INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
MESTRADO NÃO INTEGRADO EM CIÊNCIAS POLICIAIS NA ESPECIALIZAÇÃO EM SEGURANÇA INTERNA

Patrícia Isabel Pinho Santos

SEGURANÇA INFORMÁTICA:
A Importância para a Segurança Interna

Orientador: Professor Doutor Hermínio Matos

Lisboa
2016

PATRÍCIA ISABEL PINHO SANTOS

SEGURANÇA INFORMÁTICA:
A Importância para a Segurança Interna

Dissertação apresentada ao Instituto Superior de Ciências Policiais e Segurança Interna como exigência para a obtenção do grau de mestre em Ciências Policiais, na especialização em Segurança Interna.

Orientador: Professor Doutor Hermínio Matos

Lisboa
2016

AGRADECIMENTOS

A realização desta dissertação de mestrado, que se veio a arrastar durante algum tempo, resultou do apoio, incentivo e estímulo de diversas pessoas, sem as quais este projeto não se teria tornado uma realidade e às quais estou sinceramente e eternamente grata.

Como esta secção de agradecimentos é de espaço limitado, seguramente, não é possível agradecer, conforme deveria, a todos que fizeram parte deste meu percurso…

Ao meu orientador, Professor Doutor Hermínio Matos, por toda a disponibilidade, atenção dispensada, paciência, dedicação e apoio que me deu, bem como o incentivo dado para a elaboração de um melhor projeto… Muito Obrigada.

Desde do início do mestrado, tive o prazer de conhecer e de poder contar com os meus colegas de curso, por todos os momentos que passamos em conjunto, por todo o incentivo e apoio, João Goulão, Miguel Pita dos Santos e Tiago Moniz estamos todos de parabéns por chegarmos a esta fase e a estarmos a terminar!

Queria ainda agradecer ao Instituto de Defesa Nacional, em especial ao Coronel João Barbas e ao Tenente-Coronel Paulo Nunes, coordenadores do III Curso de Cibersegurança e Gestão de Crises no Ciberespaço, por terem aceite a minha candidatura para o curso, que revelou por ser um contributo indispensável para a obtenção de novos conhecimentos e sedimentação de outros, no âmbito da minha dissertação.

Aos meus grandes amigos, Ana Raquel Freitas, Daniel Lopes, Diana Paiva, Márcia Lima e ao Miguel Vale por todo o apoio e incentivo quando mais precisava mesmo que às vezes pensasse que estavam a ser “chatinhos”…. Muito Obrigada pela vossa amizade e por me “aturarem” sei que por vezes sou insuportável…

À Doutora Helena, não há palavras que descrevam o quanto grata lhe estou por sempre estar lá quando mais preciso e por me apoiar sempre em tudo.

Ao Professor Pedro Silva por toda a disponibilidade e ajuda ao longo de todo o meu projeto e, em especial, pela ajuda com a colocação *online* do inquérito.

À Professora Sofia Ventura por toda a disponibilidade e ajuda ao longo de todo o meu projeto.

Ao Hélder (não podia faltar), que apesar de parecer que temos agendas de presidentes, sempre esteve lá a apoiar-me quando precisei e por, aumentar os meus conhecimentos informáticos de iniciante… Muito Obrigada!

À minha família que, independentemente de tudo e cada um à sua maneira, esteve sempre presente e me apoiou incondicionalmente, como tal agradeço-vos "individualmente" como todos merecem: À minha irmã, por todo o interesse demonstrado no que faço mesmo que seja um tema do qual não lhe interesse tanto. Aos meus avós maternos, por mesmo que não percebam nada dos temas dos meus trabalhos e, em especial, desta dissertação de mestrado, sempre me ajudaram. À minha mãe, por sempre me ajudar a acalmar e a pensar positivo no trabalho que faço… sei que fico insuportável por ser demasiado perfeccionista. Ao meu avô paterno, que apesar de só começarmos a ter contacto há relativamente pouco tempo, sempre me incentivou e apoiou em tudo o que faço… podemos ter perdido muito tempo mas ganhamo-lo agora! Ao meu tio Manel e à minha tia Lúcia, por todos os momentos e brincadeiras em família! Ao meu tio Filipe, que apesar de também começarmos há pouco tempo a ter contacto, foi também um membro importante para este e outros projetos!

Por último, mas não menos importante, gostava de agradecer a todos os que se disponibilizaram no preenchimento completo do inquérito, pois sem as vossas respostas não seria possível chegar aos resultados obtidos. Muito, mas mesmo, Muito Obrigada!

Resumindo, Muito Obrigado a todos que apoiaram de alguma maneira este projeto a concretizar-se, sem todos vocês, talvez este projeto não chegasse ao fim.

RESUMO

A criação da Internet acarretou benefícios, mas também trouxe desvantagens, como a criação de novos crimes ou a prática dos crimes convencionais, através do uso informático.

