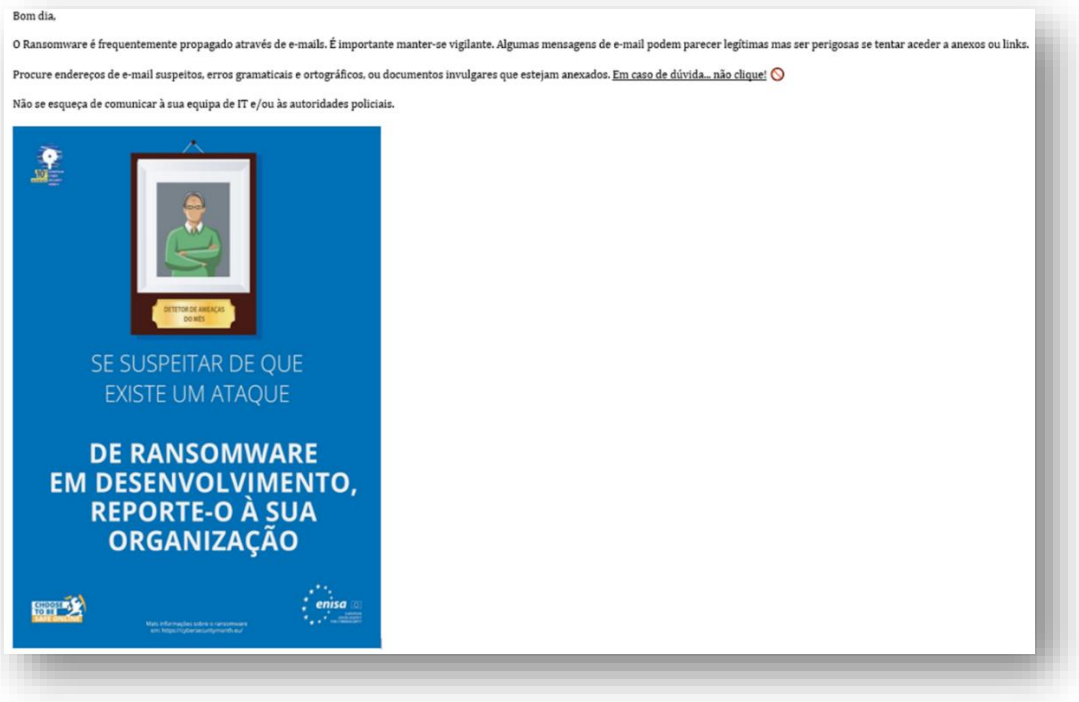


Figura 12 - e-mail frisando a importância de analisar erros ortográficos ou gramaticais

Na simulação que será realizada, haverá um link a solicitar a introdução do utilizador, ou seja, número mecanográfico e palavra-passe do utilizador, para despertar e sensibilizar neste sentido foi enviado o seguinte e-mail, figura 13:

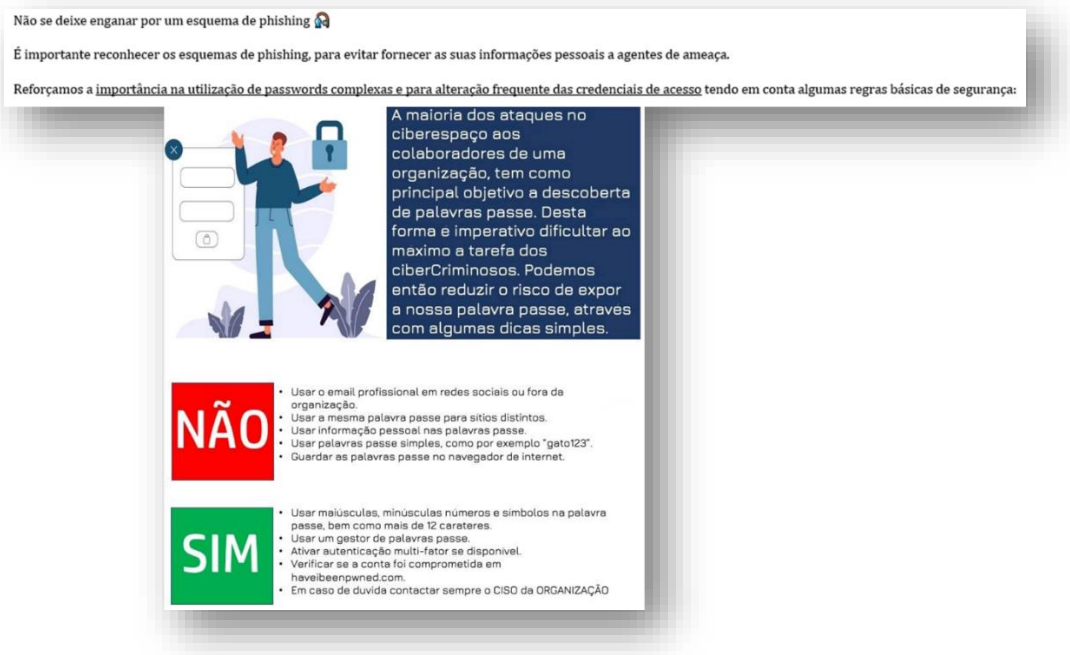


Figura 13 - e-mail alertando importância de credenciais num ataque phishing

Enviado e-mail, figura 14, com analogia ao que se pretende simular, alertando novamente para os links, erros ortográficos e gramaticais e a importância da não divulgação de credenciais de autenticação.

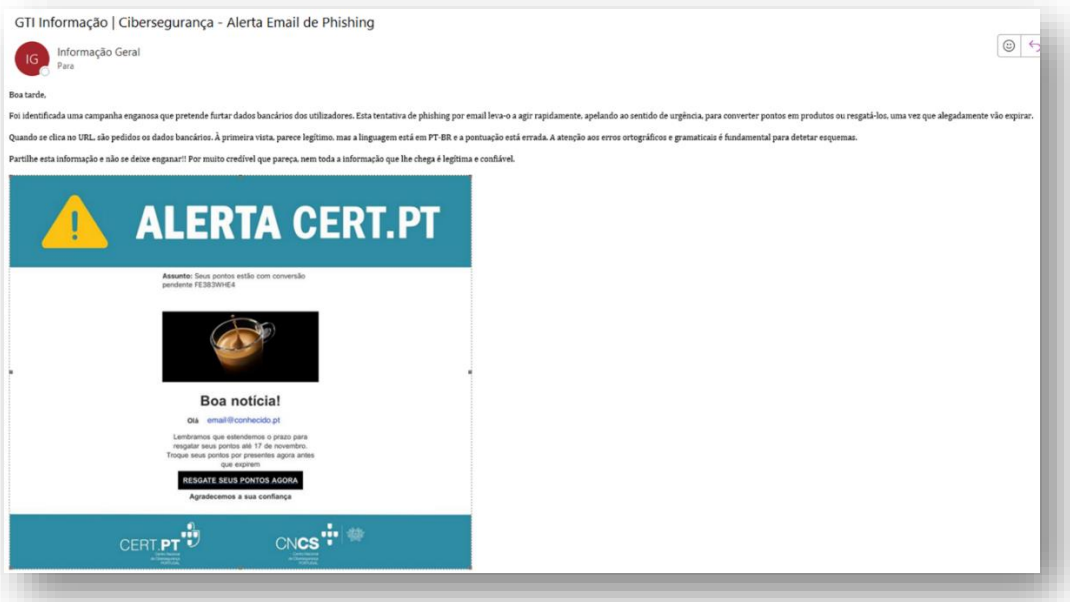


Figura 14 - e-mail com analogia à simulação de ataque phishing

Após o envio de 9 e-mails alertando e despertando para o perigo e o que identificar como suspeito nos e-mails recebidos, achei que estava na hora de iniciar a primeira simulação aos utilizadores da instituição.

5.2. Envio de e-mail de phishing:

Com recurso ao integrador "Mirth", que é o software de integração de dados de código aberto desenvolvido pela NextGen Healthcare e utilizado pelas instituições hospitalares portuguesas, permitindo que os dados sejam processados e roteados de maneira eficiente e segurança entre diferentes sistemas de saúde, nomeadamente com o integrador dos SPMS, Serviços Partilhados do Ministério da Saúde, que utiliza HL7, foi configurado o envio de e-mail para todos os endereços de e-mail da instituição, figura 15.

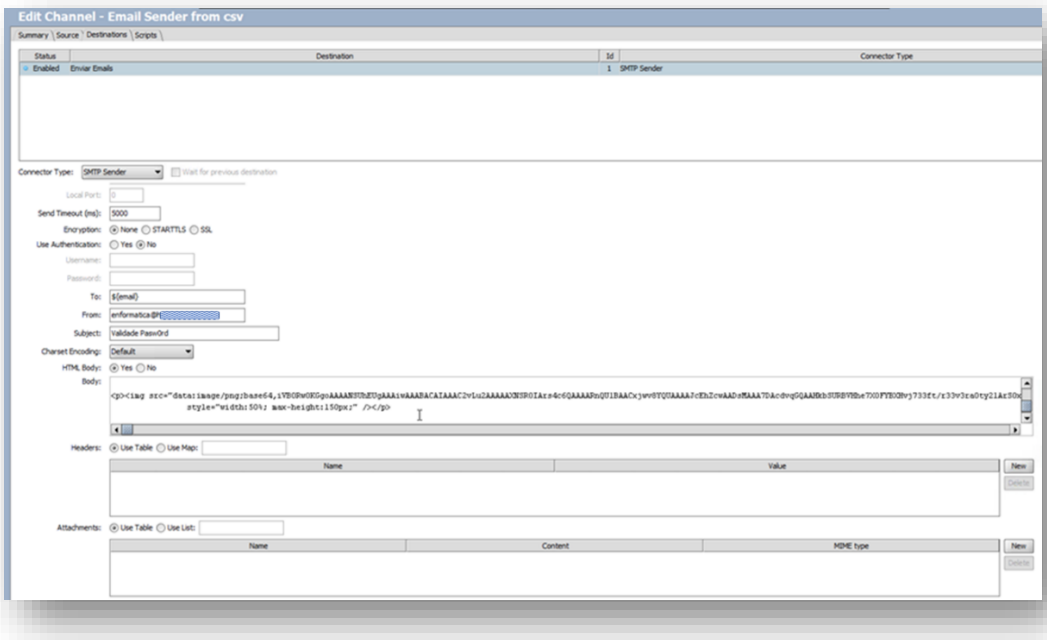


Figura 15 - Parametrização de envio de e-mail através do integrador Mirth

O corpo do e-mail em html, figura 16 a 19, foi a forma de construção da página, links e registo de credenciais na interação com o utilizador:

```
<p>Boa tarde,</p>

<p>Pelo facto de vários utilizadores terem manifestado desagrado pela constante necessidade de revalidaçao da password, deverá responder ao seguinte formulário:</p>

<p>Deve se dirigir ao site seguro e atualizar:</p>

<p><a href="http://172.16.254.55:9294/getpage?u=${nmec}">Formulário HDB</a></p>
<p>Obrigado pela colaboração,
</br>
Departamento de Enformática
</p>
```

Figura 16 – código corpo do e-mail enviado

```
var decoded = FileUtil.decode(data);

var fileName = "temp.jpg";

FileUtil.write(fileName, false, decoded);

/*

<td style="height: 83px;border -right: 0px solid #000000;" width="132"><img
style="height:40px;max -width:50px" src="temp.jpg"></img></td>

*/

var page = (<r><![CDATA[

<!DOCTYPE html>

<html>

<head>

  <title>HDS - Hospital Distrital de              </title>

</head>

<body style="font -family:Arial, Helvetica, sans -serif ;">

  <div style="width: 600px;margin: auto;">

    <div style=" text -align: center;">

      <img src="http://intgmirth.      .min -saude.pt:8080/SB/LOGO_       _2.1.png"

        style="width:50%; max -height:150px;" />

    </div>

    <div style="width: 640px;margin:10px auto;">

      <p style=" text -align: center;">

        Pelo facto de vários utilizadores terem manifestado desagrado pela constante
necessidade de revalidaçao da password, a informática pretende saber se a sua password
deverá manter a revalidação atu al ou a mesma não deverá expirar.

      </p>

      <p style=" text -align: center;">

       <u> <strong>Deverá selecionar uma das seguintes opções </strong> </u>          </p>

      <form method="POST" action="/submit">

        <input type="checkbox" id="checkbox1" name="checkbox1">

        <label for="checkbox1">Pretendo manter o prazo de renovação da minha
password</label><br>

        <input type="checkbox" id="checkbox2" name="checkbox2">
```

Figura 17 – código página inicial phishing 1/2

```
<label for="checkbox2">Pretendo que a minha password nunca expire</label><br>
            <input type="checkbox" id="checkbox3" name="checkbox3">
            <label for="checkbox3">É indiferente</label><br>
            <p>
              <label for="fname">Utilizador:</label><br>
              <input type="text" id="fname" name="fname" required>
            </p>
            <p>
              <label for="unewpass">Nova Password:</label><br>
              <input type="password" id="unewpass" name="unewpass" required>
            </p>
            <p>
              <input type="submit" value="Submeter" style="background-color: #04AA6D;color:
white">
            </p>
          </form>
        </div>
        <div style="width: 100%; margin:10px auto">
          <div>
                <a href="https://spms.min-saude.pt/" target="_blank"
              title="Clique para ir para o portal da SPMS. Abre num novo separador."><img
                src="http://intgmirth.      .min-saude.pt:8080/SB/f                png"
                alt="SPMS"></a>
          </div>
        </div>
    </div>
</body>
</html>
 ]]></r>).toString();
//https://www.portugal.gov.pt/upload/imagens/i047265.jpg
//https://www.inem.pt/wp-content/uploads/2019/03/Evolu%C3%A7%C3%A3o-dos-RH-no-
SNS.jpg
```

Figura 18 código página inicial de phishing 2/2

Submissão de phishing:

```
var page = (<r><![CDATA[
<!DOCTYPE html>
<html>
<head>
        le>HDS - Hospital Distrital de                  </title>
</head>
<body style="font-family:Arial, Helvetica, sans-serif ;">
   <div style="width: 600px;margin: auto;">
      <div style=" text-align: center;">
         <img src="http://intgmirth.XXX.min-saude.pt:8080/SB/LOGO_HDS_2.1.png"
            style="width:50%; max-height:150px;" />
      </div>
      <div style="width: 640px;margin:10px auto;">
         <p style=" text-align: center;">
          <u> <strong>Obrigado </strong> </u>          </p>
      </div>
      <div style="width: 100%; margin:10px auto">
         <div>
                  <a href="https://spms.min-saude.pt/" target="_blank"
               title="Clique para ir para o portal da SPMS. Abre num novo separador."><img
                  src="http:            rth.hds.min-saude.pt:808            terHDS.png"
                  alt="SPMS"></a>
         </div>
      </div>
   </div>
</body>
</html>
 ]]></r>).toString();
channelMap.put('html',page);
```

Figura 19 – código página após submissão de phishing

Foram inseridos vários tipos de pistas que permitiam identificar o e-mail rececionado como falso:

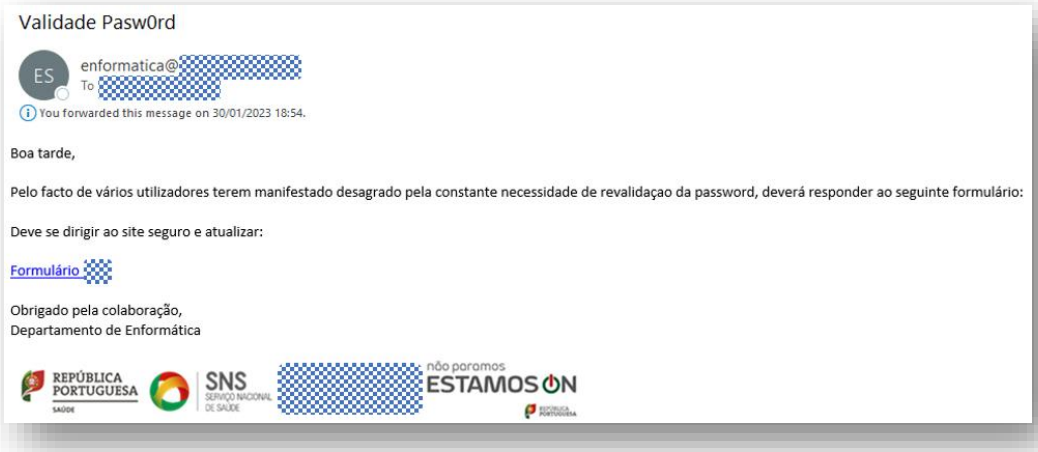


Figura 20- e-mail de phishing enviado

A figura 20, representa o e-mail rececionado pelos utilizadores onde solicitava o clicar para abertura de nova página para introdução e registo de credenciais. Na eventualidade do utilizador clicar no link, era registado numa base de dados, como tinha clicado e era redirecionado para a seguinte página, figura 21:

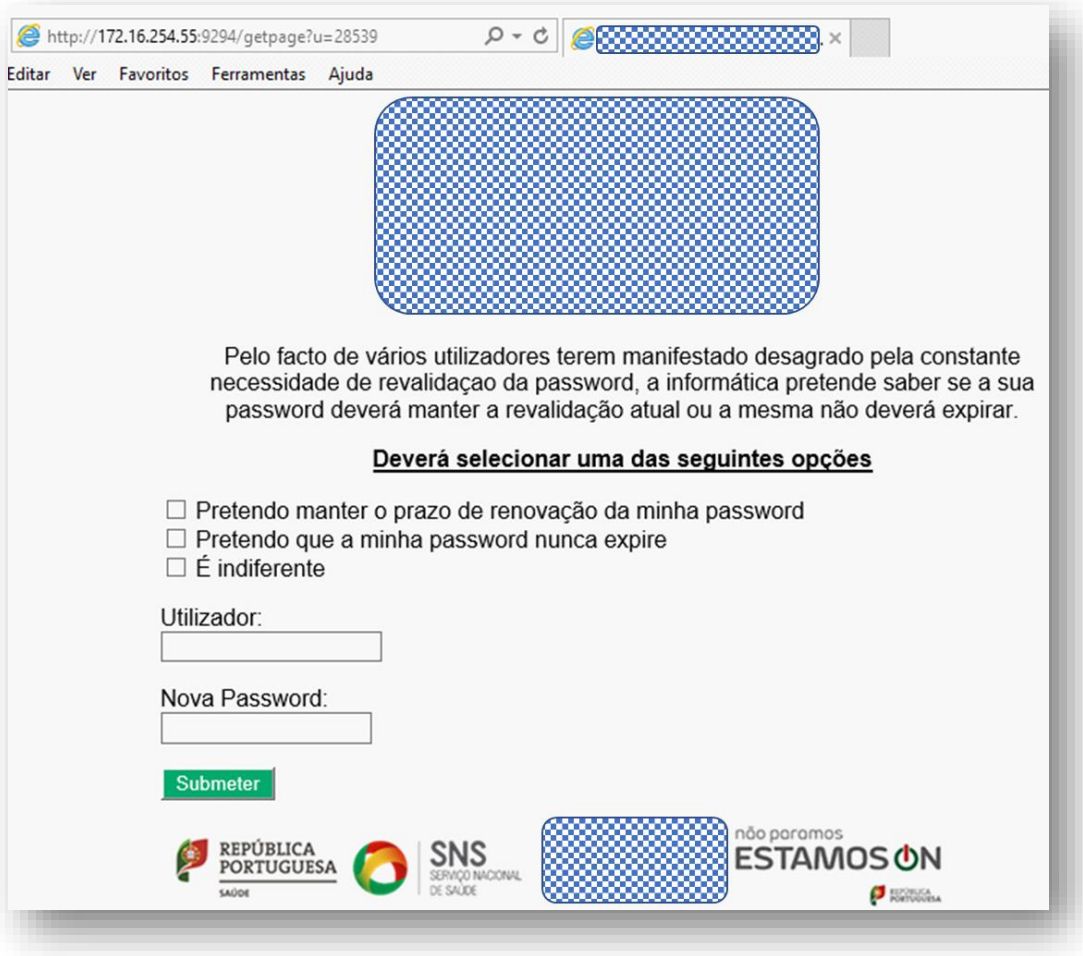


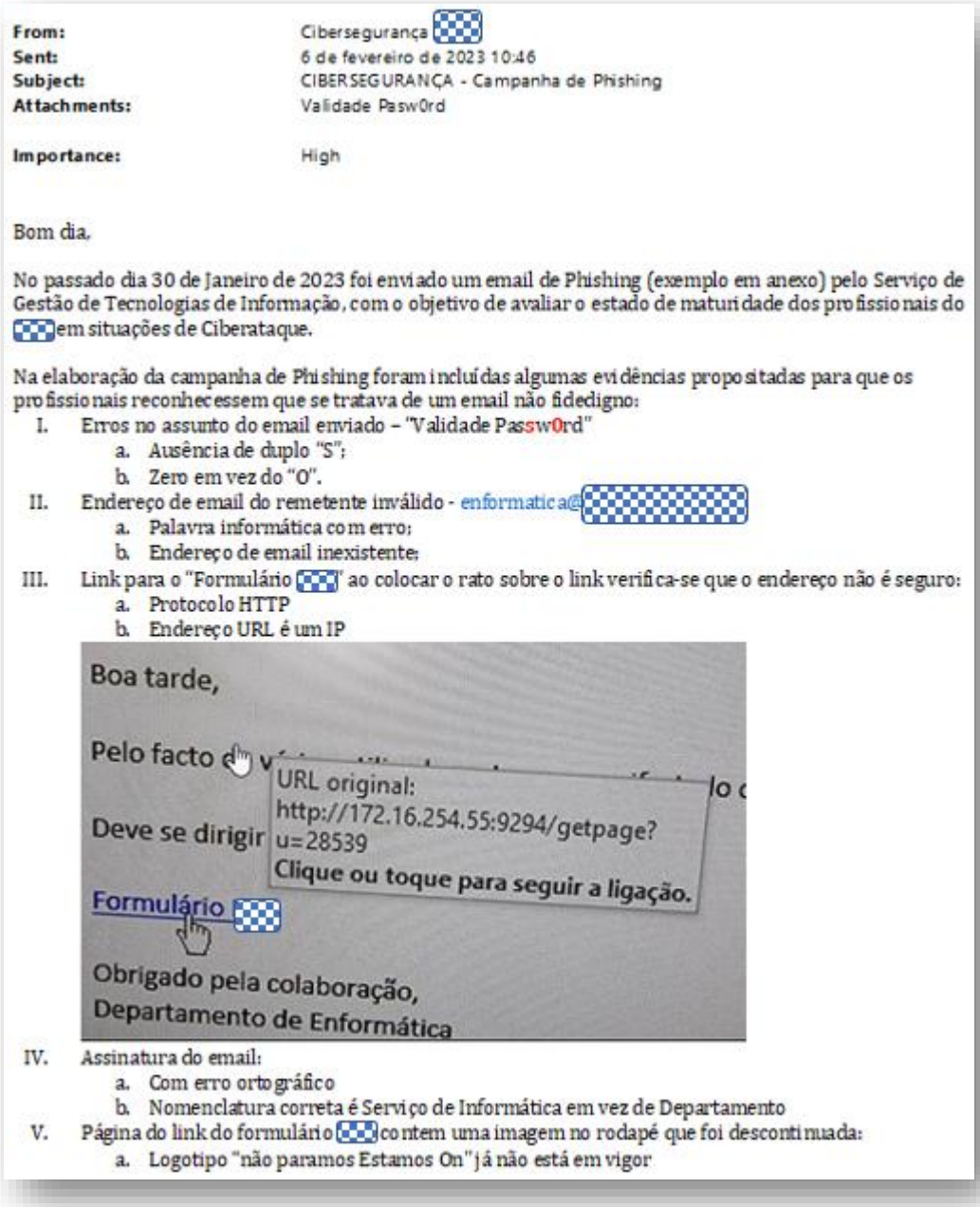
Figura 21 - página inicial de phishing

Ao submeter eram registadas as credenciais numa base de dados sql e apresentada a seguinte página, figura 22:

Figura 22 - página após submissão de credenciais

5.3. Envio de e-mail a esclarecer toda a situação, para todos os utilizadores:

Após o decorrer da campanha foi enviado e-mail a todos os utilizadores, figura 23 a 25 para esclarecer a situação:



From: Cibersegurança
Sent: 6 de fevereiro de 2023 10:46
Subject: CIBERSEGURANÇA - Campanha de Phishing
Attachments: Validade Pasw0rd

Importance: High

Bom dia,

No passado dia 30 de Janeiro de 2023 foi enviado um email de Phishing (exemplo em anexo) pelo Serviço de Gestão de Tecnologias de Informação, com o objetivo de avaliar o estado de maturidade dos profissionais do em situações de Ciberataque.