A criminalidade, gerada por estes novos crimes, deve-se à falta de segurança, podendo ser minimizada pela sensibilização da população para as medidas de segurança que devem ter.

O exponencial crescimento e dependência das Tecnologias de Informação e Comunicação, no quotidiano, dos diversos sectores económicos e governamentais, possibilita um ataque informático a estas entidades que, por consequência, colocam em causa a segurança de uma nação. Perante este estado de risco de uma emergente ameaça informática é imperativo a delineação de medidas e estratégias de segurança.

Assim, o impacto que estes ataques informáticos têm na segurança nacional compromete a economia, o funcionamento do próprio Estado, bem como todos os habitantes do país. Um caso que referencia a importância de proteger o Estado virtualmente é os ataques informáticos dirigidos, em 2007, durante semanas, à Estónia, em que diversos *sites* de jornais, emissoras de televisão e quase todos os *sites* governamentais ficaram inacessíveis.

Com esta dissertação pretende-se analisar a ligação entre a segurança interna com a segurança informática. Pretendendo, também, através da realização de um inquérito *online*, analisar se os habitantes em Portugal se encontram informados dos perigos da *Internet* e de como se devem proteger dos mesmos.

Palavras-chave: Segurança; Segurança Interna; Segurança Informática; Ciberespaço; Cibersegurança; Ciberdefesa

ABSTRACT

The creation of the Internet has brought benefits, but also brought disadvantages, such as creating new crimes as the practical of conventional crimes by using a computer.

The criminality made by these new crimes, due to the lack of security, and can be minimize by the public awareness of safety measured that they should have.

The exponential growth and dependence on information and communication technologies, in everyday life, of the diverse economic and government sectors, enables a cyberattack to these entities. Consequently, it put in danger the security of a nation. Towards, this state of risk of an emerging cyber threat is imperative to the delineation of measures and security strategies.

Therefore, the impact that these cyber-attacks have on national security compromises the economy, the operation of the State itself, as well as all the country's habitants. A case that references the importance of protecting the State virtually is the cyber-attacks, in 2007, during for weeks, on Estonia, in which multiple sites of newspapers, television stations and almost all government sites were inaccessible.

We intend, with this thesis, analyze the connection between homeland security with cyber security. We also intending, through an online survey evaluate if the Portugal's habitants are informed of Internet dangers and how they can protect themselves.

Keywords: Security; Homeland Security; Cyberspace; Cyber Security; Cyber Defense

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABELAS

LISTA DE ABREVIATURAS

ARPANET.....*Advanced Research and Projects Agency*
CERN .....Organização Europeia para Investigação Nuclear
CNCS .....Centro Nacional de Cibersegurança
CP .....Código Penal
DGPJ.....Direção-Geral da Política de Justiça
PJ .....Polícia Judiciária
RASI .....Relatório Anual de Segurança Interna
SG-SSI .....Secretário-Geral do Sistema de Segurança Interna
TIC.....Tecnologias de Informação e Comunicação
UCAT.....Unidade de Coordenação Antiterrorismo

1 INTRODUÇÃO

A presente dissertação aborda o tema da Segurança Informática, na vertente em que esta é importante na Segurança Interna de um país ou Estado.

Este trabalho é de extrema importância a todos os níveis, em especial académico-cientifico, uma vez que pode beneficiar o leitor/sociedade, por este ser um tema relativamente pouco estudado, no nosso país.

1.1 Objetivos

Com esta dissertação pretendemos analisar se o aumento da segurança e defesa de um país, a nível informático, se constrói através da utilização de medidas de segurança. E, assim, deste modo, tornar as pessoas mais conscientes para esta realidade.

O estudo desta dissertação tem por base analisar a interligação da segurança interna com a segurança informática, em como esta última se torna indispensável para um país, complementando com a estratégia nacional de cibersegurança. Pretende, também, analisar se os cidadãos conhecem os perigos que a *Internet* acarreta e se, por conseguinte, se sabem proteger ou prevenir destes perigos.

1.2 Metodologia

Na metodologia desta dissertação, tendo em conta o objetivo da mesma, inicialmente incidimos numa pesquisa bibliográfica, através da legislação nacional e internacional, da pesquisa de livros, artigos científicos e de fontes abertas de domínio público.

Posteriormente, realizamos um inquérito *online* acerca da segurança informática e das medidas de segurança. Estes resultados foram tratados e analisados de modo a contextualizar as respostas com o facto das pessoas se encontrarem informadas sobre os perigos da *Internet* e como se devem proteger dos mesmos.

1.3 Estrutura do Trabalho

A dissertação está organizada nos seguintes capítulos, com os respetivos subcapítulos:

1) Introdução – Indicação do tema do trabalho e os seus objetivos, bem como a metodologia utilizada, a estruturação do mesmo e a norma de referenciação bibliográfica utilizada;
2) Enquadramento Geral – Caracterização, sucinta, da evolução da Internet, bem como da evolução da criminalidade informática em Portugal;
3) Segurança – Definição de segurança, segurança interna e segurança informática;
4) Cibersegurança e Ciberdefesa – Definição de cada um dos conceitos, bem como caracterização das ameaças, dos atores e dos crimes cometidos no ciberespaço;
5) Centro Nacional de Cibersegurança – Descrição desta entidade e da Estratégia Nacional de Cibersegurança criada;
6) Resultados e Discussão dos mesmos – Apresentação e análise dos resultados do inquérito;
7) Considerações Finais – Enunciar as ideias relevantes do trabalho, tendo em conta os objetivos do mesmo.

Esta dissertação contém elementos pré-textuais (Agradecimentos, Resumo, *Abstract* e Lista de Abreviaturas) e pós-textuais (Referências Bibliográficas e Apêndices).

A norma de referenciação bibliográfica utilizada ao longo desta dissertação é a APA 6th.

2 ENQUADRAMENTO GERAL

Neste capítulo faremos uma breve introdução histórica da evolução da Internet, no Mundo, e da Criminalidade Informática, em Portugal.

2.1 Internet

A *Internet* é uma rede capaz de interligar todos os computadores do mundo, tendo como possibilidade a distribuição da informação a nível mundial. Assim, esta torna-se um meio de cooperação e interação entre os indivíduos e os seus computadores, independentemente da sua localização (Muniz, 2012).

Para entendermos um pouco mais sobre esta rede precisamos de conhecer a sua origem, isto é, porque foi criada e com que propósito.

Nos finais dos anos 50, no auge da Guerra Fria, o Departamento de Defesa dos Estados Unidos queria a criação de uma rede, de comando e controlo, capaz de sobreviver a uma guerra nuclear (Tanenbaum & Wetherall, 2011). Esta rede era necessária uma vez que o sistema a ser utilizado naquela época era vulnerável e as Forças Armadas norte-americanas necessitavam de manter as comunicações em caso de um ataque das forças inimigas, destruísse esse sistema (Muniz, 2012).

Em 1969, uma agência de investigação norte-americana – *Defense Advanced Research Projects* (DARPA) – lançou um projeto cujo objetivo era o desenvolvimento de uma rede experimental robusta e fiável. Este projeto, apelidado de ARPANET, estava em funcionamento com quatro computadores em rede (Tanenbaum & Wetherall, 2011; Ventura, 2015).

Um dos grandes problemas desta rede era a ligação a redes físicas separadas sem que estas aumentassem os recursos de rede para endereços constantes. A sua solução passou pelo que conhecemos hoje como “troca de pacotes”, que envolve pedidos de dados que são divididos em pequenos fragmentos (“pacotes”). Estes podem ser processados rapidamente e assim não bloqueiam a comunicação de outras partes (Francis, 2008).

Depois de finalizada a fase experimental da ARPANET, sucedeu a fase operacional, onde foram desenvolvidos diversos protocolos, que ainda hoje são a base da atual *Internet*, por exemplo, os protocolos TCP/IP – *Transmission Control Protocol/Internet Protocol* (Ventura, 2015). Assim, este protocolo fomentou a integridade da transmissão para um computador servidor, diminuindo o papel da rede, tornando

possível a comunicação, com facilidade quase em todas as redes, em simultâneo (Alves, 2006; Francis, 2008).

Neste ano, a ARPANET foi dividida em dois componentes: a MILNET (uma rede para fins e ambientes militares) e a ARPANET (a restante rede que chega à população geral). A rede global, composta por estas duas, foi denominada de *Internet* (Ventura, 2015). Em 1990, o engenheiro inglês Tim Berners-Lee desenvolveu o *World Wide Web*. Este sistema possibilitou o uso da interface gráfica e a criação de *sites* mais dinâmicos e visualmente cativantes. A 20 de Abril de 1993, a Organização Europeia para Investigação Nuclear (CERN) colocou o código-fonte do *World Wide Web* em domínio público, permitindo que qualquer pessoa pudesse alterar ou modificar o mesmo, sem qualquer taxa indexada (Francis, 2008; Muniz, 2012).

Desde 1993 até hoje, 2016, a *Internet* tem sofrido inúmeras alterações. De uma forma geral, muito sucintamente, a **Figura 2.1** demonstra a evolução da Internet desde a sua criação até aos dias de hoje. Uma rede que, em 2009, contava com 685 milhões de computadores ligados entre si. Este número continua a crescer com a introdução de dispositivos móveis no mercado (Ventura, 2015).