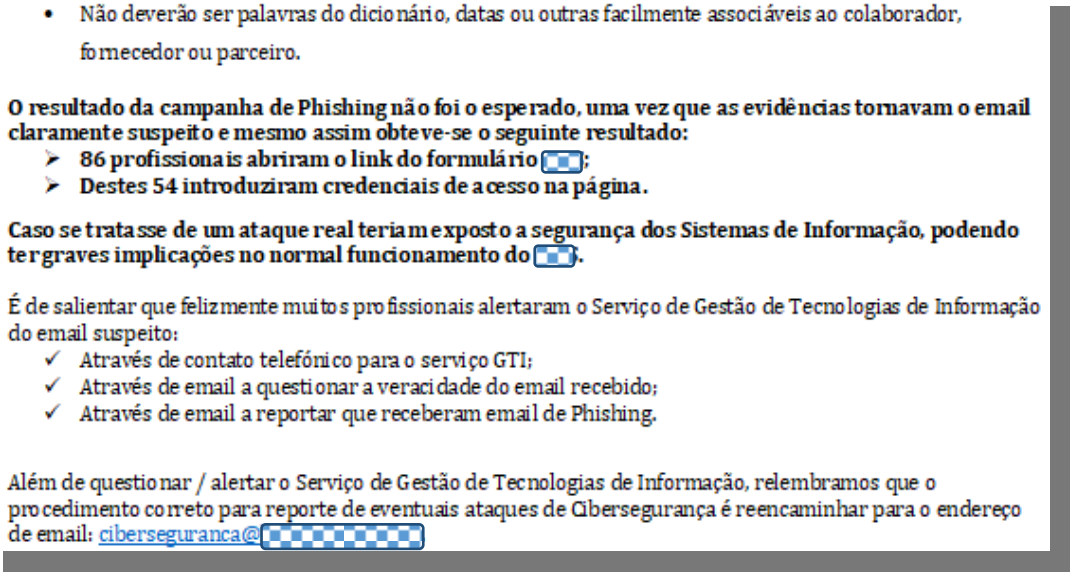
Na elaboração da campanha de Phishing foram incluídas algumas evidências propositadas para que os profissionais reconhecessem que se tratava de um email não fidedigno:

I. Erros no assunto do email enviado – "Validade Passw0rd"
   a. Ausência de duplo "S";
   b. Zero em vez do "O".
II. Endereço de email do remetente inválido - enformatica@
   a. Palavra informática com erro;
   b. Endereço de email inexistente;
III. Link para o "Formulário" ao colocar o rato sobre o link verifica-se que o endereço não é seguro:
   a. Protocolo HTTP
   b. Endereço URL é um IP

IV. Assinatura do email:
   a. Com erro ortográfico
   b. Nomenclatura correta é Serviço de Informática em vez de Departamento
V. Página do link do formulário contem uma imagem no rodapé que foi descontinuada:
   a. Logotipo "não paramos Estamos On" já não está em vigor

Figura 23 - e-mail de esclarecimento 1ª campanha 1/3

Figura 24 - e-mail de esclarecimento 1ª campanha 2/3



- Não deverão ser palavras do dicionário, datas ou outras facilmente associáveis ao colaborador, fornecedor ou parceiro.

O resultado da campanha de Phishing não foi o esperado, uma vez que as evidências tornavam o email claramente suspeito e mesmo assim obteve-se o seguinte resultado:

- **86 profissionais abriram o link do formulário [redacted];**
- **Destes 54 introduziram credenciais de acesso na página.**

Caso se tratasse de um ataque real teriam exposto a segurança dos Sistemas de Informação, podendo ter graves implicações no normal funcionamento do [redacted].

É de salientar que felizmente muitos profissionais alertaram o Serviço de Gestão de Tecnologias de Informação do email suspeito:

- ✓ Através de contato telefónico para o serviço GTI;
- ✓ Através de email a questionar a veracidade do email recebido;
- ✓ Através de email a reportar que receberam email de Phishing.

Além de questionar / alertar o Serviço de Gestão de Tecnologias de Informação, relembramos que o procedimento correto para reporte de eventuais ataques de Cibersegurança é reencaminhar para o endereço de email: cibersegurança@[redacted]

Figura 25 - e-mail de esclarecimento 1ª campanha 3/3

6. Segunda campanha de phishing

6.1. Envio de e-mails alertando novamente para os perigos de ataques

A figura 26, representa o e-mail enviado novamente a todos os utilizadores, neste caso específico salientando a importância de diversificação de passwords.

Figura 26 - Importância da palavra-passe ser distinta nas várias aplicações

Na figura 27, foi alertada a situação dos endereços das páginas e dos links, é frequente esta técnica nos e-mails de phishing.

Figura 27 - Alerta de manipulação de URL

A figura 28, foi o e-mail que pretende sensibilizar que todos têm um papel importante e é crucial termos todos consciência dos perigos e responsabilidade sobre as nossas ações.

Figura 28 - consciencialização da responsabilidade dos utilizadores

6.2. Envio de e-mail de phishing

À semelhança da primeira campanha foi utilizado o Mirth para envio de um segundo e-mail de phishing, figura 29, para todos os utilizadores:

Figura 29 - Segundo e-mail de phishing

Ao selecionar “Reservar Ingresso” o utilizador era redirecionado para um URL, figura 30,“http://172.16.254.55:9294/getpage1?u=”Número mecanográfico”

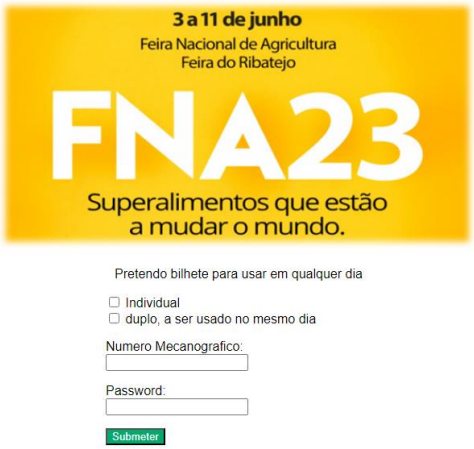


Figura 30 - Página de inscrição, falsa

Foi ainda salvaguardada a impossibilidade de submeter sem preenchimento dos campos, figura 31:

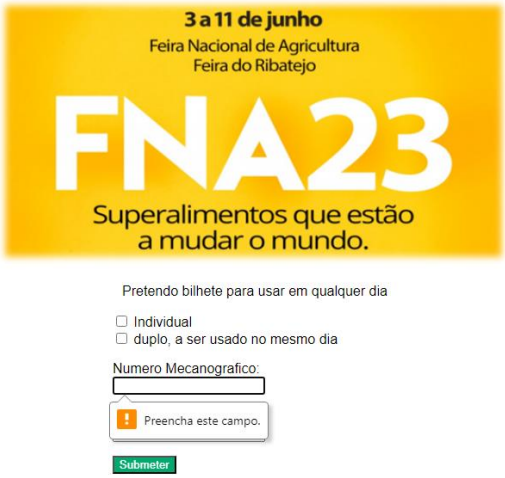


Figura 31 - Obrigatoriedade de preenchimento dos campos

No preenchimento não havia match entre a password introduzida e a do utilizador, o campo só obrigava a preencher, após a submissão do formulário, era apresentada uma mensagem de agradecimento pela participação, figura 32:

Figura 32 - Mensagem de agradecimento pela participação

6.3. Elaboração de fluxograma de análise de e-mails de phishing

Foi criado um fluxograma, figura 33, com o intuito de ajudar os utilizadores na interpretação de dúvidas nos e-mails rececionados:

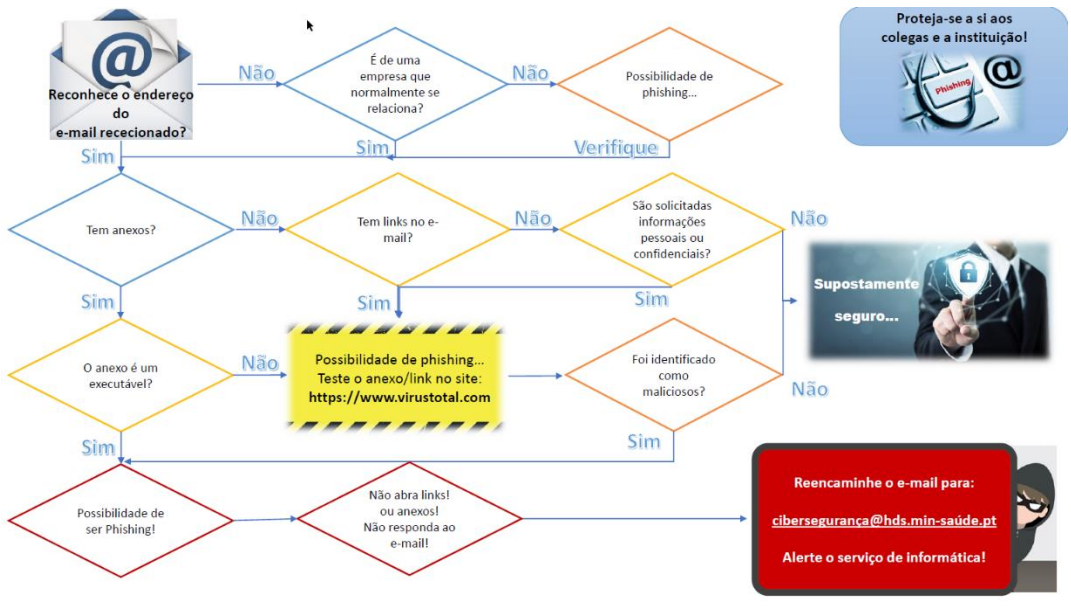
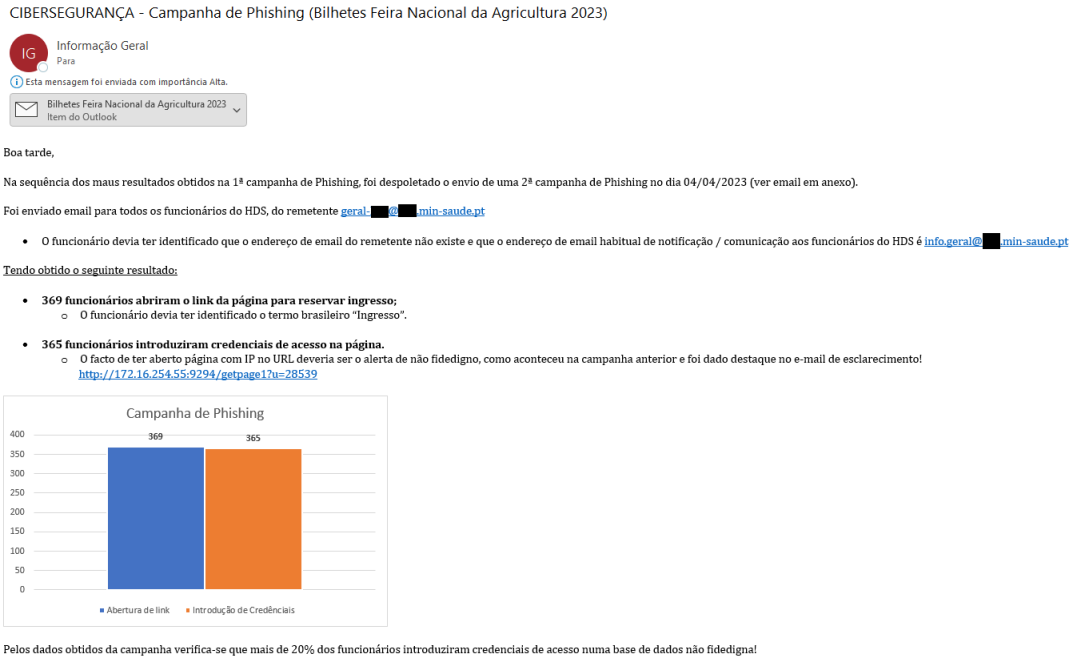


Figura 33 - Fluxograma de análise de e-mail de phishing

6.4. Envio de e-mail a esclarecer toda a situação, para todos os utilizadores:

Na figura 34 a 37 está representado o e-mail enviado a todos os utilizadores esclarecendo acerca da segunda campanha de phishing que decorreu na instituição:



CIBERSEGURANÇA - Campanha de Phishing (Bilhetes Feira Nacional da Agricultura 2023)

IG Informação Geral
Para
Esta mensagem foi enviada com importância Alta.
Bilhetes Feira Nacional da Agricultura 2023
Item do Outlook

Boa tarde,

Na sequência dos maus resultados obtidos na 1ª campanha de Phishing, foi despoletado o envio de uma 2ª campanha de Phishing no dia 04/04/2023 (ver email em anexo).

Foi enviado email para todos os funcionários do HDS, do remetente geral[redacted]@[redacted].min-saude.pt

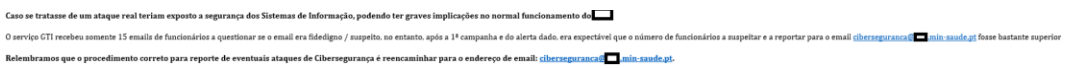
- O funcionário devia ter identificado que o endereço de email do remetente não existe e que o endereço de email habitual de notificação / comunicação aos funcionários do HDS é info.geral@[redacted].min-saude.pt

Tendo obtido o seguinte resultado:

- **369 funcionários abriram o link da página para reservar ingresso;**
  - O funcionário devia ter identificado o termo brasileiro "Ingresso".
- **365 funcionários introduziram credenciais de acesso na página.**
  - O facto de ter aberto página com IP no URL deveria ser o alerta de não fidedigno, como aconteceu na campanha anterior e foi dado destaque no e-mail de esclarecimento! http://172.16.254.55:9294/getpage1?u=28539

Pelos dados obtidos da campanha verifica-se que mais de 20% dos funcionários introduziram credenciais de acesso numa base de dados não fidedigna!

Figura 34 - e-mail de esclarecimento 2ª campanha 1/4



Caso se tratasse de um ataque real teriam exposto a segurança dos Sistemas de Informação, podendo ter graves implicações no normal funcionamento do[redacted]

O serviço GTI recebeu somente 15 emails de funcionários a questionar se o email era fidedigno / suspeito, no entanto, após a 1ª campanha e do alerta dado, era expectável que o número de funcionários a suspeitar e a reportar para o email cibersegurança@[redacted].min-saude.pt fosse bastante superior

Relembramos que o procedimento correto para reporte de eventuais ataques de Cibersegurança é reencaminhar para o endereço de email: cibersegurança@[redacted].min-saude.pt.

Figura 35 - e-mail de esclarecimento 2ª campanha 2/4

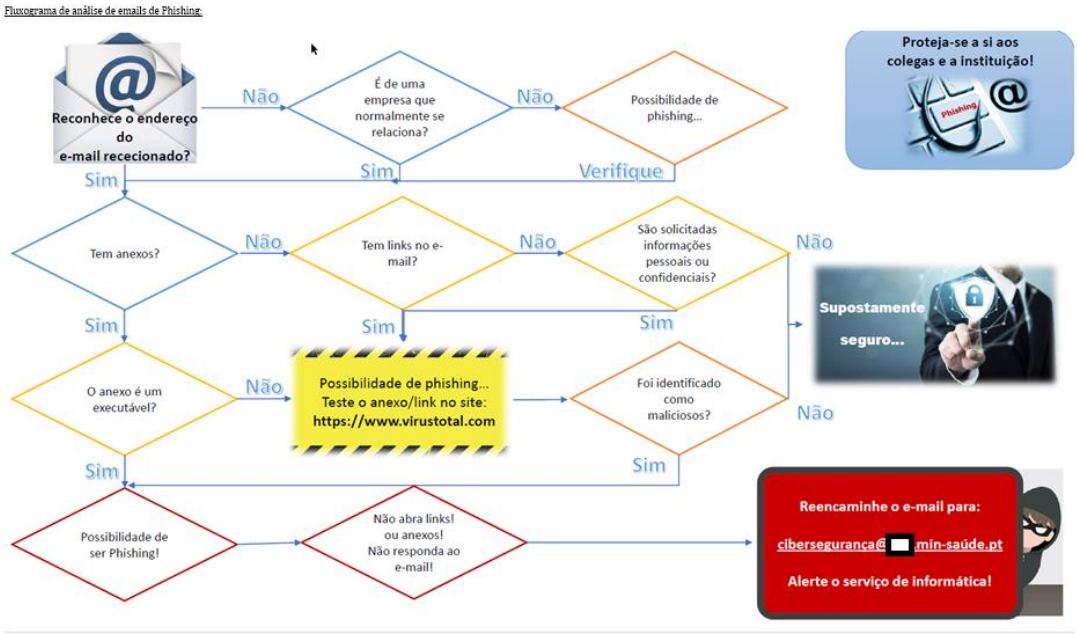


Figura 36 - e-mail de esclarecimento 2ª campanha 3/4

Figura 37 - e-mail de esclarecimento 2ª campanha 4/4

7. QUIZ – (e-learning)

Com recurso ao SB utilizado na instituição, dei início à implementação de um quiz, com o objetivo de ajudar os utilizadores e em simultâneo aumentar o conhecimento de empenho e resultados da interação dos utilizadores com o mesmo.

7.1. Criação de quiz teve como base alguns temas que determinaram a elaboração por segmentos, nomeadamente:

7.1.1. Download de ficheiros

Por ter consciência que os downloads de ficheiros estão acessíveis e são portas de entrada para malware, achei um tema importante a abordar:

1. Os ficheiros que fazemos download da internet podem abrir o nosso computador a terceiros
   a. Verdadeiro
   b. Falso

2. As redes Peer to Peer são utilizadas para:
   a. Download de filmes
   b. Download de música
   c. Dessiminação de Malware
   d. Todas as anteriores

3. Que tipo de websites usualmente contém Malware?
   a. Sites de notícias
   b. Sites de pornografia
   c. Sites de pirataria
   d. Todas as anteriores

4. Uma forma adequada de executar ficheiros duvidosos é executá-los em ambientes isolados ou virtualizados

a. Verdadeiro

b. Falso

5. Os atacantes usualmente mudam o nome dos ficheiros ou as extensões para disfarçá-los de ficheiros fidedignos?

a. Nomes

b. Extensões

7.1.2. Navegação Segura com Web Browser

Na prática a abordagem do browser não foi assumida pela vulnerabilidade de utilização na instituição, uma vez que as atualizações são geridas pelo serviço de GTI, mas os utilizadores podem aceder remotamente à instituição através de browser e neste sentido é importante a sensibilização na utilização do mesmo.