> *"Internet fará parte integrante do nosso dia-a-dia, desde o acordar até ao deitar. Em qualquer dispositivo, e qualquer lugar, na escola, trabalho e em casa…." Corning Incorporated (retirado de Brandão, 2013).*

Figura 2.1 Evolução sucinta da *Internet*.

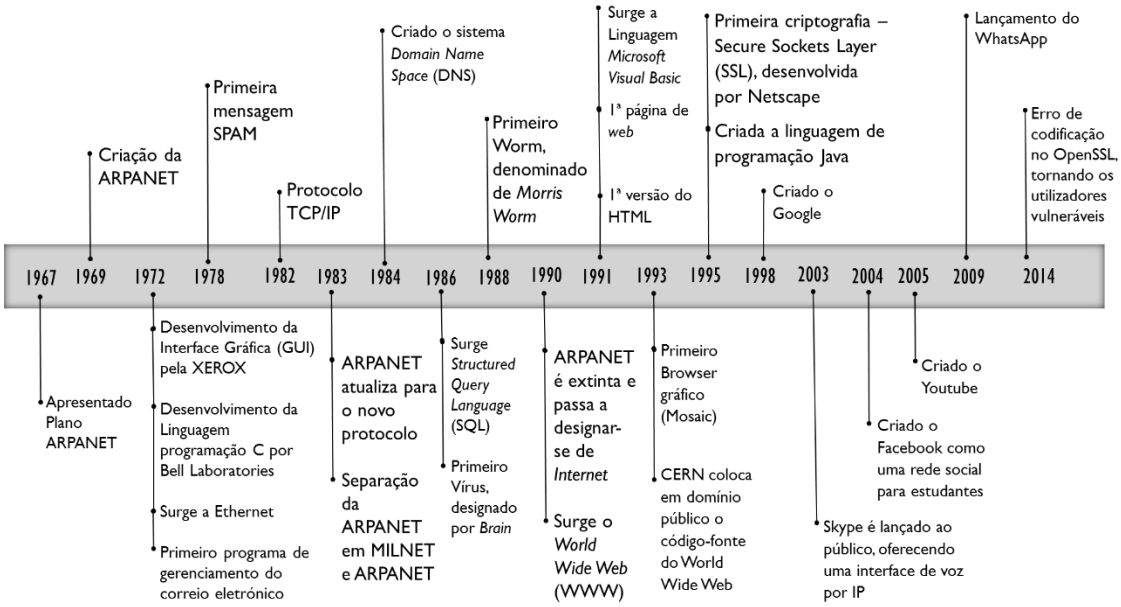


Imagem feita pelo autor com recurso a Flloress, 2010; Francis, 2008; Hollinger & Mart, n.d.; Muniz, 2012; Ventura, 2015.

2.2 Criminalidade Informática

Atualmente, vivemos numa *Cyber Era*, como muitos consideram. A evolução da tecnologia possibilitou que, hoje em dia, a *Internet* se torne um instrumento imprescindível para qualquer organização, ou pode-se mesmo dizer indispensável para qualquer indivíduo, tanto a nível pessoal como profissional. Infelizmente, este evoluir da tecnologia também trouxe consigo "novas ameaças que colocam em perigo toda a comunidade que a utiliza" (Souza & Medeiros, 2011).

O crime deixou de ser tão convencional. Novas ameaças surgiram e ameaças conhecidas passaram a ter uma vertente informática, consequentemente, a legislação vigente teve de ser alterada em função destas ameaças. Por conseguinte, originou a criação de uma nova forma de criminalidade – o crime informático ou cibercrime.

O crime informático define-se, segundo um acórdão do Tribunal da Relação do Porto, como "*todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo desse ato*" (Portugal, 2015a).

No entanto, nem sempre foi assim, inicialmente este tipo de crimes apenas estava exposto em alguns artigos do Código Penal (CP), crimes como a burla informática e nas comunicações (art.º 221.º), a devassa por meio de informática (art.º 193.º), a difusão de pornografia infantil (art.º 172.º, atualmente, descrito no art.º 176.º - Pornografia de menores) e o abuso de cartão de garantia ou de crédito (art.º 225.º). Posteriormente, em 1991, foi criada a Lei da Criminalidade Informática (*Lei n.º 109/1991, de 17 de Agosto, da Assembleia da República*) onde foram inseridos seis novos crimes ligados à informática: Falsidade informática (art.º 4.º), Dano relativo a dados ou programas informáticos (art.º 5.º), Sabotagem informática (art.º 6.º), Acesso ilegítimo (art.º 7.º), Intercepção ilegítima (art.º 8.º) e Reprodução ilegítima de programa protegido (art.º 9.º).

Com a Convenção sobre o Cibercrime (a 23 de novembro de 2001) houve uma maior preocupação com esta temática, uma vez que até ao momento algumas definições, como «dados informáticos» (conceito alargado do já descrito em «programa informático»), «fornecedor de serviço» e «dados de tráfego», não estavam contempladas na legislação portuguesa. Foram efetuadas alterações nas legislações em vigor e foi criada a Lei do Cibercrime (*Lei n.º 109/2009, de 15 de Setembro, da Assembleia da República*).

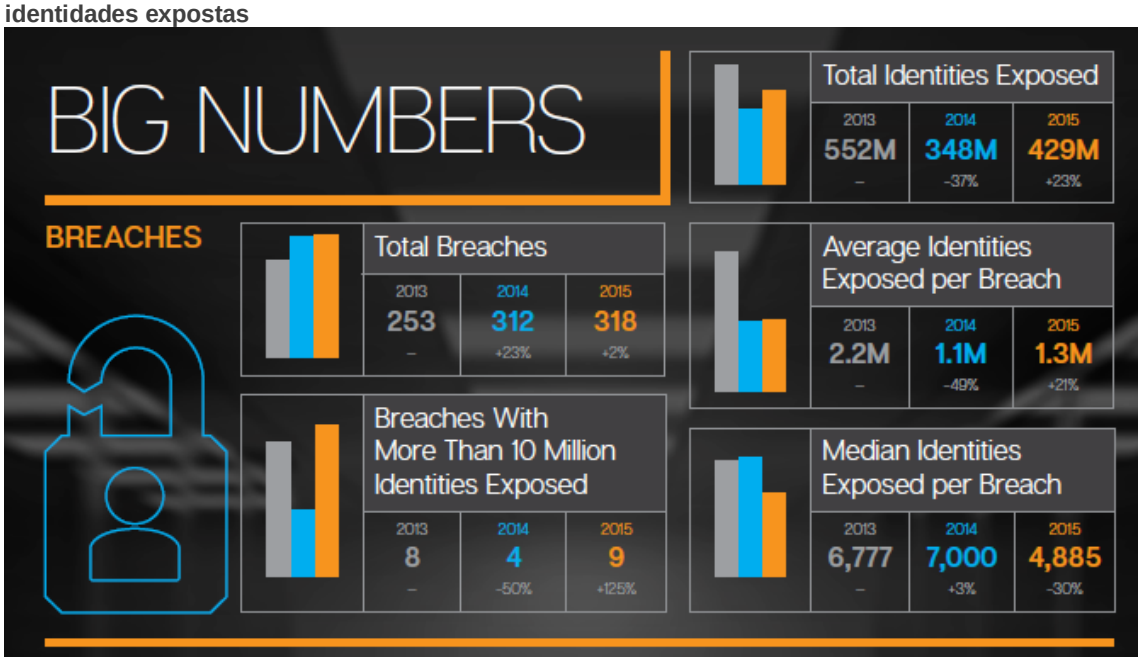
Esta doutrina distingue a criminalidade relacionada com a utilização de computadores e da *Internet* em quatro grupos (Dias, 2012):

1) Crimes que recorrem a meios informáticos, não alterando o tipo penal comum, por exemplo, devassa por meio de informática (art.º 193.º do CP) e burla informática e nas comunicações (art.º 221.º do CP);
2) Crimes relativos à proteção de dados pessoais ou de privacidade, descritos na Lei n.º 67/98, de 26 de outubro;
3) Crimes informáticos, em sentido estrito, ou seja, crimes praticados com a utilização de um meio informático. Neste grupo incluem-se os crimes previstos na Lei do Cibercrime;
4) Crimes relacionados com o conteúdo, onde temos, por exemplo, a difusão de pornografia infantil (art.º 176.º do CP).

Assim, como podemos observar, a legislação portuguesa tem vindo a sofrer diversas alterações a nível do direito informático, mas mesmo assim continua com algumas falhas. Uma das razões é o avanço tecnológico e as inúmeras possibilidades que a *Internet* traz aos criminosos.