1. O Navegador é a ferramenta que usa para navegar na Internet. O que pode fazer para mantê-lo mais seguro?
    a. Atualiza-lo sempre que solicitado
    b. Usar diferentes navegadores no mesmo computador
    c. Fechá-lo se não estiver a usar
    d. Todas as anteriores

2. Porque devem ser evitados sites com alguns tipos de conteúdos (pornografia, aplicações gratuitas, cracks, etc.)?
    a. Porque é ilegal
    b. Porque pode conter "*malware*" e infetar o computador
    c. Porque é preciso autenticação
    d. Por nenhuma das razões anteriores

3. Porque devem ser limpos os cookies regularmente ou sempre que utilize um computador público?

a. Para não encher o disco com informação
b. Porque possuem informação sobre as minhas sessões e pode ser usado para me comprometer
c. Não é necessário apagar os cookies nunca
d. Para manter as sessões anónimas

4. Quando estou perante uma página que permite a transação segura dos dados, o url deverá começar por:
   a. HTTP
   b. FTP
   c. SSL
   d. HTTPS

5. O antivírus é uma ferramenta que garante total segurança do meu computador
   a. Verdadeiro
   b. Falso

7.1.3. Palavras-passe e Controlo de Acessos

Pela importância e vulnerabilidade que pode causar os acessos aos sistemas por hackers e também pelos resultados obtidos nas simulações das campanhas de phishing a presença deste tema seria imprescindível no quis.

1. Quais as características de uma palavra-passe forte?

a. 8 ou mais caracteres e Letras maiúsculas e minúsculas

b. Números e Letras

c. Caracteres especiais

d. 8 ou mais caracteres, letras maiúsculas e minúsculas, números e caracteres especiais

2. Qual, das seguintes palavras-passe, é mais usada e consequentemente a mais fraca?

a. Qwerty

b. IloveYou

c. 123456

d. LetMeIn

3. Qual a dimensão máxima aconselhada para uma palavra-passe

a. 8 caracteres

b. 15 caracteres

c. O maior possível

d. Não é importante

4. Uma palavra-passe forte é difícil de recordar. O que pode ser feito para não esquecer?

a. Usar mnemónicas

b. A partir de uma frase com significado, criar uma palavra-passe

c. Guardar de um modo seguro (cifrado)

d. Todas as técnicas anteriores

5. Se já tenho uma palavra-passe forte, posso usá-la durante anos. Verdadeiro ou Falso?

a. Verdadeiro

b. Falso

7.1.4. Redes Sociais

O crescimento da oferta de redes sociais e da quantidade de tempo que os utilizadores dedicam às mesmas, deve ser um tema preocupante a abordar na segurança da informação.

1. Nunca Partilhe as suas credenciais sem ter a certeza que está a fazer login no website correto.

   Qual a afirmação correta?

a. Não existe perigo desde que esteja conectado numa rede Wi-Fi conhecida ou com os dados móveis

b. Desde que aceda através do meu login do Facebook não corro esse risco

c. Os responsáveis por fraudes podem criar sites falsos semelhantes aos das redes sociais e pedir-lhe para iniciar a sessão e colocar o seu login e palavra-passe.

d. Se for com amigos do Instagram não corro esse perigo

2. Nunca clique em links suspeitos, mesmo que pareça vir de alguém que conhece. Qual a afirmação correta?

a. Isso incluí ligações em qualquer rede ou até em emails.

b. Nas redes sociais não existe esse risco

c. Só é arriscado se for através de e-mail

d. Se for da minha lista de amigos não tem problema

3. Não aceite pedidos de amizade de pessoas que na realidade não conhece. Ao se tornar amigo desse tipo de pessoas está a permitir que eles enviem spam para a sua cronologia, que o identifiquem ou até possam enviar

mensagens maliciosas para si ou para os seus contatos. Nunca clique em links suspeitos, mesmo que pareça vir de alguém que conhece. Qual a afirmação correta?

a. Nas redes sociais não existe esse risco

b. Se reconhecer o nome aceito, porque conheço o meu amigo, desse modo não aceito estranhos

c. Só aceito pedidos de amizade que conheço a pessoa pela foto, logo não tem risco aceitar conhecidos

d. Um esquema comum de fraude é criar contas para adicionar pessoas.

4. Devo terminar sempre a sessão quando utilizar um computador partilhado?
Qual a afirmação correta?

a. Nas redes sociais não existe esse risco

b. Eventualmente posso me esquecer, mas geralmente termino, por isso não é grave

c. Fecho sempre o browser, por isso não necessito de terminar sessão, porque a conta fica protegida

d. A sessão deverá ser sempre terminada

5. Porque devem ser usados grupos privados nas redes sociais?

Escolha a afirmação correta.

a. Para não incomodar os restantes utilizadores

b. Para garantir que informação privada não seja divulgada por terceiros

c. Porque é a única maneira de partilhar informação

d. Todas as afirmações anteriores são verdadeiras

6. Quais os dados que não devem ser colocados numa publicação de uma rede social? Escolha todas as opções que considere corretas

a. A localização atual

b. A morada de casa

c. Uma foto com amigos

d. Um título de um livro

7. Que tipo de pessoas podem ser encontradas nas redes sociais?

a. Artistas

b. Amigos

c. Criminosos

d. Todos os anteriores

7.1.5. Segurança em Dispositivos Móveis

Os dispositivos móveis fazem parte do nosso cotidiano e muitos utilizadores acabam por armazenar palavras-passe e informações pessoais nos mesmos, dai achar pertinente abordar também esta fonte de risco:

1. Porque deve ser utilizado um código de bloqueio?

a. Porque se o dispositivo for roubado, o atacante não conseguirá aceder aos conteúdos

b. Para impedir a entrada de Vírus no dispositivo

c. Porque se o dispositivo for roubado, os dados serão autodestruídos

d. Para impedir a instalação automática de aplicações

2. Porque não devemos instalar aplicações de lojas não oficiais?

a. Porque são pagas

b. Porque ocupam mais espaço no dispositivo

c. Porque é um risco de segurança alto

d. Porque não conhecemos a origem

3. Devem ser instaladas sempre as últimas atualizações de segurança, quer do sistema, quer das aplicações.

a. Verdadeiro

b. Falso

4. Porque devem ser validadas as permissões das aplicações instaladas?

a. Porque o fabricante assim o exige

b. Para validar se são em excesso

c. Para validar se colocam em causa a segurança dos dados

d. Todas as anteriores

5. O dispositivo deve ter sempre ligadas as redes wi-fi e Bluetooth.

a. Verdadeiro

b. Falso

7.1.6. Rasomware

Pelo facto da própria instituição já ter sido no passado vítima deste tipo de ataque achei importante incluir o tema:

1. O antivírus é totalmente eficaz contra o Ransomware

a. Verdadeiro

b. Falso

2. Qual o principal meio de propagação de Ransomware?

a. Phishing

b. Websites infetados

c. Pen drives USB

d. Discos externos

3. Quem pode ser afetado pelo Ransomware?

a. Utilizadores de Windows

b. Utilizadores de Mac

c. Utilizadores de Linux

d. Todos

4. O que é Ransomware?

a. Malware que torna o nosso computador parte de uma botnet

b. Malware da família Ransom

c. Malware que codifica os dados para pedir um resgate

d. Malware que clica em links falsos

5. As atualizações regulares são umas das principais defesas contra Ransomware

a. Verdadeiro

b. Falso

7.1.7. Phishing

Sendo este o método utilizado nas campanhas não poderia ficar excluído deste processo de e-learning:

1. O único método conhecido de Phishing é por meio de E-Mails.

a. Verdadeiro

b. Falso

2. Que tipo de informação nunca deve ser cedida a terceiros?

a. Palavra-Passe

b. Nome de utilizador

c. Nome de utilizador e Palavra-passe

d. Todas as anteriores

3. Qual é a forma mais comum de os atacantes encontrarem informação sobre o seu alvo de Phishing direcionado?

a. Youtube

b. Google

c. Jornais

d. Redes Sociais

5. Que tipo de características explora o Phishing?

a. Confiança

b. Falta de informação

c. Falta de atenção

d. Todas as anteriores

7.1.8. RGPD

Sendo um diploma que determina as regras relativas à proteção e ao tratamento, bem como à livre circulação dos dados pessoais das pessoas e é das responsabilidade de todos nós, fazia todo o sentido despertar responsabilidades acerca do assunto.

1. O regulamento geral de proteção de dados é entra em vigor a partir de 25 de maio de 2018. Em que países é aplicável?

a. Apenas em Portugal

b. Nos países que aderiram ao regulamento

c. Em todos os estados-membros

d. Nos países que aderiram à moeda única

2. O RGPD diferencia dados sensíveis dos restantes dados pessoais. Escolha a opção mais assertiva que se enquadra como dados sensíveis.

a. Dados biométricos

b. Etnia

c. Dados de saúde

d. Todas as anteriores

3. Possibilidade de solicitar que sejam apagados todos os dados referentes à sua pessoa, pedido que têm de ser acedido, excetuando onde existam requisitos legais ou contratuais que inibam. Classifique se é verdadeira ou falsa a afirmação anterior.

a. Verdadeira

b. Falsa

4.Direito de solicitar em suporte informático os seus dados pessoais. Classifique se é verdadeira ou falsa a afirmação anterior.

a. Verdadeira

b. Falsa

5. Não posso limitar o uso dos meus dados, nomeadamente através do consentimento explicito na altura da recolha dos mesmos.

a. Verdadeira

b. Falsa

6. Em caso de haver uma fuga de dados pessoais, as organizações têm de notificar a autoridade de controlo. O período máximo para notificação é de;

a. 24 horas após conhecimento da fuga

b. 48 horas após conhecimento da fuga

c. 72 horas após conhecimento da fuga

d. Não existe prazo, apenas obrigação de notificar após conhecimento da fuga

7. Em função da gravidade do incumprimento a organização pode ser alvo de;

a. Aviso / Reprimenda / Suspensão de tratamento de dados / multa de 20 Milhões de Euros ou 4% do volume de faturação do grupo

b. Aviso / Suspensão de tratamento de dados / multa de 20 Milhões de Euros ou 4% do volume de Faturação do grupo

c. Aviso / Reprimenda / multa de 20 Milhões de Euros ou 2% do volume de faturação do grupo

d. Reprimenda / Suspensão de tratamento de dados / multa de 10 Milhões de Euros ou 2% do volume de faturação do grupo

7.2. Implementação no software SB:

Criação de quiz com sinalização das respostas corretas, figura 38:

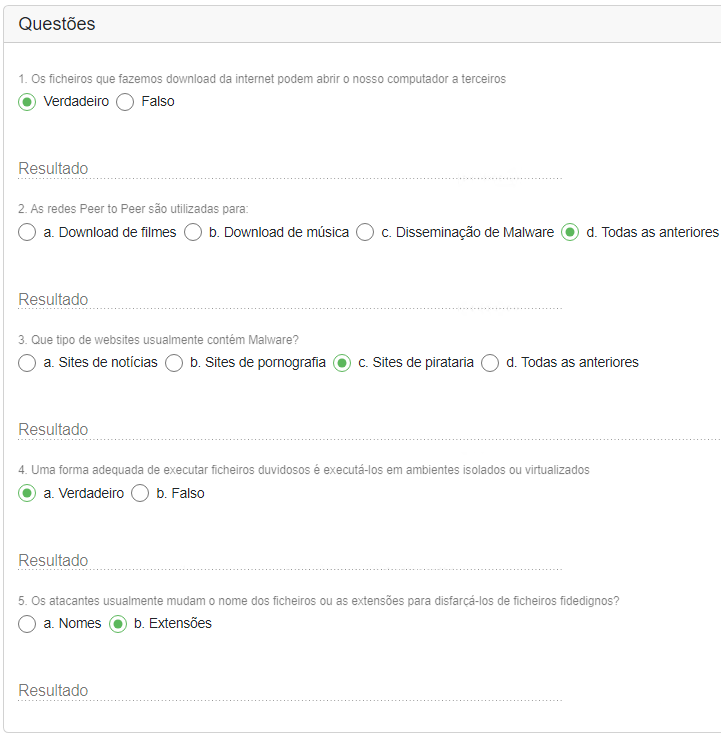


Figura 38 - primeira bateria de questões

Os utilizadores têm acesso através da plataforma, podendo preencher e visualizar os resultados das opções por si selecionadas.

a. Caso em que todas as respostas estão corretas:

Na figura 39 está representada a situação em que as respostas estão todas corretas.

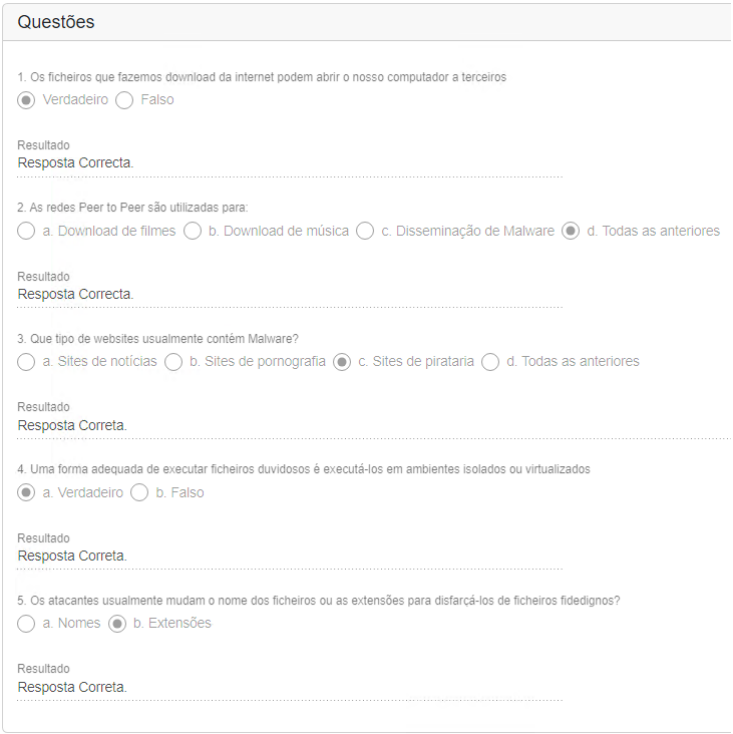


Figura 39 - exemplo de todas as respostas corretas

Caso o utilizador não acertasse todas as questões, as respostas corretas eram identificadas no resultado, como se constata na situação seguinte, figura 40, em que a única opção correta é a 3.

b. Caso de respostas incorretas e identificação das corretas

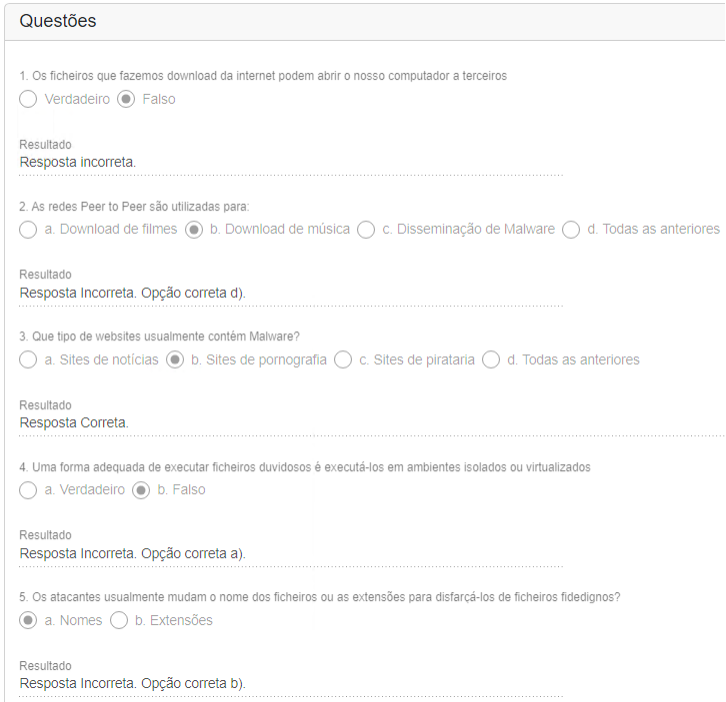


Figura 40 - Questões incorretamente assinaladas com identificação das opções corretas

Na questão três da figura 40, foi identificada uma dificuldade na plataforma disponibilizada, uma vez que o pretendido seriam duas respostas como opção correta, no entanto esta opções não está contemplada, permitindo somente uma resposta como correta. Esta implementação foi solicitada à empresa gestora da aplicação.

Ao preencher o quiz, é registado na plataforma o número mecanográfico do utilizador e os resultados das suas opções, desta forma permite ao serviço GTI identificar quais os utilizadores e serviços mais vulneráveis, assim como as áreas mais frágeis a possíveis ataques. Esta funcionalidade foi testada em qualidade, no entanto quando foi colocada em produção, coincidiu com uma atualização da aplicação SB, o que por motivos alheios inativou a funcionalidade, posteriormente a situação foi corrigida, novamente testada e a funcionar corretamente, no entanto dos questionários preenchidos só quatro assumiram o número mecanográfico, o que inviabilizou a análise sobre quem foram os utilizadores a dar feedback.

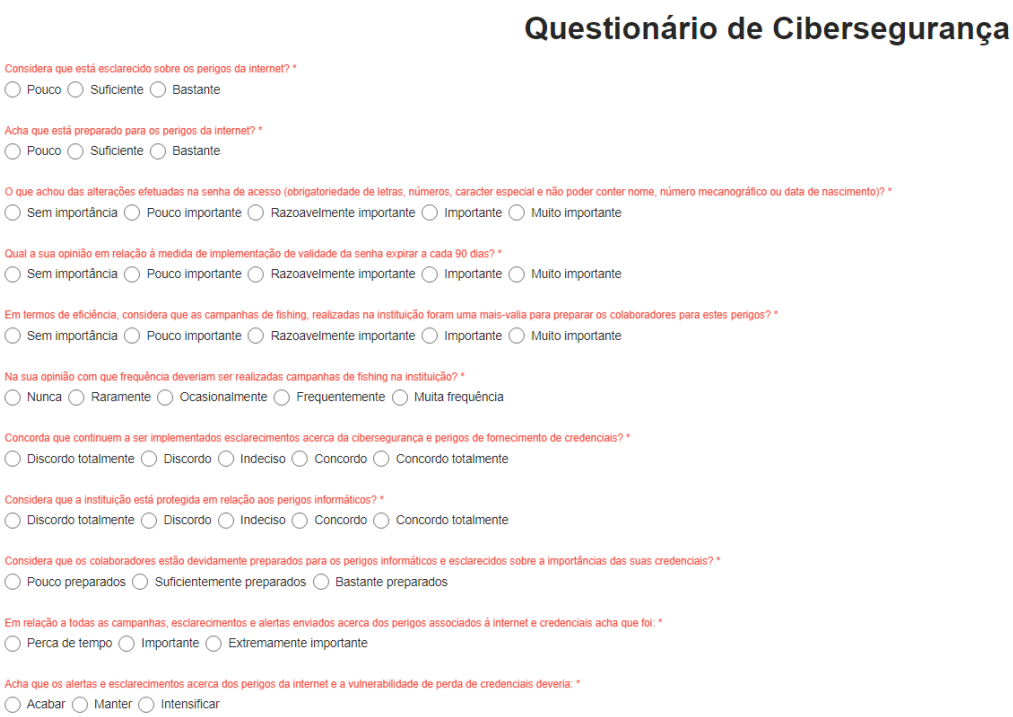
7.3. Envio de e-mail a informar e solicitar colaboração na participação do quiz

Após testes de qualidade na disponibilização dos vários temas implementados no quiz, com o objetivo de melhorar a maturidade dos utilizadores, foi enviado e-mail a informar e solicitar a interação com os mesmos, para melhoramento da informação dos utilizadores acerca das vulnerabilidades informáticas.

9. INQUÉRITOS

Criei um questionário, figura 41, relacionado com a cibersegurança com o intuito de perceber o nível de consciencialização dos utilizadores sobre as vulnerabilidades e do que foi realizado com o objetivo de despertar essa mesma consciência, com recurso à plataforma SB utilizada na instituição foi disponibilizado a todos os utilizadores o acesso e a solicitação de colaboração no preenchimento do mesmo.

a. Questionário de cibersegurança:



Questionário de Cibersegurança

Considera que está esclarecido sobre os perigos da internet? *
◯ Pouco ◯ Suficiente ◯ Bastante

Acha que está preparado para os perigos da internet? *
◯ Pouco ◯ Suficiente ◯ Bastante

O que achou das alterações efetuadas na senha de acesso (obrigatoriedade de letras, números, caracter especial e não poder conter nome, número mecanográfico ou data de nascimento)? *
◯ Sem importância ◯ Pouco importante ◯ Razoavelmente importante ◯ Importante ◯ Muito importante

Qual a sua opinião em relação à medida de implementação de validade da senha expirar a cada 90 dias? *
◯ Sem importância ◯ Pouco importante ◯ Razoavelmente importante ◯ Importante ◯ Muito importante

Em termos de eficiência, considera que as campanhas de fishing, realizadas na instituição foram uma mais-valia para preparar os colaboradores para estes perigos? *
◯ Sem importância ◯ Pouco importante ◯ Razoavelmente importante ◯ Importante ◯ Muito importante

Na sua opinião com que frequência deveriam ser realizadas campanhas de fishing na instituição? *
◯ Nunca ◯ Raramente ◯ Ocasionalmente ◯ Frequentemente ◯ Muita frequência

Concorda que continuem a ser implementados esclarecimentos acerca da cibersegurança e perigos de fornecimento de credenciais? *
◯ Discordo totalmente ◯ Discordo ◯ Indeciso ◯ Concordo ◯ Concordo totalmente

Considera que a instituição está protegida em relação aos perigos informáticos? *
◯ Discordo totalmente ◯ Discordo ◯ Indeciso ◯ Concordo ◯ Concordo totalmente

Considera que os colaboradores estão devidamente preparados para os perigos informáticos e esclarecidos sobre a importâncias das suas credenciais? *
◯ Pouco preparados ◯ Suficientemente preparados ◯ Bastante preparados

Em relação a todas as campanhas, esclarecimentos e alertas enviados acerca dos perigos associados à internet e credenciais acha que foi: *
◯ Perca de tempo ◯ Importante ◯ Extremamente importante

Acha que os alertas e esclarecimentos acerca dos perigos da internet e a vulnerabilidade de perda de credenciais deveria: *
◯ Acabar ◯ Manter ◯ Intensificar

Figura 41 - Questionário cibersegurança

b. O referido questionário foi enviado por e-mail:

A figura 41, representa o e-mail enviado a solicitar a participação e preenchimento do questionário

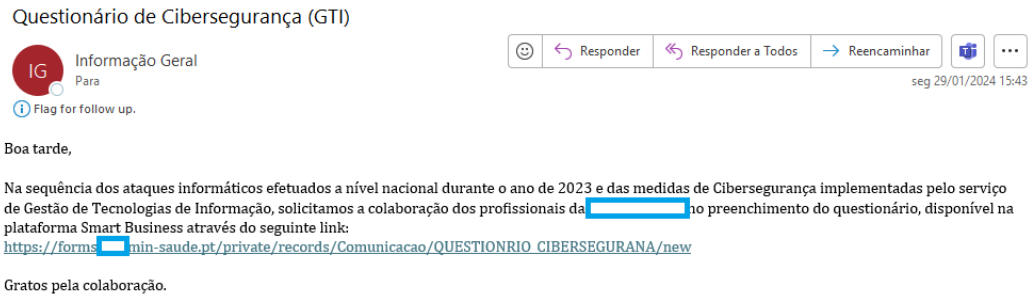


Figura 42 - e-mail enviado a solicitar preenchimento de questionário

10. RESULTADOS

a. Primeira Campanha de phishing

A simulação do primeiro e-mail de phishing foi despoletada no dia 30 de janeiro de 2023, oito dias após, ou seja, no dia 6 de janeiro foi enviado e-mail a esclarecer e alertar sobre os resultados obtidos na campanha de phishing. Neste dia 86 profissionais tinham aberto o link e 54 destes tinham inclusive introduzido credenciais.

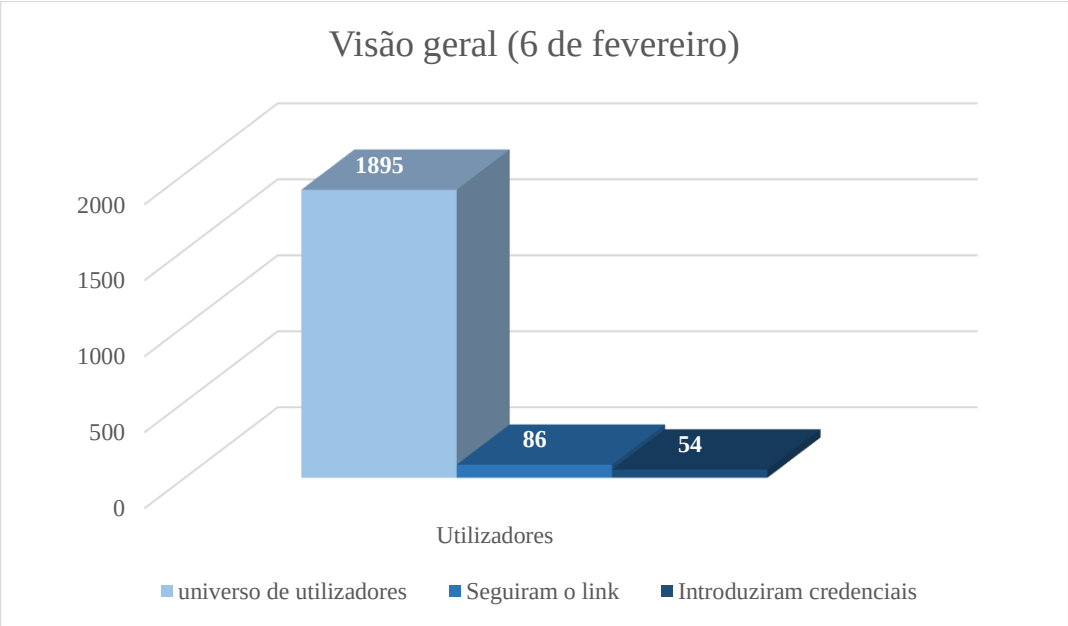


Gráfico 16 - visão geral dos utilizadores a 6 de fevereiro

Era espectável que após o envio de e-mail com explicação do inicialmente enviado alertando para o perigo caso tivesse sido uma situação real e alertando para os elementos que deveriam ter suscitado alerta sobre a veracidade do mesmo, mais nenhum utilizador fosse enganado pelo e-mail inicialmente enviado, no entanto para admiração em meados de fevereiro, os registos eram os seguintes:

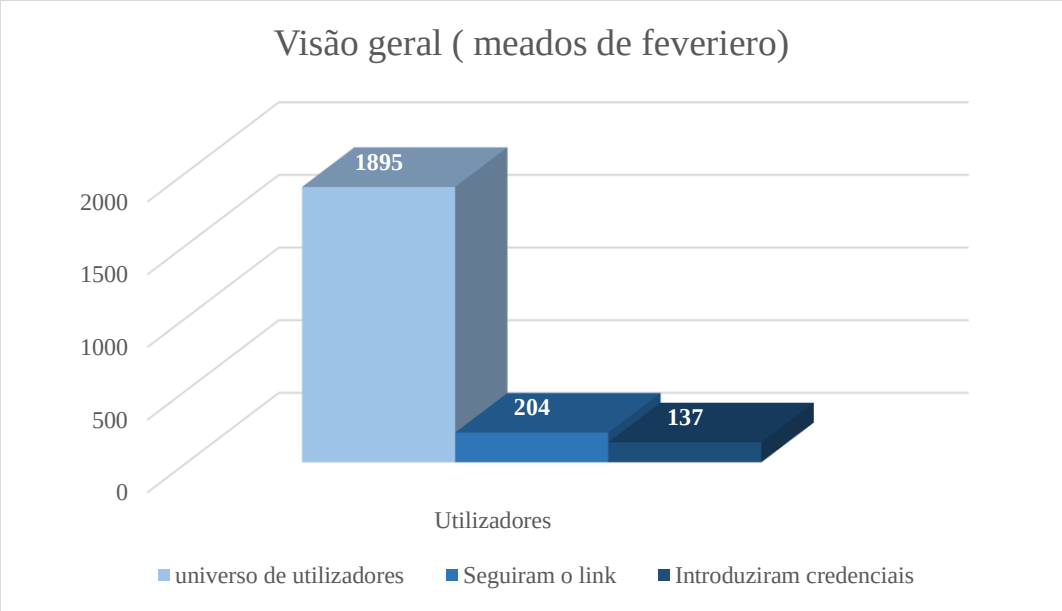


Gráfico 17 - visão geral dos utilizadores a meados de fevereiro

Em termos comparativos, houve um aumento significativo e preocupante de utilizadores, o que é alarmante, tendo em consideração que entre os novos registos estão administradores hospitalares, tiveram o bom senso de após introdução de credenciais contactar de imediato o serviço de gti.

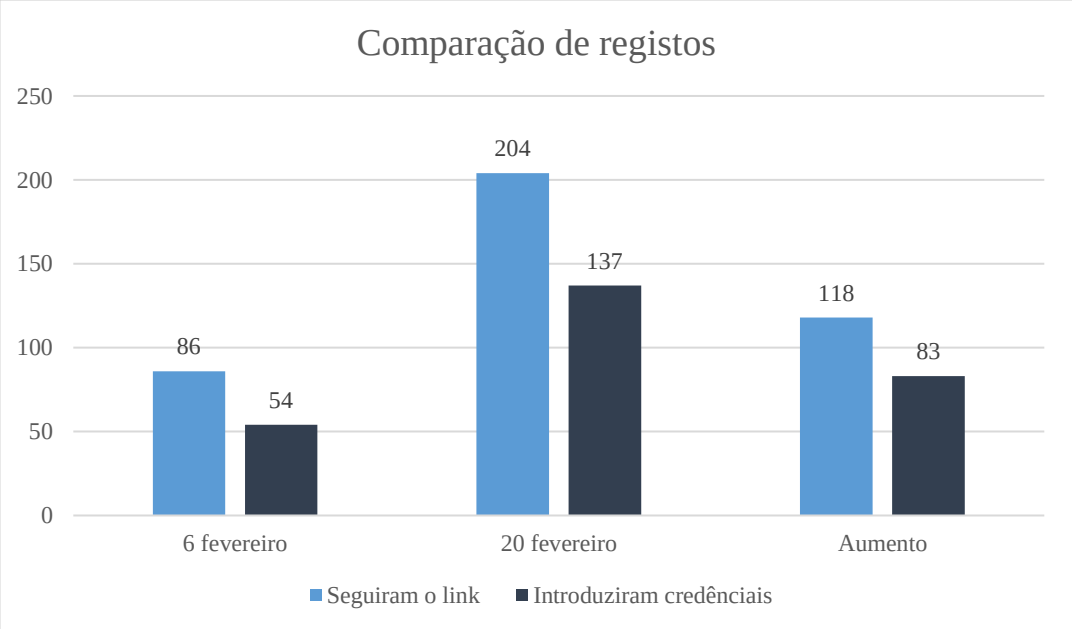


Gráfico 18 - Registos antes e após esclarecimento da campanha de phishing

Analisando os utilizadores que introduziram credenciais, nomeadamente por grupo profissional:

Tabela 30 - Categorias profissionais que introduziram credenciais

	06/fev	20/fev
Assistente Operacional	14	22
Assistente Técnico	4	26
Pessoal de Enfermagem	21	48
Pessoal em formação pré-carreira Médica	1	3
Pessoal Farmacêutico	1	1
Pessoal Médico	9	22
Pessoal Técnico Sup. de Diagnóstico e Terapêutica	3	9
Pessoal Técnico Superior de Saúde	0	1
Técnicos Superiores	0	4
Outro Pessoal	1	1
Total	**54**	**137**

Graficamente é visível o aumento de utilizadores de introduziram credenciais após ter sido enviado e-mail a esclarecer sobre a campanha de phishing:

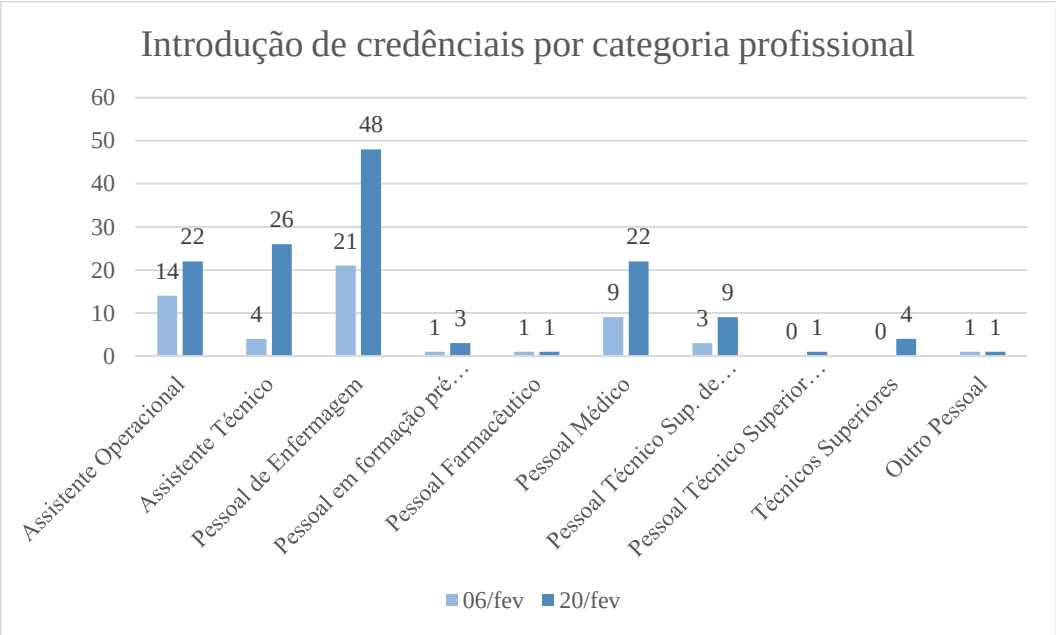


Gráfico 19 - Introdução de credenciais por categoria profissional

Comparativamente o registo de credenciais registadas até ao dia 6 e até ao dia 20 de fevereiro:

Tabela 31 - Percentagem de funcionário por categoria profissional que introduziram credenciais

	06/fev	20/fev
Assistente Operacional	25.9%	42.0%
Assistente Técnico	7.4%	26.4%
Pessoal de Enfermagem	38.9%	73.9%
Pessoal em formação pré-carreira Médica	1.9%	4.0%
Pessoal Farmacêutico	1.9%	2.6%
Pessoal Médico	16.7%	32.7%
Pessoal Técnico Sup. de Diagnóstico e Terapêutica	5.6%	12.1%
Pessoal Técnico Superior de Saúde	0.0%	0.7%
Técnicos Superiores	0.0%	2.9%

Outro Pessoal	1.9%	2.6%
Total	100%	100%

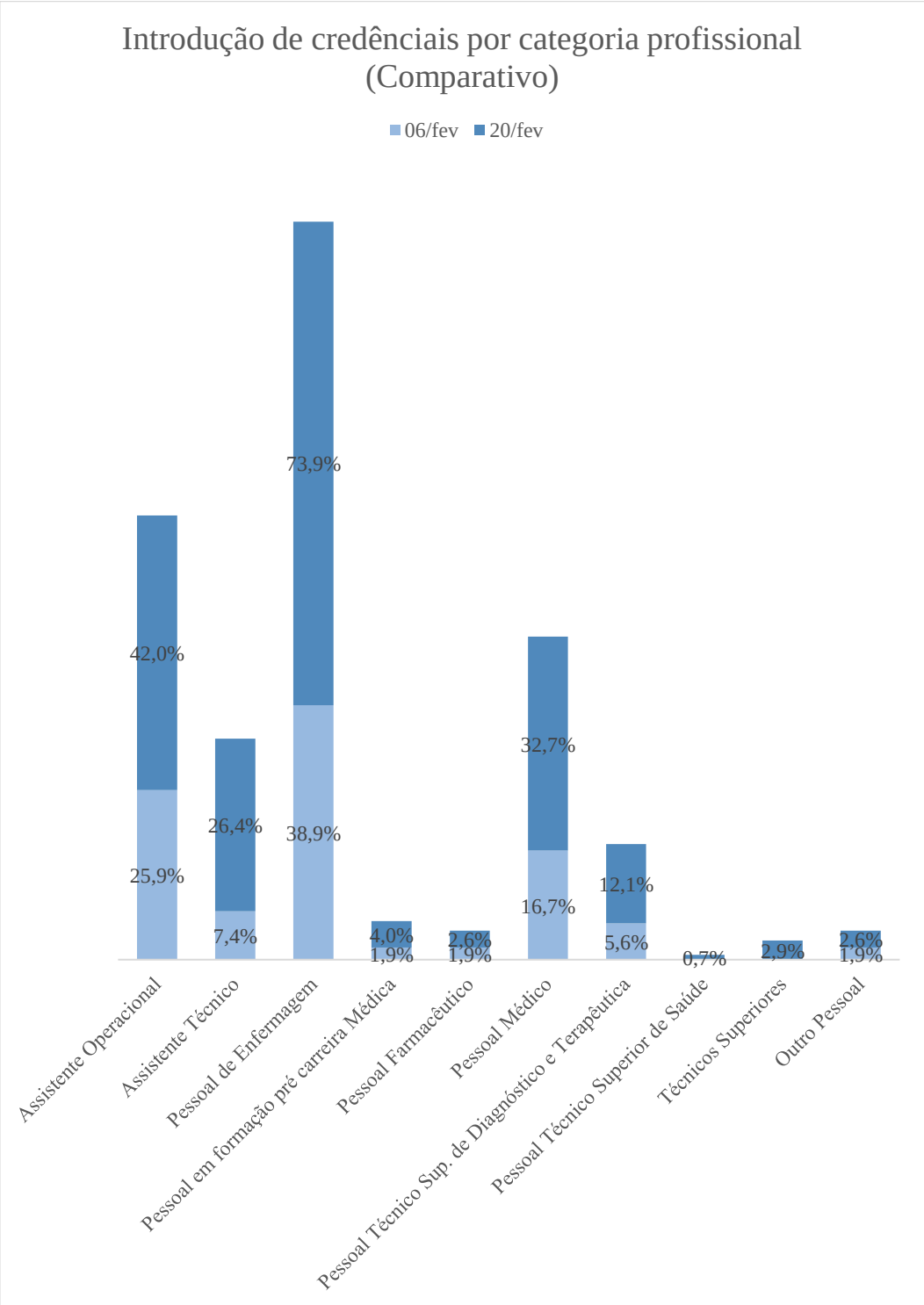


Gráfico 20 - Percentagem de utilizadores que adicionaram credenciais por categoria profissional

Analisando as idades dos utilizadores que adicionaram credenciais:

Tabela 32 - Número de funcionários que adicionaram credenciais distribuídos por classes de idades

Classe de Idades	Número de funcionários
20 a 29	7
30 a 39	23
40 a 49	41
50 a 59	45
60 a 69	21

Analisando graficamente:

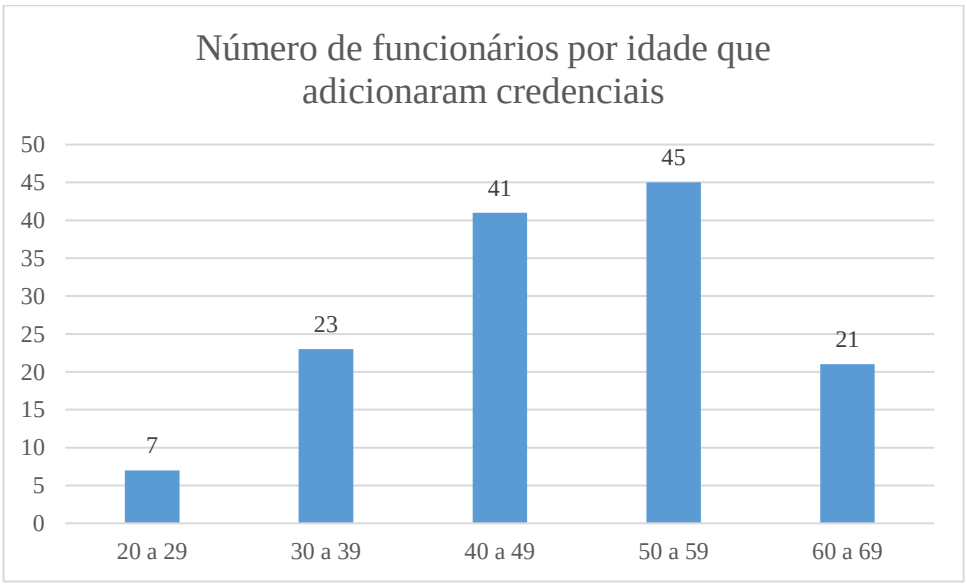


Gráfico 21 - Número de funcionários que adicionaram credencias distribuídos por classes de idade

Em termos percentuais:

Tabela 33 - Percentagem de funcionários que adicionaram credencias distribuídos por classes de idades em termos percentuais

Classe de Idades	Percentagem de funcionários
20 a 29	5.1%
30 a 39	16.8%
40 a 49	29.9%
50 a 59	32.8%
60 a 69	15.3%

Analisando graficamente:

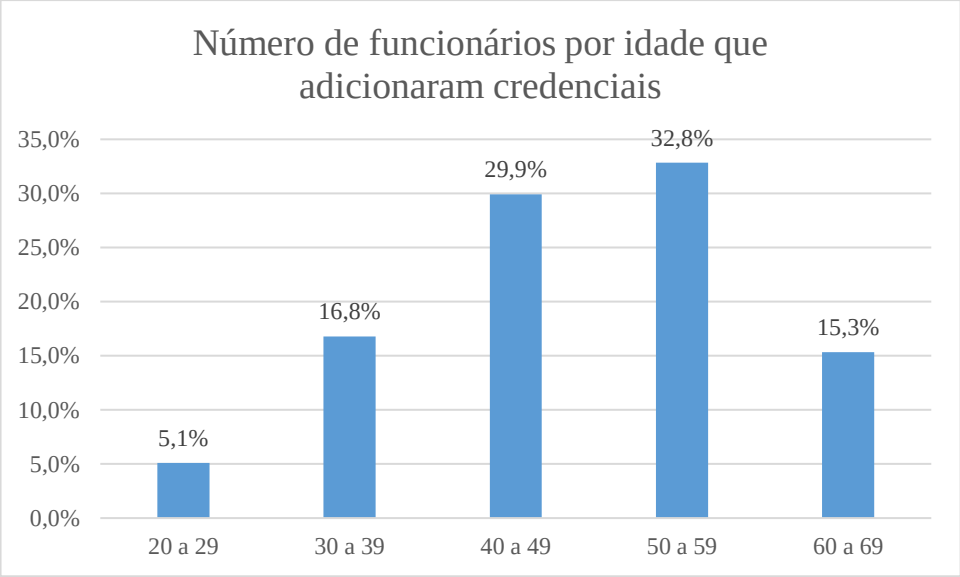


Gráfico 22 - Percentagem de funcionários que adicionaram credencias distribuídos por classes de idades em termos percentuais