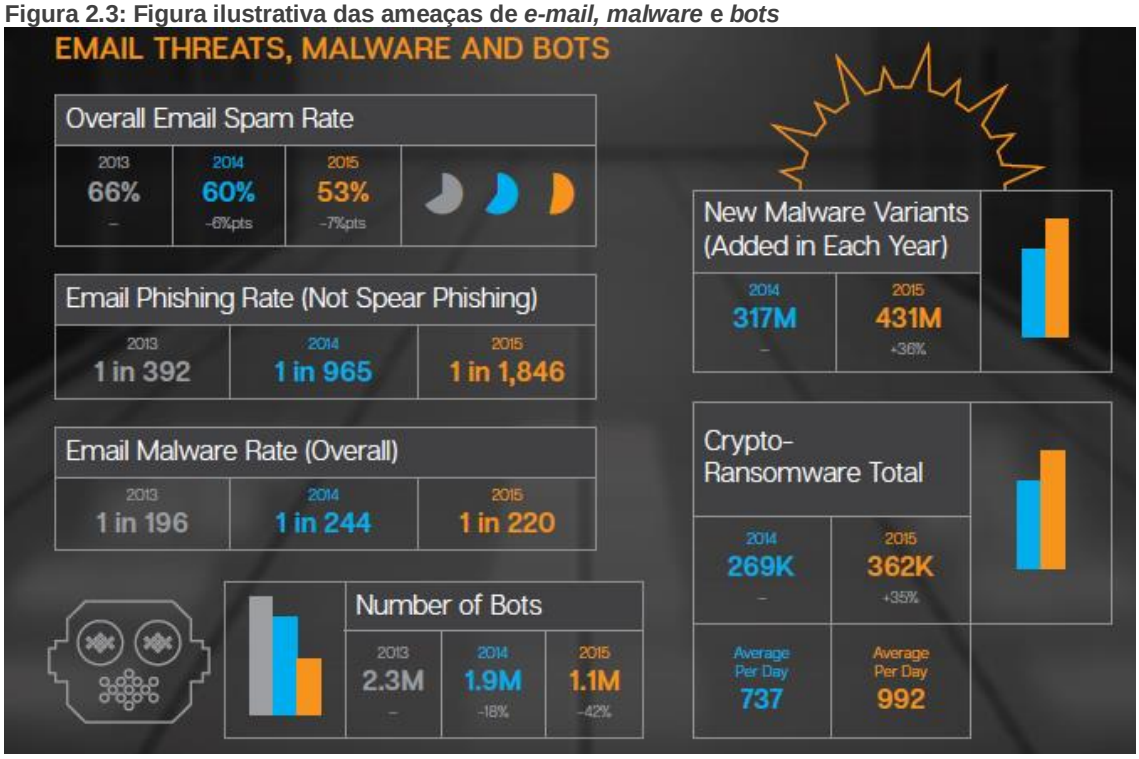
Segundo o Relatório de Ameaças à segurança na *Internet*, da Symantec, em 2015, descobriram mais de 430 milhões de tipos exclusivos de *malware*, o que não é uma surpresa na medida em que a aceleração das ameaças informáticas contra empresas e países ocupam os *media* com alguma regularidade.

Figura 2.2: Figura ilustrativa do número total de quebras de segurança e do número total de identidades expostas



Fonte: Symantec, 2016

Figura 2.3: Figura ilustrativa das ameaças de *e-mail, malware* e *bots*



Fonte: Symantec, 2016

Comparando a evolução dos registos deste tipo de crime podemos observar que, em Portugal, no Relatório Anual de Segurança Interna (RASI), só a partir de 2014 os crimes informáticos foram objeto de uma apreciação mais profunda, antes eram apenas referidos os números de participação deste tipo de crime, descrito em legislação avulsa. Contudo, os crimes informáticos só incluem o acesso indevido ou ilegítimo/interrupção ilegítima, falsidade informática, sabotagem informática, reprodução ilegítima de programa protegido, viciação ou destruição de dados/dano relativo a dados/programas e outros crimes informáticos. Deste modo, a burla informática e nas telecomunicações faz parte das estatísticas de crimes de burla.

Há que ressalvar que o crime de burla informática e nas comunicações teve, em 2015, 7830 participações de crimes, aumentando mais de 73,7% em relação ao ano anterior que só teve 4508 participações (MAI, 2016).

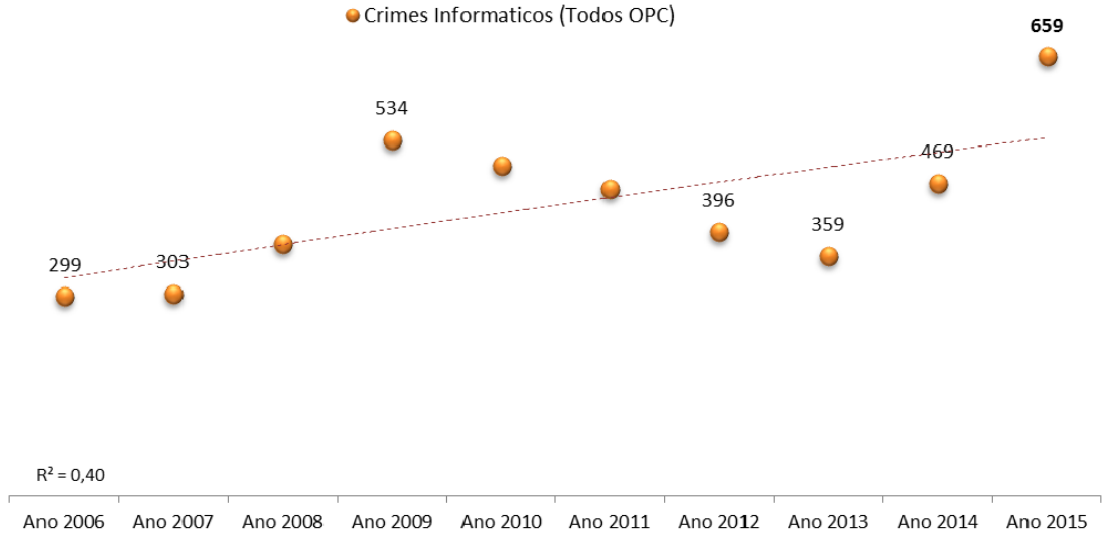
Observando e refletindo acerca dos dados estatísticos do RASI e do *site* da Direção-Geral da Política de Justiça (DGPJ), podemos concluir que os crimes informáticos têm vindo a aumentar, mas no período de 2009 a 2013 houve sensivelmente um decréscimo. Porém, nestes dois últimos anos houve um grande aumento, atingindo em 2015 o valor mais elevado de crimes registados (659 registos), desde 1998. Contudo, desses 659 crimes registados, só em 414 deles foram constituídos arguidos (DGPJ, 2016; MAI, 2016).

Tabela 2.1: Crimes informáticos registados, segundo o tipo de crime, no período de 2008 a 2015

Crime \ Ano	2008	2009	2010	2011	2012	2013	2014	2015
Falsidade Informática	5	6	34	39	59	36	49	101
Sabotagem Informática	8	16	13	12	17	21	37	76
Reprodução Programa protegido	70	97	48	41	12	17	36	28
Acesso/Intercepção ilegítimos	253	378	353	333	278	259	304	409
Vic./destruição/dano dados/programas	11	8	8	7	7	13	11	11
Outros crimes informáticos	31	29	39	28	23	13	32	34
TOTAL	**378**	**534**	**495**	**460**	**396**	**359**	**469**	**659**

Fonte: DGPJ, 2016

Gráfico 2.1: Gráfico dos crimes informáticos registados desde 2006 a 2015, por todos os Órgãos de Polícia Criminal



Fonte: MAI, 2016

A Polícia Judiciária (PJ) dedica especial atenção a três métodos utilizados na prática de crimes informáticos, pelo seu crescimento exponencial e danos sociais e económicos que causam (MAI, 2015):

1) Meios de pagamento, envolvendo aqui áreas da banca *online* e do *phishing*, devido à ameaça que acarreta ao património de empresas e particulares, à credibilidade do sistema financeiro e ao financiamento de outras atividades criminosas;

2) *Hacking,* principalmente o que tem as instituições do Estado como alvo, com consequências ao nível da proteção de dados pessoais, da gestão de serviços públicos e da credibilidade do próprio Estado de direito;
3) *Malware,* sobretudo com a produção e utilização de programas maliciosos e com a possibilidade de utilização em todo o tipo de dispositivos móveis, com implicações nos dois pontos anteriores.

Podemos também relacionar os registos dos crimes informáticos com a sua localização, chegando à conclusão de que na sua maioria é cometido, como é de se esperar, no Continente contudo, tem vindo a aumentar os registos em que não se sabe a localização (DGPJ, 2016). Tal pode dever-se ao facto de neste tipo de crimes, o criminoso poder encobrir a sua identidade, localização, entre outras informações acerca dele. No Continente temos, em 2015, 421 registos de crimes informáticos (DGPJ, 2016).

Tabela 2.2: Crimes informáticos registados, segundo a localização, no período de 2008 a 2015

Ano / Localização	2008	2009	2010	2011	2012	2013	2014	2015
Continente	156	395	329	280	207	173	295	421
Região Autónoma dos Açores	…	11	28	27	5	15	16	22
Região Autónoma da Madeira	…	5	…	8	10	7	6	4
N. E.	220	123	136	145	174			
TOTAL	**378**	**534**	**495**	**460**	**396**	**359**	**469**	**659**

Fonte: DGPJ, 2016

3 SEGURANÇA

Este capítulo irá centrar-se em duas vertentes da segurança: a segurança interna e a segurança informática. Estas duas vertentes, com a passagem dos anos, têm vindo a associar-se de tal maneira que se tornam complementares.

"A segurança é um anseio de todo o ser vivo." (Nunda, n.d., p. 28)

O conceito de segurança é sem dúvida o conceito "*mais ambíguo e perturbador relativamente ao edifício político-estratégico*" (Borges, 2010, p. 8). Ao longo da história, este conceito tem tomado diversas definições consoante a época, pode-se dizer que vai do individuo (em si) até à sociedade de forma a contextualizar-se no meio ambiente em que está inserido, ou seja, a proteção dos cidadãos e da nação.

Segundo o General Cabral Couto, a segurança "*exprime a efectiva carência de perigo, quando não existem (ou foram removidas) as causas dele*" (Sequeira, 2004, p. 57).