Em termos de habilitações os funcionários que introduziram credenciais distribuem-se da seguinte forma:

Tabela 34 - Habilitações dos funcionários que introduziram credenciais

Habilitações	06/fev	20/fev
6º ano	1	1
7º ano	1	1
9º ano	7	11
10º ano	0	1
11º ano	0	5
12º ano	9	25
Curso Técnico Profissional	0	1
Bacharelato	3	13
Licenciatura	24	60
Pós-Licenciatura (Especialização)	4	8
Pós-Graduação	1	2
Mestrado	4	8
Doutoramento	0	1

Para uma melhor análise, recorri à representação gráfica:

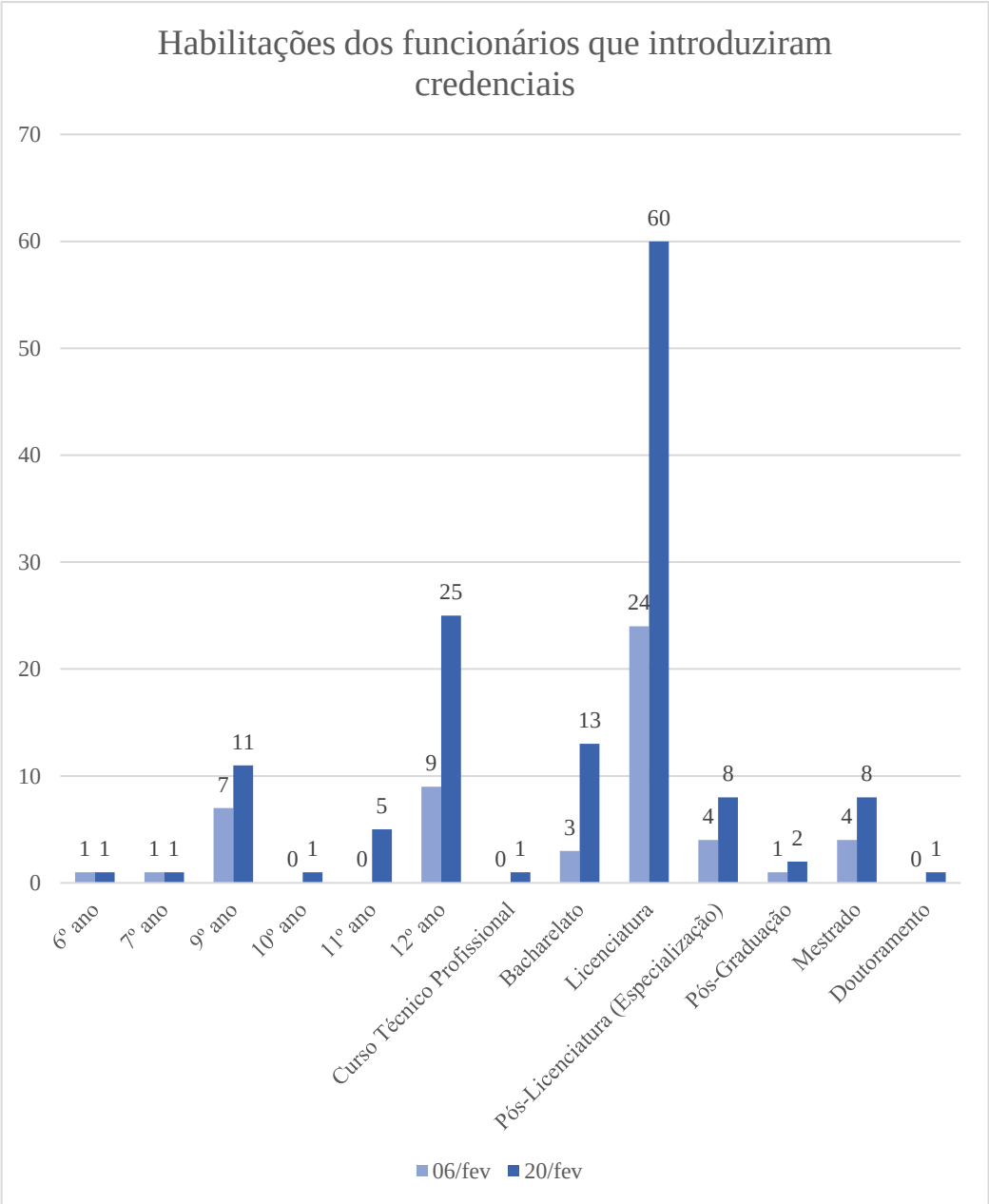


Gráfico 23 - Habilitações dos funcionários que introduziram credenciais

Funcionários que reportaram a situação para o serviço GTI:

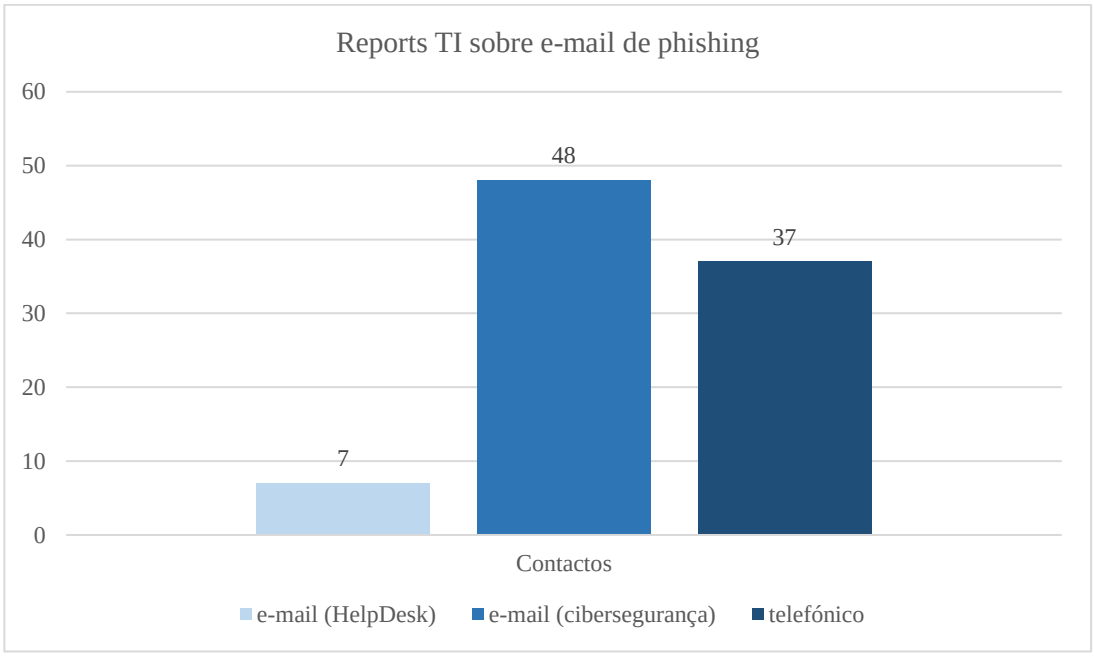


Gráfico 24 - Contactos de utilizadores alertando sobre o e-mail phishing

b. Segunda campanha de phishing

Como não criei nenhuma condição para impedir registos duplicados, ou seja, não havia nenhuma validação acerca se o número mecanográfico já tinha efetuado algum registo, criou a possibilidade de o mesmo utilizador poder registar-se mais do que uma vez, na prática traduziu-se em 534 registos no total. Outra validação que tinha sido pertinente seria a introdução do número mecanográfico, como não havia, permitiu a introdução de dois números onde um deles tinha dois algarismos a mais e outro onde faltava um dígito.

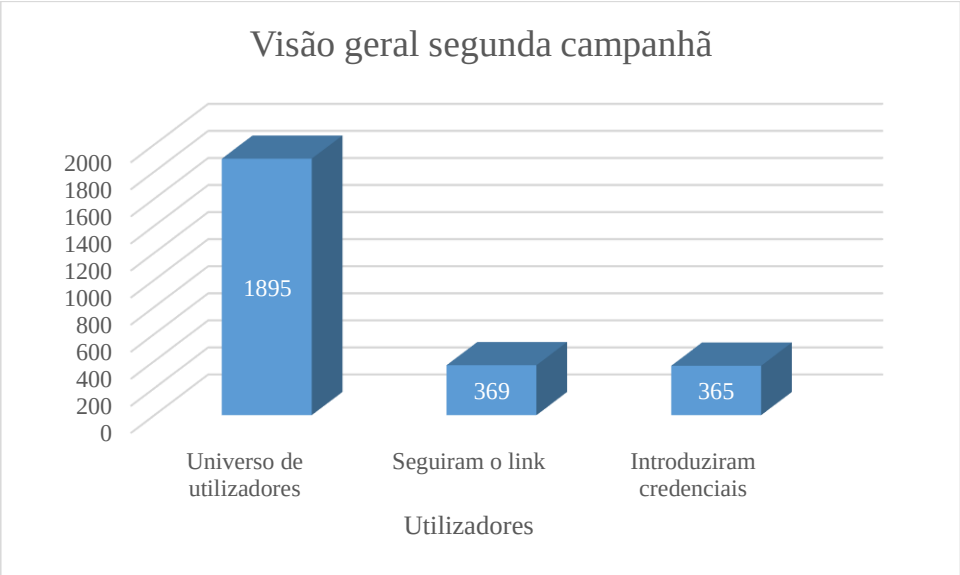


Gráfico 25 - Visão geral do resultado da segunda campanha

Analisando os utilizadores que introduziram credenciais, nomeadamente por grupo profissional:

Tabela 35 - Categorias profissionais que introduziram credenciais

Administração Hospitalar	2
Assistente Operacional	61
Assistente Técnico	80
Pessoal Dirigente	3
Pessoal de Enfermagem	132

Pessoal em formação pré-carreira Farmacêutica	2
Pessoal em formação pré carreira Médica	12
Pessoal Farmacêutico	2
Pessoal Médico	26
Pessoal Técnico Sup. de Diagnóstico e Terapêutica	32
Técnicos Superiores	13

Analisando graficamente os resultados obtidos:

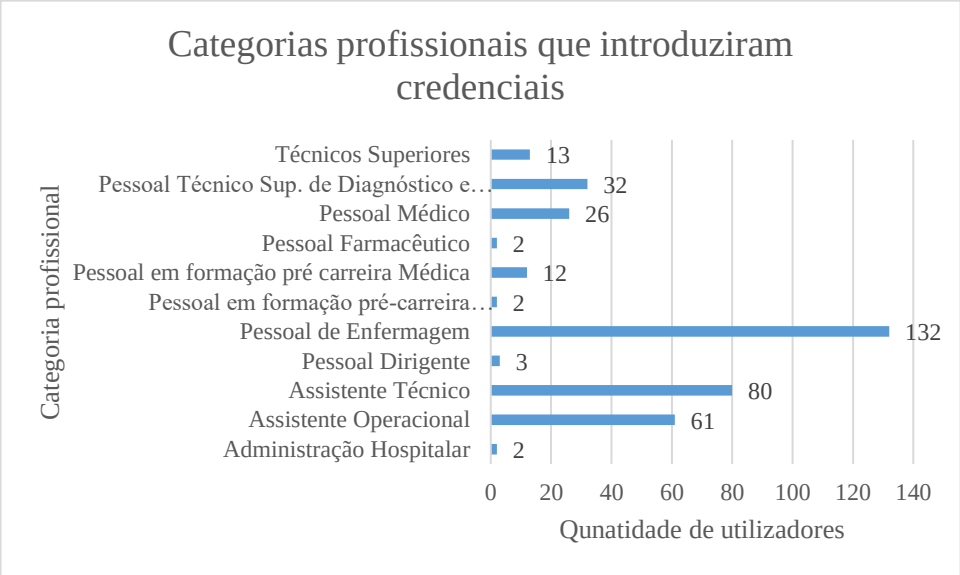


Gráfico 26 - Categorias profissionais que introduziram credenciais

Analisando as idades dos utilizadores que introduziram credenciais:

Tabela 36 - Quantidade de funcionários que introduziram credenciais distribuídos por classes

Classe de idades	Quantidade de funcionários
20 a 29	33

30 a 39	78
40 a 49	115
50 a 59	103
60 a 69	36

Analisando graficamente:

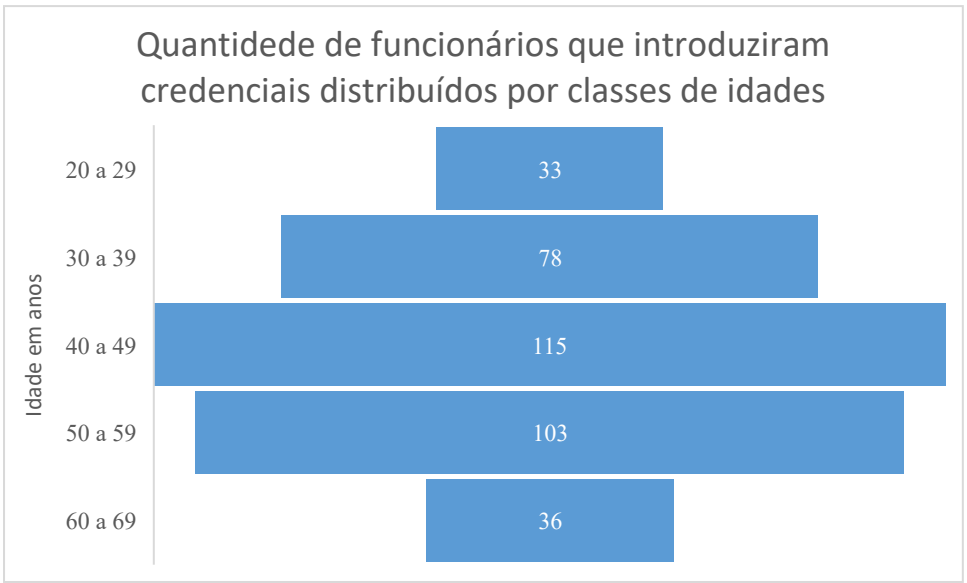


Gráfico 27 - Número de funcionários que introduziram credenciais distribuídos por classes de idades

Analisando a distribuição percentual por classes de idades de funcionários que introduziram credencias:

Tabela 37 - Percentagem de funcionários que introduziram credenciais distribuídos por classes de idades em termos percentuais

Classe de idades	Quantidade de funcionários
20 a 29	9.0%
30 a 39	21.4%
40 a 49	31.5%

50 a 59	28.2%
60 a 69	9.9%

Em termos gráficos:

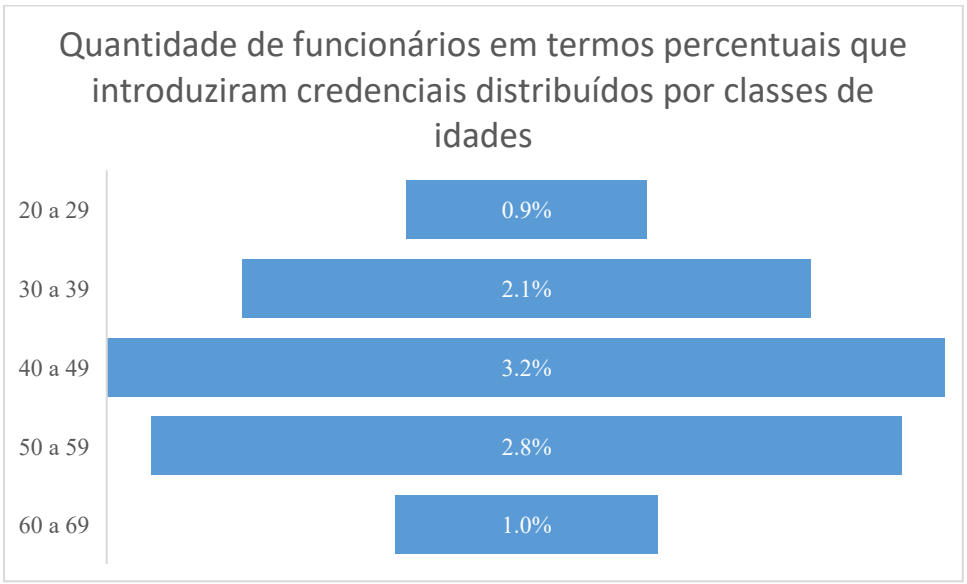


Gráfico 28 - Quantidade de funcionários em termos percentuais que introduziram credenciais distribuídos por classes de idades

Em termos de habilitações os funcionários que introduziram credenciais distribuem-se da seguinte forma:

Tabela 38 - Habilitações dos funcionários que introduziram credenciais

Habilitações	**Quantidade de funcionários**
4º ano	1
6º ano	10
8º ano	1
9º ano	22
10º ano	0

11º ano	11
12º ano	70
Ensino Secundário Não Superior de Nível IV	1
Curso Técnico Profissional	2
Bacharelato	35
Licenciatura	162
Pós-Licenciatura (Especialização)	8
Pós-Graduação	4
Mestrado	36
Doutoramento	2

Analisando graficamente:

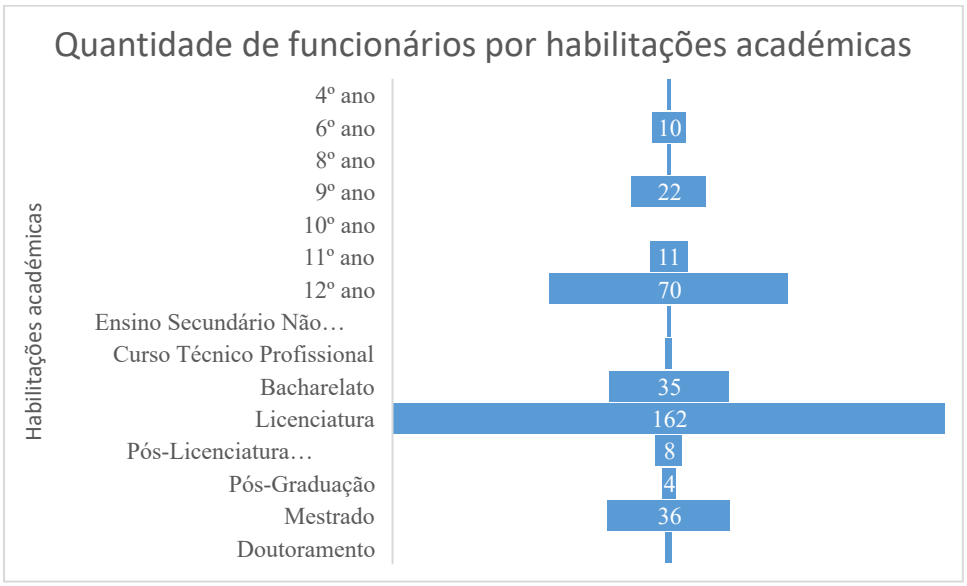


Gráfico 29 - Quantidade de funcionários por habilitações académicas que introduziram credencias na segunda campanha de phishing

Em termos percentuais:

Tabela 39- Habilitações dos funcionários em termos percentuais que introduziram credenciais

Habilitações	**Quantidade de funcionários**
4º ano	0.3%
6º ano	2.7%
8º ano	0.3%
9º ano	6.0%
10º ano	0.0%
11º ano	3.0%
12º ano	19.2%
Ensino Secundário Não Superior de Nível IV	0.3%
Curso Técnico Profissional	0.5%
Bacharelato	9.6%
Licenciatura	44.4%
Pós-Licenciatura (Especialização)	2.2%
Pós-Graduação	1.1%
Mestrado	9.9%
Doutoramento	0.5%

Graficamente fica:

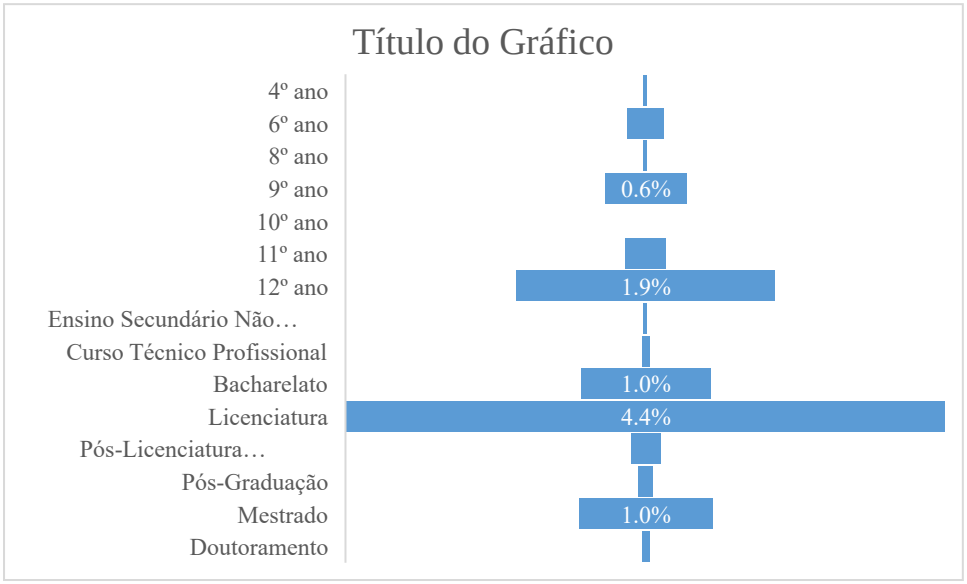


Gráfico 30 - Habilitações dos funcionários em termos percentuais que introduziram credenciais

Funcionários que reportaram a situação para o serviço GTI na segunda campanha:

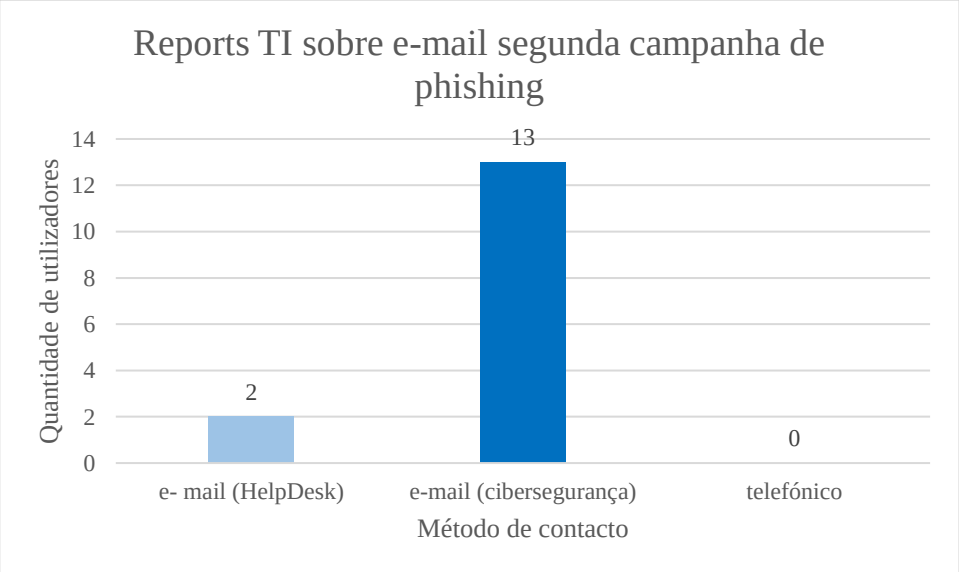


Gráfico 31 - Quantidade de utilizadores e meio utilizado para reportar ao serviço de GTI na segunda campanha

Foi feita uma segunda recolha de resultados, à semelhança da primeira campanha, no entanto não houve mais casos registados após o e-mail de esclarecimento. Este comportamento interpreto como positivo, porque poderia ter aumentado o número de registo como na primeira por este facto depreendo que os utilizadores se tornaram de certa forma mais cautelosos após terem sido alertados do número dramático do resultado da segunda campanha.

c. **Inquéritos**:

Após três semanas só consegui obter o preenchimento de 70 questionários, com os seguintes resultados:

i. Considera que está esclarecido sobre os perigos da internet?

Tabela 40 - Respostas acerca da opinião dos colaboradores referente ao esclarecimento dos perigos da internet

Pouco	Suficiente	Bastante
5	49	16

Graficamente

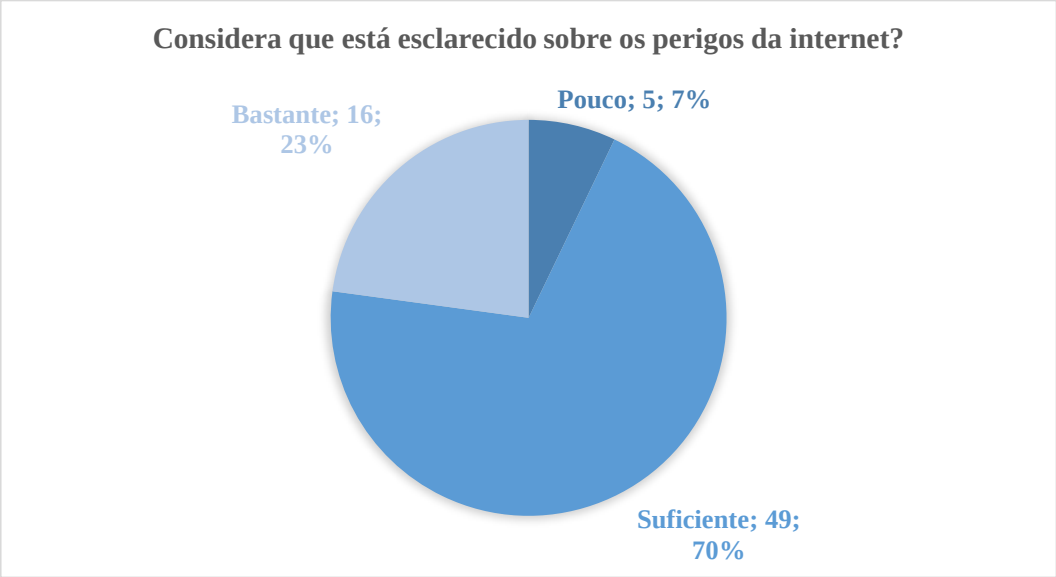


Gráfico 32 - Respostas acerca da opinião dos colaboradores referente ao esclarecimento dos perigos da internet

ii. Acha que está preparado para os perigos da internet?

Tabela 41- Respostas acerca da opinião dos colaboradores referente á sua preparação para os perigos da internet

Pouco	Suficiente	Bastante
15	46	9

Graficamente:

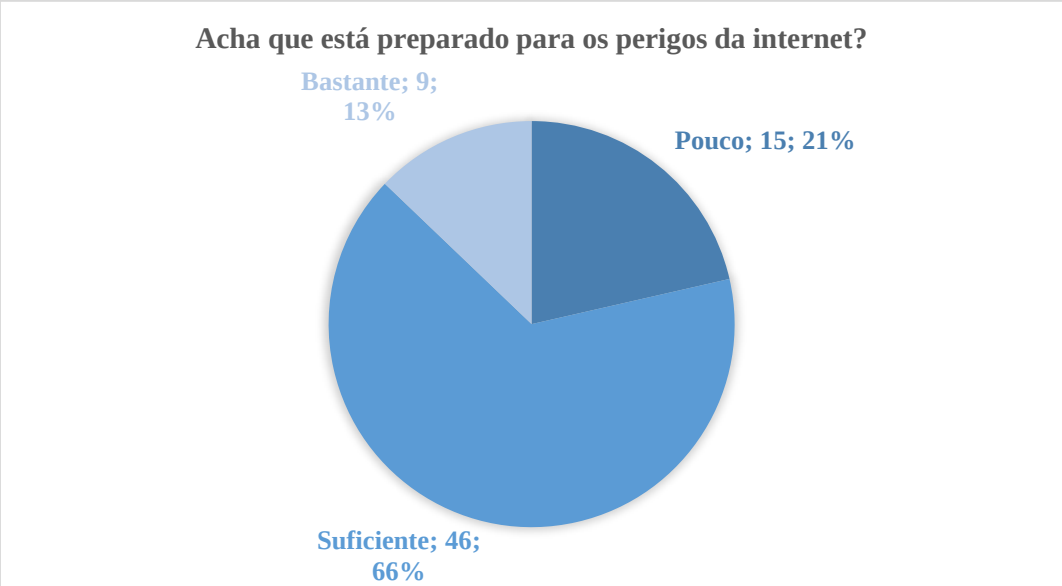


Gráfico 33 - Respostas acerca da opinião dos colaboradores referente á sua preparação para os perigos da internet

iii. O que achou das alterações efetuadas na senha de acesso (obrigatoriedade de letras, números, caracter especial e não poder conter nome, número mecanográfico ou data de nascimento)?

Tabela 42 - Respostas acerca da opinião dos colaboradores referente às alterações efetuadas na senha de acesso

Sem importância	Pouco importante	Razoavelmente importante	Importante	Muito importante
0	0	9	31	30

Graficamente:

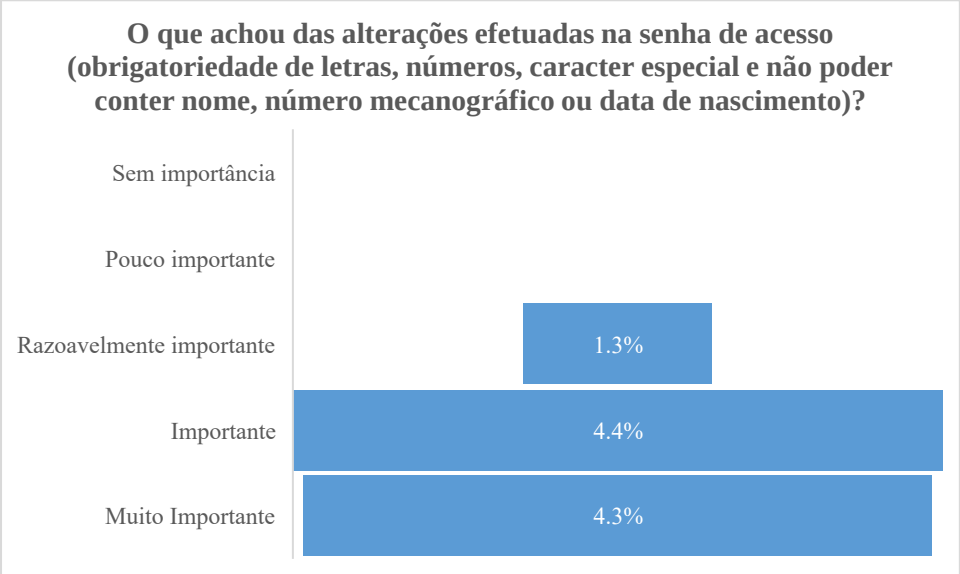


Gráfico 34 - Respostas acerca da opinião dos colaboradores referente às alterações efetuadas na senha de acesso

iv. Qual a sua opinião em relação à medida de implementação de validade da senha expirar a cada 90 dias?

Tabela 43 - Respostas acerca da opinião dos colaboradores referente às alterações da validade das senhas

Sem importância	Pouco importante	Razoavelmente importante	Importante	Muito importante
0	9	13	31	17

Graficamente:

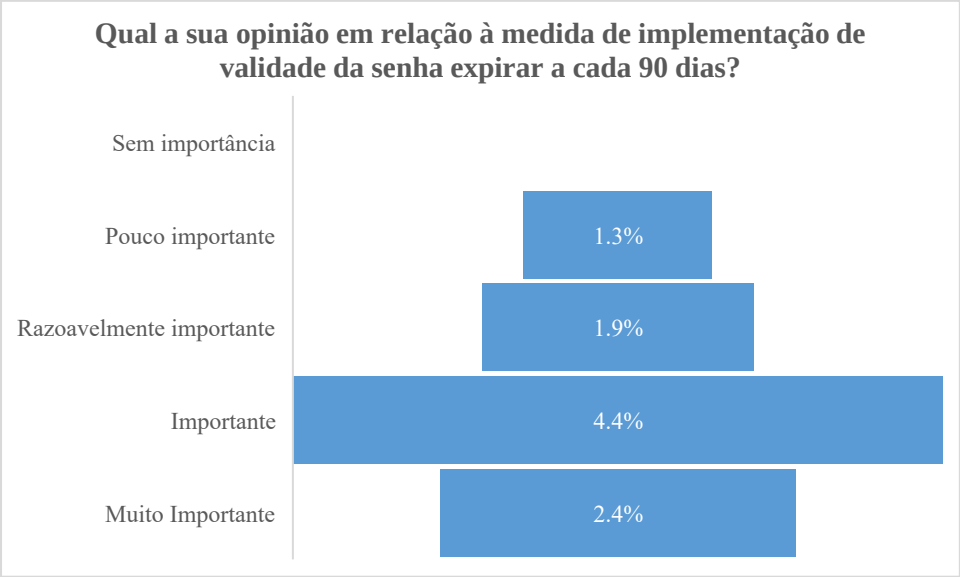


Gráfico 35 - Respostas acerca da opinião dos colaboradores referente às alterações da validade das senhas

v. Em termos de eficiência, considera que as campanhas de fishing, realizadas na instituição, foram uma mais-valia para preparar os colaboradores para estes perigos?

Tabela 44 - Respostas acerca da opinião dos colaboradores referente às campanhas de phishing

Sem importância	Pouco importante	Razoavelmente importante	Importante	Muito importante
0	2	15	31	22

Graficamente:

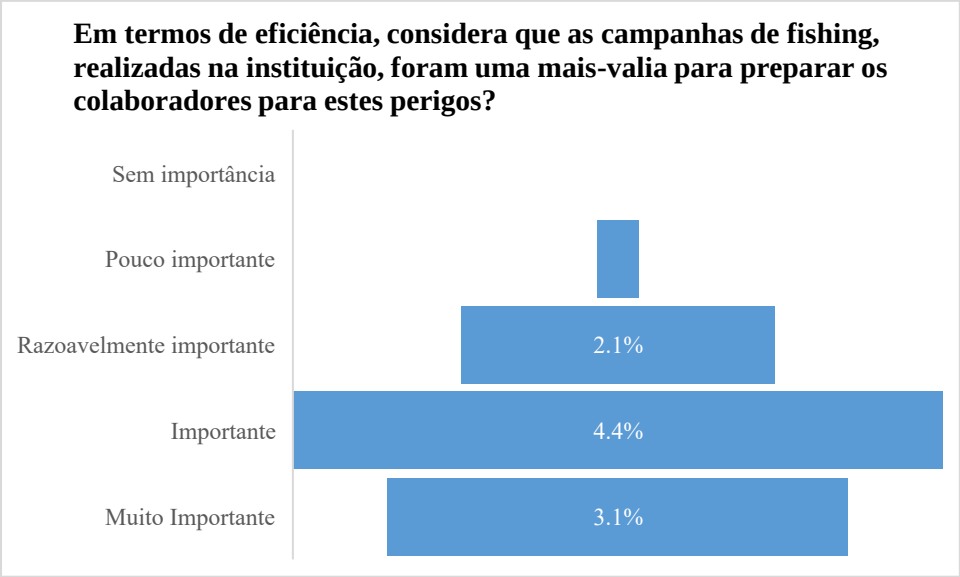


Gráfico 36 - Respostas acerca da opinião dos colaboradores referente às campanhas de phishing

vi. Na sua opinião com que frequência deveriam ser realizadas campanhas de fishing na instituição?

Tabela 45 - Respostas acerca da opinião dos colaboradores referente á frequência das campanhas

Nunca	Raramente	Ocasionalmente	Frequentemente	Muita Frequência
0	0	14	49	7

Graficamente:

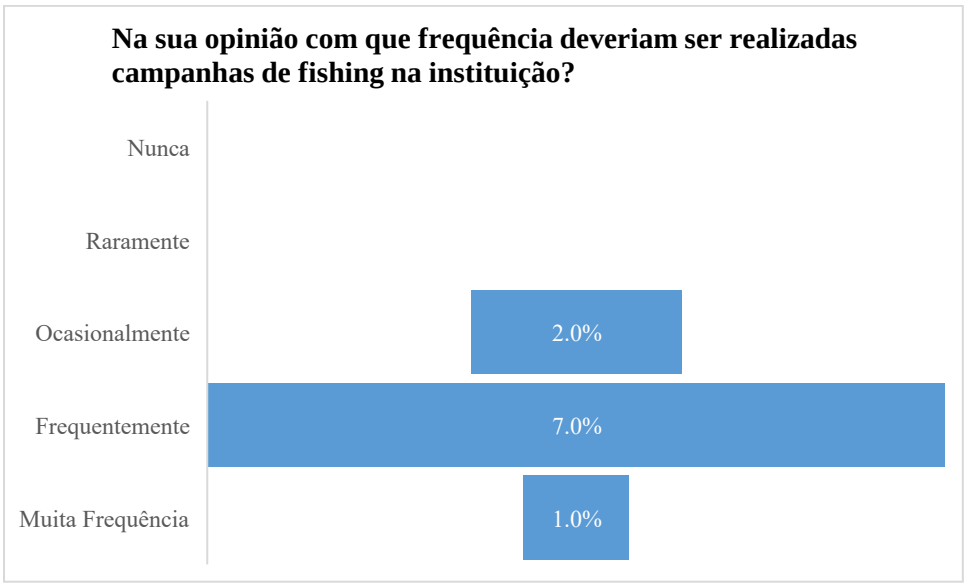


Gráfico 37 - Respostas acerca da opinião dos colaboradores referente á frequência das campanhas

vii. Concorda que continuem a ser implementados esclarecimentos acerca da cibersegurança e perigos de fornecimento de credenciais?

Tabela 46 - Respostas acerca da opinião dos colaboradores referente á continuação de esclarecimentos acerca da cibersegurança e perigos de fornecimento de credenciais

Discordo totalmente	Discordo	indeciso	Concordo	Concordo totalmente
0	0	0	28	42

Graficamente:

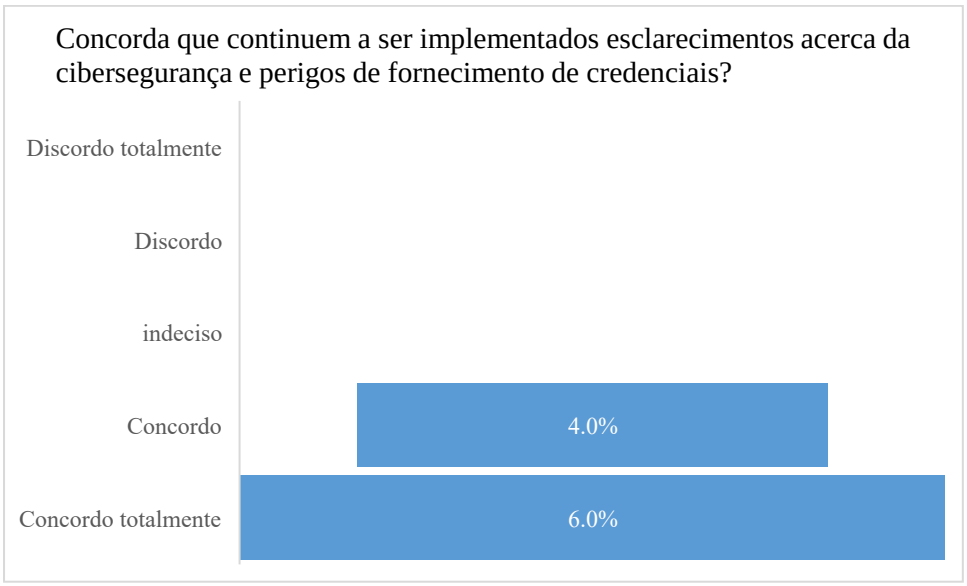


Gráfico 38- Respostas acerca da opinião dos colaboradores referente á continuação de esclarecimentos acerca da cibersegurança e perigos de fornecimento de credenciais

viii. Considera que a instituição está protegida em relação aos perigos informáticos?

Tabela 47 - Respostas acerca da opinião dos colaboradores referente á proteção da instituição relativamente aos perigos informáticos

Discordo totalmente	Discordo	indeciso	Concordo	Concordo totalmente
0	8	27	31	4

Graficamente:

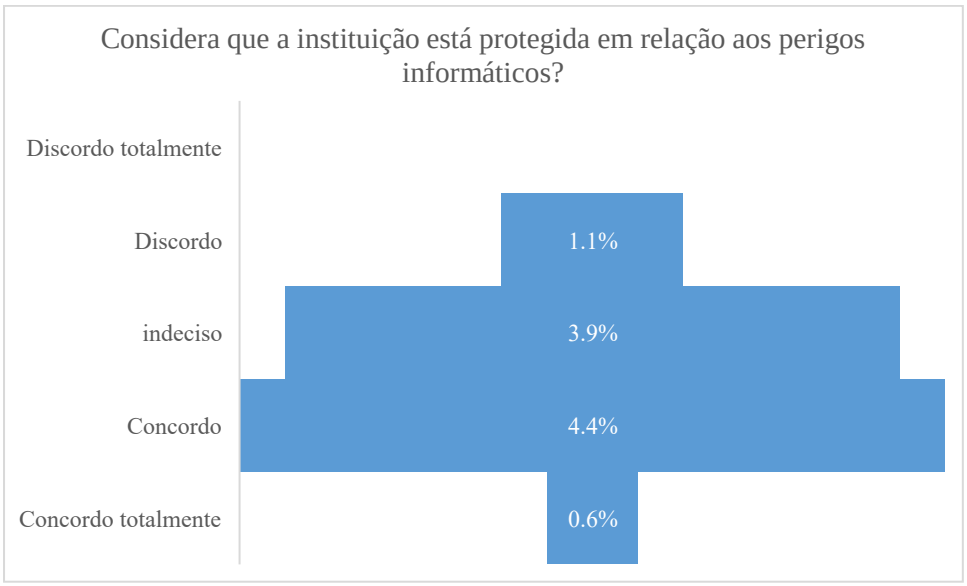


Gráfico 39 - Respostas acerca da opinião dos colaboradores referente á proteção da instituição relativamente aos perigos informáticos

ix. Considera que os colaboradores estão devidamente preparados para os perigos informáticos e esclarecidos sobre a importâncias das suas credenciais?

Tabela 48 - Respostas acerca da opinião dos colaboradores referente á importância das suas credenciais

Pouco preparados	Suficientemente preparados	Bastante preparados
34	34	2

Graficamente:

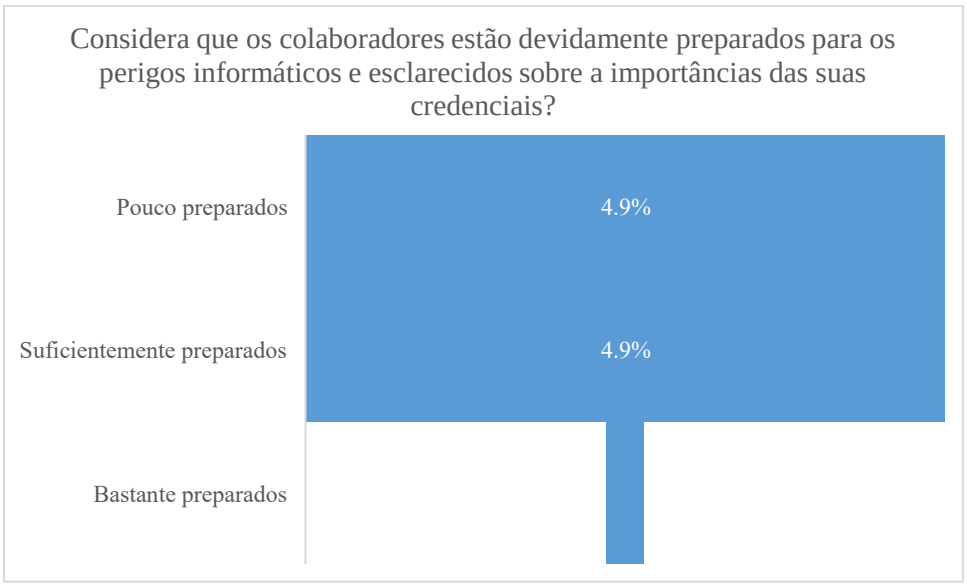


Gráfico 40- Respostas acerca da opinião dos colaboradores referente á importância das suas credenciais

x. Em relação a todas as campanhas, esclarecimentos e alertas enviados acerca dos perigos associados à internet e credenciais acha que foi:

Tabela 49 - Respostas acerca da opinião dos colaboradores referente ás campanhas, esclarecimentos e alertas enviados acerca dos perigos associados à internet e credenciais

Perca de tempo	importante	extremamente importante
0	40	30

Graficamente:

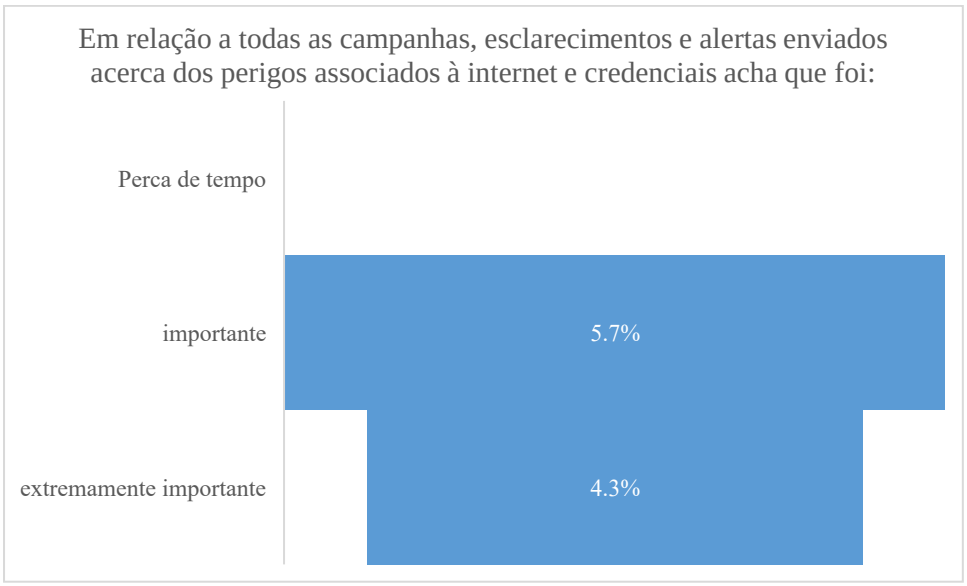


Gráfico 41 - Respostas acerca da opinião dos colaboradores referente ás campanhas, esclarecimentos e alertas enviados acerca dos perigos associados à internet e credenciais

xi. Acha que os alertas e esclarecimentos acerca dos perigos da internet e a vulnerabilidade de perda de credenciais deveria:

Tabela 50 - Respostas acerca da opinião dos colaboradores referente á continuidade de alertas e esclarecimentos sobre os perigos da internet

Acabar	Manter	Intensificar
0	34	36

Graficamente:

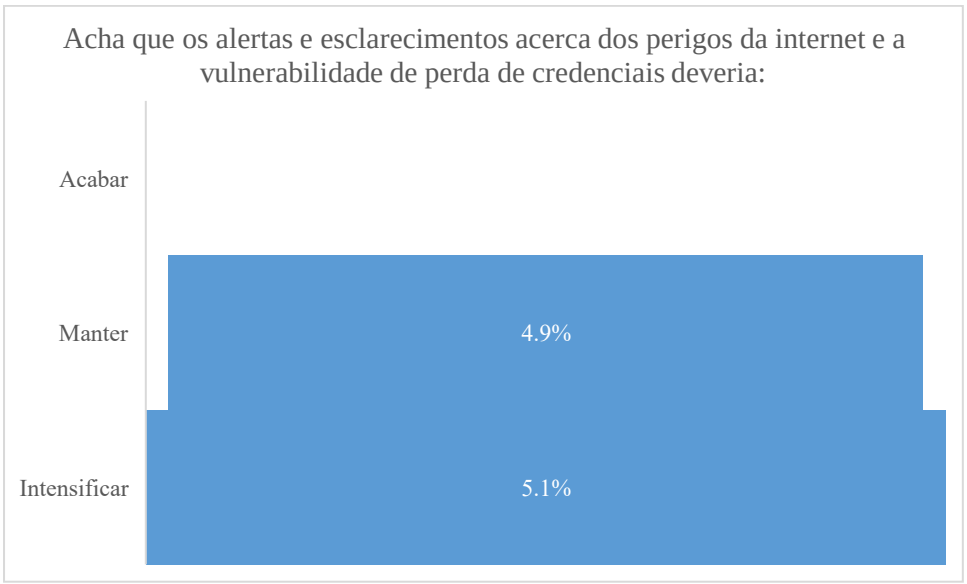


Gráfico 42- Respostas acerca da opinião dos colaboradores referente á continuidade de alertas e esclarecimentos sobre os perigos da internet

11. DISCUSSÃO DOS RESULTADOS

Era inicialmente espectável que o resultado não fosse muito promissor em relação ao nível de preparação e segurança por parte dos utilizadores, no entanto o resultado revelou-se ainda mais preocupante.

O aumento do registo de utilizadores após o e-mail esclarecedor da campanha de phishing pode ser diversas interpretações, nomeadamente pode e houve de certeza utilizadores que caíram no engodo, mas neste incremento de resultados podem estar eventualmente utilizadores que ao terem conhecimento que a campanha tinha sido despoletada pela informática e que não iria representar perigo para estes ou para a própria instituição, por curiosidade foram impelidos a verificar os links e as ações, fica a dúvida. Num prisma otimista quero acreditar que a esmagadora maioria se situa no segundo motivo, no entanto houve uma administradora hospitalar que ligou em pânico porque tinha seguido o link e colocado credenciais, mesmo após o e-mail que esclarecia o sucedido.

Uma das limitações do estudo realizado prende-se com o facto de não termos dados sobre quem efetivamente abriu e leu o e-mail, uma vez que podem existir utilizadores que não o façam, efetivamente houve manifesto de utilizadores que alegaram não utilizar o e-mail institucional, nomeadamente alguns auxiliares e prestadores.

Outra das limitações foi a imposição dos e-mails serem sempre enviados do domínio da instituição, pelo facto do integrador não permitir inserir outro.

O serviço de GTI não foi envolvido como alvo na campanha implementada, uma vez que a equipa de helpdesk era notificada do que iria acontecer devido às possíveis chamadas telefónicas sobre o e-mail rececionado e teriam de parecer surpreendidos, a equipa de cibersegurança também era notificada pelo facto da receção dos e-mails reencaminhado a dar o alerta do sucedido.

Na segunda campanha de phishing seria espectável que o número de utilizadores a serem ludibriados e inclusive disponibilizarem credencias fosse substancialmente menor,

no entanto a segunda campanha foi mais subtil nas evidências, uma vez que não era a primeira vez que os utilizadores seriam abordados, assim como o assunto não era novidade a simulação teria de ser mais realista.

Em ambas as campanhas a categoria profissional mais atingida foi o pessoal de enfermagem, embora seja a categoria com mais funcionários na instituição (36.9%), não deixa de ser preocupante a quantidade de utilizadores que colocaram credenciais.

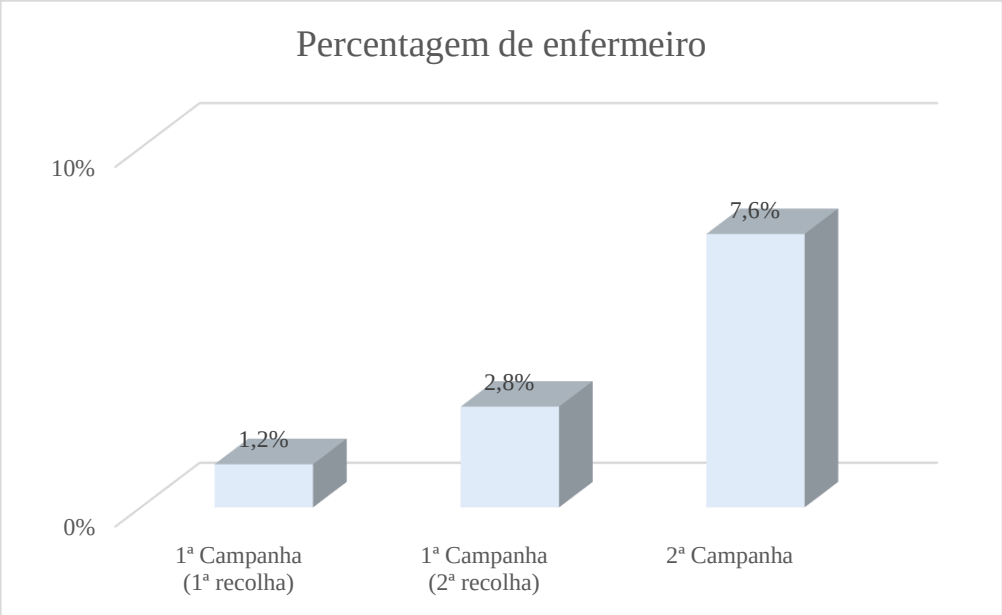


Gráfico 43 - Percentagem de enfermeiros que introduziram credenciais em relação ao total de funcionários

Tendo em consideração que o universo de utilizadores são 1895 no total, se não contemplarmos os prestadores, 1734 e que a categoria dos enfermeiros representam 36.9% dos funcionários, não tendo em consideração a segunda recolha na primeira campanha, a segunda campanha, os enfermeiros já representam 7.6% dos funcionários que cederam credencias, o que implica que 132 utilizadores ficaram expostos só no grupo de enfermeiros, na segunda campanha.

Destacam-se essencialmente três grupos na segunda campanha que aumentaram consideravelmente, os assistentes técnicos, assistentes operacionais e o pessoal técnico de diagnóstico e terapêutica, este último na primeira campanha não teve registo na primeira

recolha e somente um na segunda recolha, surpreendentemente destacou-se na segunda campanha com 32 utilizadores.

Na análise efetuada nas idades, o comportamento não é muito divergente, sendo a facha etária com maior risco entre os 40 e 60 anos, o que totalizaram em ambas as campanhas cerca de 60% dos utilizadores identificados, no entanto estas idades representam praticamente metade dos funcionários.

Em termos de habilitações os funcionários com licenciatura são 45.6% e em ambas as campanhas a percentagem de utilizadores que introduziram credencias com esta habilitação foi cerca de 44% o que foi um resultado coerente.

Um fator mais preocupante prendeu-se efetivamente com a quantidade de utilizadores a não reportar o e-mail rececionado. O esperado seria que mais utilizadores reportassem para o serviço de GTI o e-mail como não fidedigno, o que não se verificou!

Acerca dos quiz elaborados, acho que são uma mais-valia para a instituição e espero que seja um projeto a ser impulsionado pela mesma, pois será sem dúvida uma mais-valia para todos.

Os resultados dos questionários desiludiram-me pelo facto de serem poucos os respondidos, por 70 porcento das respostas acharem que estão suficientemente esclarecidos e 23 por cento ainda acham que estão bastante esclarecidos acerca dos perigos da internet

Só 15 por cento considera que está pouco preparado para os perigos da internet, o que acho um valor baixo para os valores obtidos, no entanto não consigo enquadrar estas opiniões com os utilizadores das campanhas de phishing.

Acho muito positivo, além das reclamações acerca da alteração da complexidade e validade da palavra-passe, quase 90 por centos das respostas acharem que é uma política importante a alteração da complexidade da palavra-passe, sendo uma mais valia para a

segurança de todos, no entanto ainda existe uma pequena percentagem que acha desnecessária a frequência de revalidação da senha.

Quando questionados acerca da importância das campanhas de phishing levadas a cabo na instituição os utilizadores acharam na sua maioria que foram uma mais-valia, inclusive manifestaram interesse na repetição deste tipo de campanhas, todos foram unanimes na continuação de esclarecimentos acerca da cibersegurança e dos perigos de fornecimento de credenciais na instituição.

A consciencialização da vulnerabilidade da instituição em relação aos perigos informáticos não está clara, uma vez que 38.6 por cento das respostas estão indecisos só 11.4 por cento não considera que a instituição está protegida, no entanto cerca de 50 por cento considera a instituição protegida.

Cerca de metade dos utilizadores que responderam consideram que estão suficientemente esclarecidos acerca da importância das suas credenciais e estão devidamente preparados para os perigos da internet e outra metade consideram-se pouco preparados.

Todas as respostas dadas acerca da importância das campanhas de phishing consideraram as mesmas importantes e cerca de 43 por cento considerou de extrema importância, o que considero muito positivo.

Os utilizadores acham importante manter alertas e esclarecimentos acerca dos perigos da internet e a vulnerabilidade de perda de credencias e 51.4 por cento ainda acha este tipo de acções deveriam ser intensificadas.

Este tipo de campanha passou a fazer parte da rotina do serviço de GTI, no entanto, certamente existem muitas mais instituições que relevam este fator de segurança, não implementado sistemas para melhorar a preparação dos utilizadores de forma a garantir uma maior segurança da informação e afiançar o normal funcionamento da instituição.

Dos inúmeros estudos e pesquisas analisados entre os quais alguns que nem chegaram a ser referenciados neste trabalho, sobre a vulnerabilidade dos utilizadores, todos destacaram a importância de soluções comportamentais, treino e consciencialização como forma de preparação para os perigos do phishing e como evitar ser vítima deste tipo de ataques.

Outra dificuldade que foi sentida, foi o facto de tudo ser interno, ou seja, os endereços de e-mail das campanhas de phishing tiveram de ser os do domínio da instituição, neste caso, porque se o e-mail não fosse do domínio não era permitido o envio para vários endereços em simultâneo, não foi permitido serem externos, as páginas das campanhas de phishing tiveram de ser internas, pelo facto de registarem informação dos utilizadores, as páginas foram parametrizadas no integrador Mirth, o que originou que os utilizadores que selecionassem o link quando abrissem o e-mail fora da instituição iriam ver a mensagem de página não encontrada, uma vez que fora não estava acessível. Pode ter havido vários utilizadores a tentar abrir o link no exterior que não foram registados, o que não era pretendido, era suposto registar todas as tentativas de acesso.

Contudo as campanhas foram pertinentes para a consciencialização, tanto dos utilizados assim como da própria instituição, inclusive revelou a necessidade de implementação de um plano de segurança de cibersegurança na mesma. Ficou a vontade e a consciência da necessidade e da importância deste tipo de ações na instituição como mecanismo de defesa dos utilizadores e preservação do bom funcionamento da instituição.

Teria feito sentido a realização de inquéritos antes das simulações dos ataques e após, para poder comparar as respostas dos mesmos, teria de haver mais insistência na solicitação de preenchimento dos inquéritos, uma vez que obtive menos de 4% de respostas em relação ao número de colaboradores.

Na minha opinião as instituições deveriam de estar mais despertas para os perigos da cibersegurança e de implementar mecanismos de consciencialização e treino de práticas com o intuito de aumentar a robustez de segurança das próprias instituições.

Esta opinião é corroborada por diversos estudos realizados, não somente na saúde, mas em muitas outras áreas. É uma debilidade generalizada, como exemplo pela dissertação levada a cabo pela Vanessa Alexandra Nunes Gomes, no Instituto universitário de Lisboa, assim como o Paulo Ricardo Saramago Dias, no Instituto Superior de Tecnologias de Lisboa e muitos mais que identificam o utilizador como fator importante na vulnerabilidade da segurança das instituições.

Existe um longo caminho que já deveria ter sido iniciado e é emergente metodologia de avaliação, consciencialização e treino para com os colaboradores. A instituição deve melhorar as práticas defensivas e preventivas acerca da cibersegurança.

Existem sites de ajuda para prevenir o utilizador de se tornar vítima, nomeadamente a google desenvolveu, à semelhança de muitos outros, acesso na web para validar se o endereço é perigoso/malicioso, https://safebrowsing.google.com, a Microsoft tem página com documentação acerca da prevenção de ataques phishing, Anti-phishing protection - Microsoft Defender for Office 365 | Microsoft Learn, no entanto é necessário proatividade da empresa no alerta dos risco e prevenção acerca desta matéria-

12. CONCLUSÕES

Inicialmente criei uma expectativa de implementação e desenvolvimento do trabalho que na prática não se revelou como espectável, uma vez que as permissões para realizar algo eram demoradas, nomeadamente, foi necessária a aprovação do GTI, seguido pelo GCI em tudo o que era enviado para os utilizadores e posteriormente pelo CA, que consultava o gabinete responsável pelo RGPD, este processo por vezes tornava-se moroso o que criou alguma entropia no desenrolar de todo o processo. Aliado a este processo moroso, o trabalho coincidiu com a restruturação do SNS, ou seja, foram agrupados os ACES aos hospitais, o que implicou grande restruturação no hospital e as prioridades eram mais do que muitas, ficando as minhas solicitações em espera perante as necessidades emergentes da instituição e dos serviços. Além dos contratempos mencionados houve ainda alteração do CA, o que implicou que durante a aproximação do término do mandato e a tomada de posse do seguinte houvesse um período em que não houve seguimento do que não era estritamente necessário à instituição e para passagem de pastas.

Considero que as questões inicialmente colocadas foram efetivamente respondidas, ou seja, a preparação dos utilizadores é frágil, p nível de maturidade dos utilizadores acerca do tema é baico e representa uma grande vulnerabilidade e fragilidade para a segurança da instituição. O impacto das campanhas de phishing foram e são positivas para a preparação dos utilizadores e consequentemente segurança da instituição. Este trabalho foi eficaz deforma a despertar não só os utilizadores, mas também o serviço GTI para a importância e necessidade de investimento de soluções nesta área afinal o azar nem sempre bate só na porta do lado.

Seria interessante, realizar futuramente campanhas de phishing e analisar a evolução do comportamento dos utilizadores, inclusive verificar se haveria utilizadores consecutivamente reincidentes, após os alertas e esclarecimentos efetuados entre campanhas.

Bibliografia

Alexandra nunes Gomes, Vanessa (2019, outubro). A Engenharia Social e os Perigos do phishing

Bikov, T. D., Iliev, T. B., Mihaylov, Gr. Y., & Stoyanov, I. S. (2019, May 1). Phishing in Depth – Modern Methods of Detection and Risk Mitigation. IEEE Xplore. https://doi.org/10.23919/MIPRO.2019.8757074

Camurça, F (2022, 27 de abril). Ataques cibernéticos atingem hospitais em Portugal. Welivesecurity by eset. https://www.welivesecurity.com/br/2022/04/27/ataques-ciberneticos-atingem-hospitais-em-portugal/

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., … Zuccarelli, R. (2017). Assessment of employee susceptibility to phishing attacks at US health care institutions. JAMA Network Open, 1(5), e phishing attacks at US health care institutions. JAMA Network Open, 1(5), e178233. doi: 10.1001/jamanetworkopen.2017.8233.

Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association*, *26*(6), 547–552. https://doi.org/10.1093/jamia/ocz005

Jakobsson, M., & Myers, S. (2006). Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley

Mitnick, K. D., & Simon, W. L. (2003). The Art of Deception: Controlling the Human Element of Security. Wiley.

Pereia, J. P. (2017, 12 de maio). Ataque informático de larga escala afecta empresas em Portugal. Publico. https://www.publico.pt/2017/05/12/tecnologia/noticia/ataque-informatico-internacional-afecta-empresas-e-hospitais-1771939

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: threats, mitigation and approaches. *BMJ Health & Care Informatics*, *26*(1), e100031. https://doi.org/10.1136/bmjhci-2019-100031

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2019). Phishing simulation exercise in a large hospital: A case study. International Journal of Healthcare Management, 12(1), 47-56. doi: 10.1080/20479700.2018.1495804.

Ricardo Saramago Dias, Paulo (2021, dezembro), Prevenir um ataque de phishing

Wittkop, J. (2016). Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices. Syngress.

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2020). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? Journal of Computer Information Systems. https://doi.org/10.1080/08874417.2020.1812134&#8203

Ferramentas ajuda identificação sites maliciosos

Google Safe Browsing. About Safe Browsing. https://safebrowsing.google.com

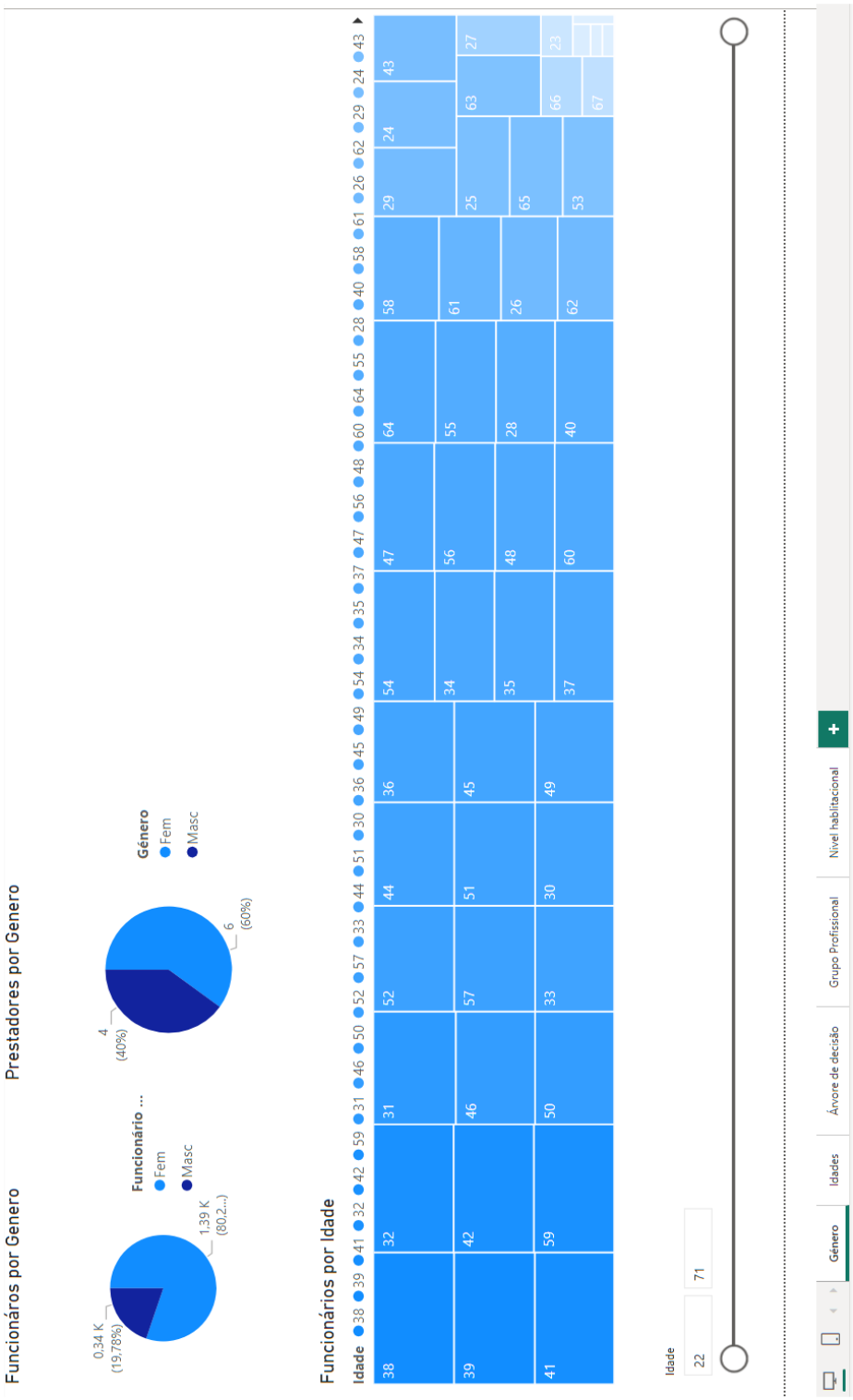
Microsoft. (2021). *Office 365 Phishing Attack Prevention*. Microsoft Documentation

ANEXOS

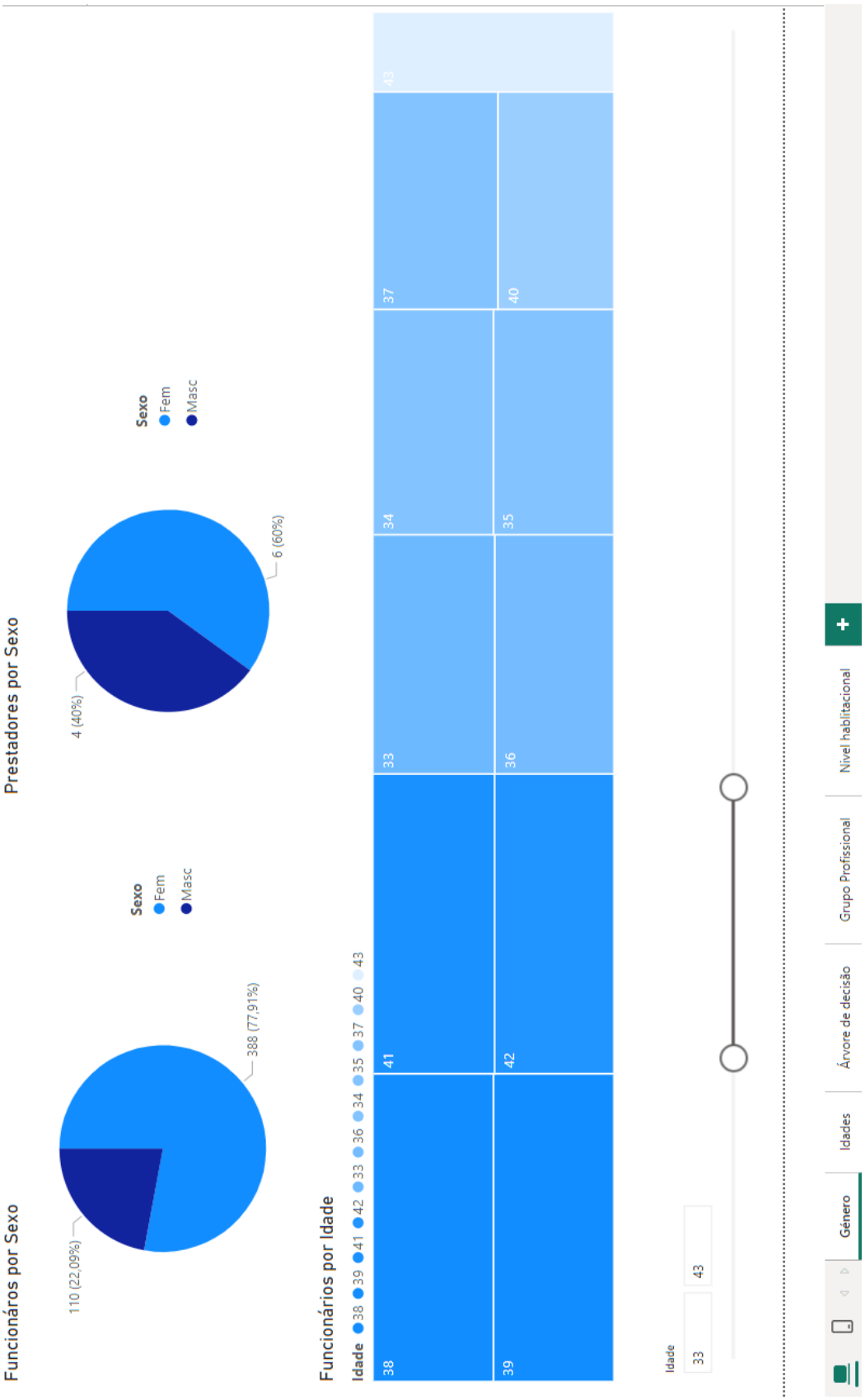
Anexo A - Distribuição de funcionários por categoria profissional e escolaridade

		Técnicos	Pessoal									Conselho	Assistente		Administração	
	TOTAL PARCIAL	Superiores	Técnico Superior de Saúde	Técnico Sup. de Diagnóstico e Terapêutica	Médico	Farmacêutico	em formação pré-carreira Farmacêutica	em formação pré-carreira Médica	Dirigente	de Informática	de Enfermagem	Fiscal	Técnico	Operacional	Hospitalar	
0.1%	**2**													2		menos 4º ano
1.6%	**27**													27		4º ano
4.5%	**78**													78		6º ano
0.2%	**3**													3		7º ano
0.2%	**4**													4		8º ano
8.9%	**155**			1						1			14	139		9º ano
0.3%	**5**												1	4		10º ano
1.9%	**33**										2		14	17		11º ano
14.4%	**249**			1						1	1		75	171		12º ano
0.5%	**9**													9		Ensino Secundário Não Superior de Nível IV
0.1%	**1**													1		Ensino Pós-Secundário Não Superior de Nível V
0.9%	**15**									3			3	9		Curso Técnico Profissional
8.5%	**148**			27					1		114		4	2		Bacharelato
45.6%	**790**	24	3	84	129	9	1	15	7	2	465	2	34	11	4	Licenciatura
2.2%	**38**	1			1			1			35					Pós-Licenciatura (Especialização)
0.9%	**15**	2		3	3						6		1			Pós-Graduação
9.1%	**157**	3	1	14	46		2	72	2		16		1			Mestrado
0.3%	**5**			1				1	1		1	1				Doutoramento
100.0%	**1734**	**30**	**4**	**131**	**179**	**9**	**3**	**89**	**11**	**7**	**640**	**3**	**147**	**477**	**4**	TOTAL PARCIAL
	100.0%	1.7%	0.2%	7.6%	10.3%	0.5%	0.2%	5.1%	0.6%	0.4%	36.9%	0.2%	8.5%	27.5%	0.2%	

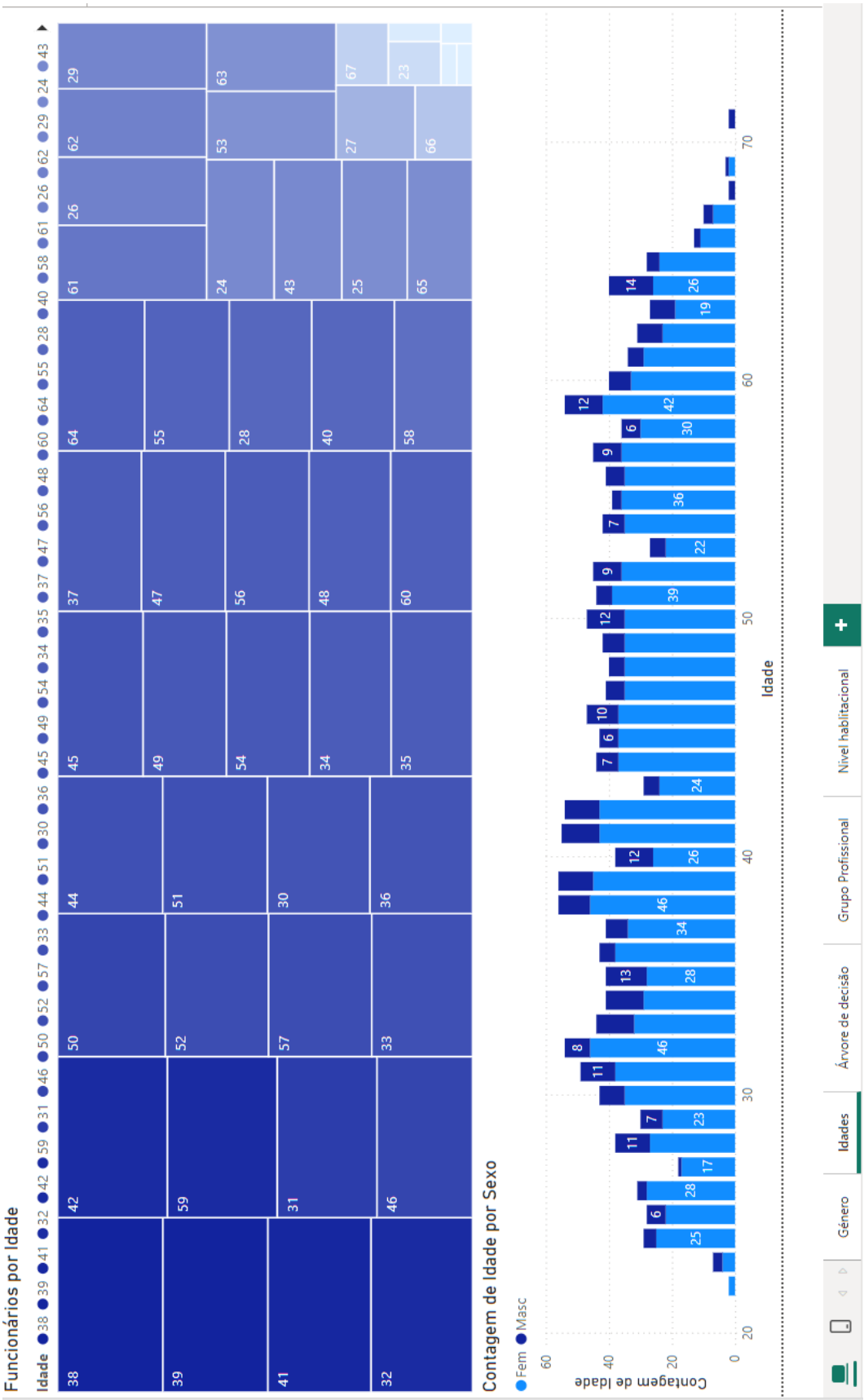
Anexo B – Funcionário e Prestadores por idades



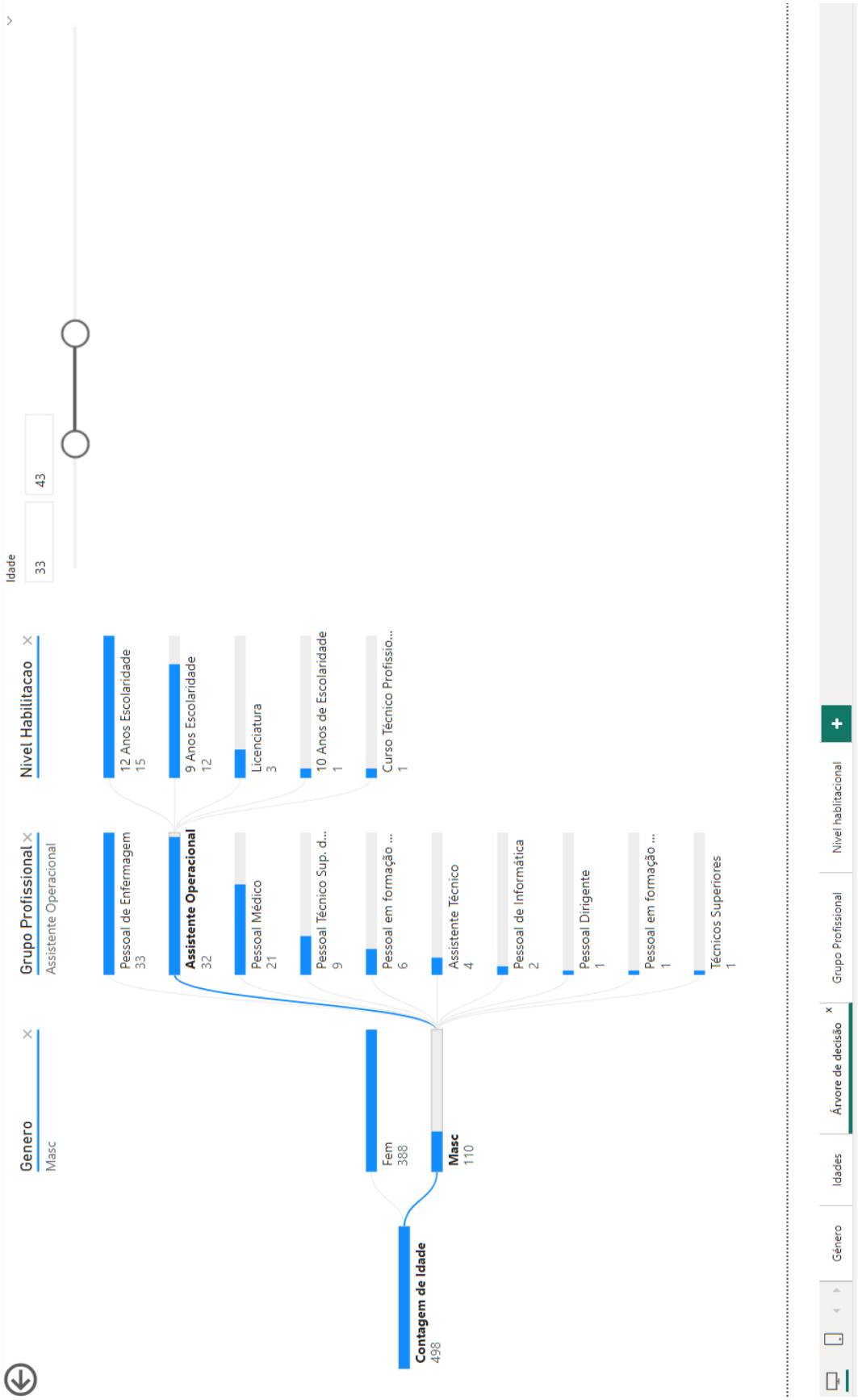
Anexo C – Funcionários e Prestadores por sexo


Funcionários por Sexo
Sexo
Fem
Masc
110 (22,09%)
388 (77,91%)
Prestadores por Sexo
Sexo
Fem
Masc
4 (40%)
6 (60%)
Funcionários por Idade
Idade
38
39
41
42
33
36
34
35
37
40
43
Idade
33
43
Género
Idades
Árvore de decisão
Grupo Profissional
Nível habilitacional

Anexo D – Idades por sexo

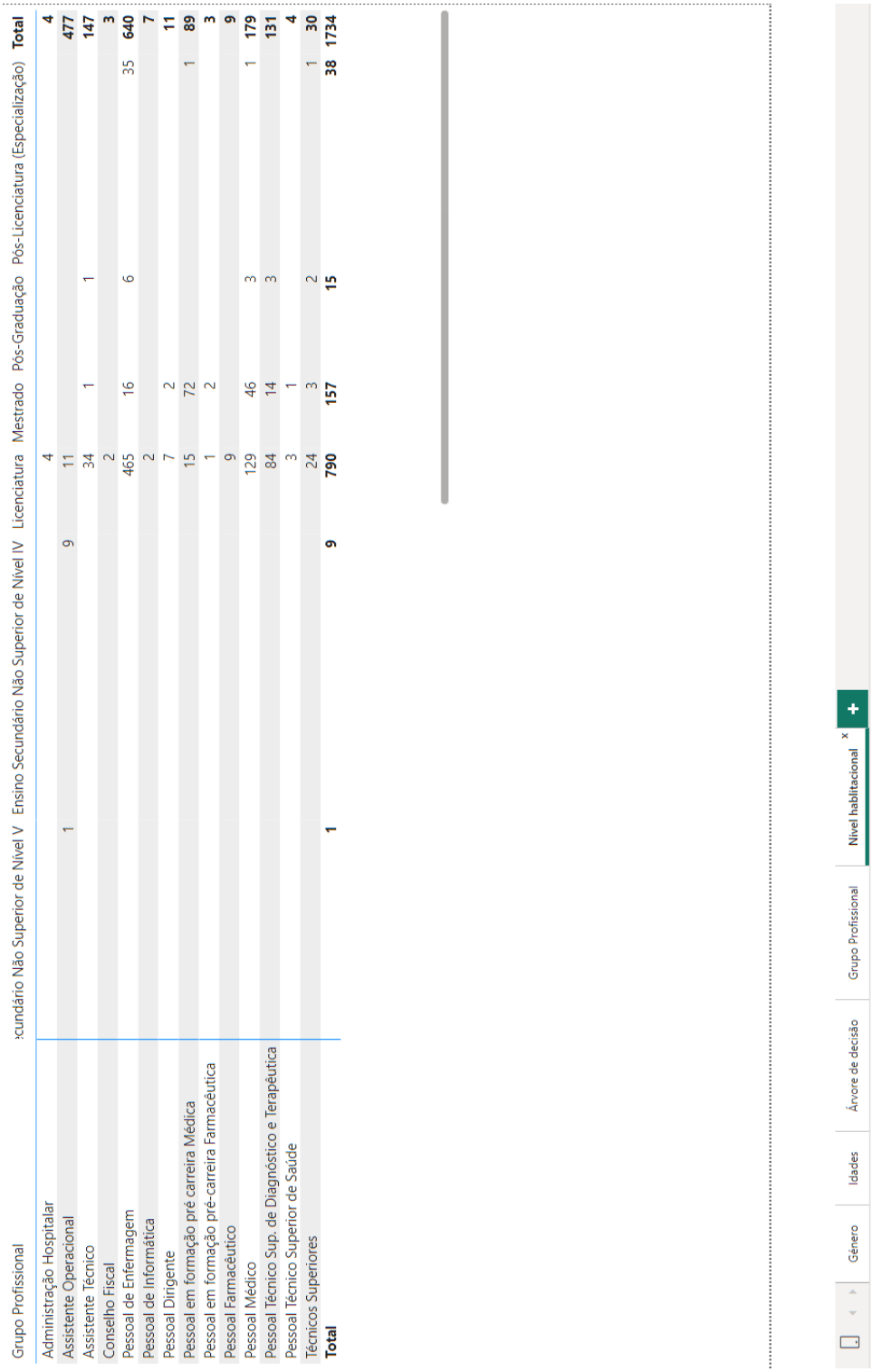


Anexo E – Árvore de decisão da amostra



Anexo F – Nível habilitacional por grupo profissional

Anexo G – Grupo profissional por nível habilitacional



Grupo Profissional	:cundário Não Superior de Nível V	Ensino Secundário Não Superior de Nível IV	Licenciatura	Mestrado	Pós-Graduação	Pós-Licenciatura (Especialização)	Total
Administração Hospitalar			4				4
Assistente Operacional	1	9	11				477
Assistente Técnico			34	1	1		147
Conselho Fiscal			2				3
Pessoal de Enfermagem			465	16	6	35	640
Pessoal de Informática			2				7
Pessoal Dirigente			7	2			11
Pessoal em formação pré carreira Médica			15	72		1	89
Pessoal em formação pré-carreira Farmacêutica			1	2			3
Pessoal Farmacêutico			9				9
Pessoal Médico			129	46	3	1	179
Pessoal Técnico Sup. de Diagnóstico e Terapêutica			84	14	3		131
Pessoal Técnico Superior de Saúde			3	1			4
Técnicos Superiores			24	3	2	1	30
Total	**1**	**9**	**790**	**157**	**15**	**38**	**1734**