Este conceito como referido é um conceito complexo. Na tentativa de chegar a uma definição mais concreta, existem três objetivos que se encontram sempre assentes nestas definições (Sequeira, 2004):

1) Garantir os direitos do cidadão proporcionados pelas normas jurídicas, bem como pelas autoridades que os editam e aplicam;
2) Salvaguardar a ordem constitucional democrática contra perturbações graves de origem interna;
3) Preservar a coletividade contra agressões e ameaças externas.

A segurança tem tomado um rumo cada vez mais científico e académico, no qual se enquadra a segurança como um objeto. No entanto, para se estudar a "segurança" não podemos colocar de lado o que a compõe (os vários atores e as várias ciências do discurso), pois sem isto estaríamos a reduzi-la a um sistema fechado e inócuo (Valente, 2013).

Com o surgimento de "novas ameaças", este conceito voltou a alterar a sua definição passando a designar-se de "*um estado ou uma situação de relação de forças condicionada à percepção por parte do Estado ou sociedade de um perigo iminente, que visa modificar as condições de equilíbrio e estabilidade*", isto é, não haver perigo de um ataque militar, pressão política ou coerção económica (Mathias, 2016).

"A história ensina-nos que o passado é o espelho dos erros do presente e do futuro, principalmente quando lhe atribuímos um papel menor." (Valente, 2013)

3.1 Segurança Interna

A segurança interna, em Portugal, segundo a lei vigente, consiste numa "*atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger as pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática*" (n.º 1 do artigo 1.º da *Lei n.º 53/2008 de 29 de Agosto, da Assembleia da República*, com respetiva atualização pela *Lei n.º 59/2015 de 24 de junho, da Assembleia da República*).

Continuando, para o n.º 3 do mesmo artigo, podemos assentar em quatro pilares a segurança interna (prevenção, ordem pública, informação e investigação criminal), que se encontram interligados com a cooperação internacional, como podemos observar na seguinte figura:

Figura 3.1: Os quatro pilares da Segurança Interna, interligados com a Cooperação Internacional.

Fonte: Adaptado de Matos, 2014

Enquanto atividade, a segurança interna não pode ser abordada sem nos referirmos à inteligência (tradicionalmente designada, em Portugal, por informações), uma vez que esta é um dos pilares essenciais a par dos quatro pilares referidos anteriormente (Fernandes, 2014b).

Até ao momento ainda existe uma certa resistência à adoção de melhores vocábulos, tradicionalmente como declara o autor Luís Fiães Fernandes "*A tradução portuguesa* assume que *dados* são equivalentes a *informação* e que *informações* são equivalentes a *inteligência*" (Fernandes, 2014b). Contudo, para evitar equívocos com o

vocábulo «informações» iremos utilizar os vocábulos «dados», «informações» e «inteligência».

Por «dados» subentende-se "*partículas elementares constituintes das informações*". «Informações» "*são constituídas por conjuntos de dados que, quando organizados e contextualizados, têm o potencial de perder o seu carácter ambíguo*". Por último, a «Inteligência» "*é o resultado de um processo que utiliza informações, integradas num quadro coerente, permitindo produzir inferências e conclusões sobre determinado incidente ou fenómeno, destinada a cliente (s) específico (s)* " (Fernandes, 2014a).

Este último conceito, no sentido orgânico, refere-se aos serviços que desenvolvem atividades de inteligência e que têm como objetivos apoiar o processo de decisão político-estratégico e garantir que outras organizações da mesma natureza, mas pertencentes a outros atores estatuais, não prejudiquem os interesses do Estado (Fernandes, 2014b).

O Sistema de Segurança Interna é definido como o "*conjunto de órgãos aos quais cabe a manutenção da ordem e da segurança pública e a protecção e integridade do Estado de Direito Democrático*". Contudo, com as "novas ameaças" cada vez mais a segurança interna e externa associam-se e dão lugar a uma perspetiva de "segurança e defesa" (Matos, 2010).

Deste modo, não obstante a junção conceptual, é da competência da segurança interna conhecer as ameaças e potencialidades de um adversário, isto é, torna-se imprescindível para um Estado o papel da Inteligência, no conhecimento das vulnerabilidades, intenções e capacidades desse adversário (Matos, 2010).

> "*Apenas o soberano iluminado e o general de valor são capazes de se servir das pessoas cuja inteligência as torna próprias para actuar como agentes e realizar grandes feitos. As operações secretas são básicas na guerra, pois delas dependem todos os movimentos dos exércitos. (...) Um exército sem agentes secretos é como um homem sem olhos e sem ouvidos*." *(Tzu, 1993)*

Sun Tzu na citação anterior acredita que qualquer conquista militar é realizada através do conhecimento, em particular com informações sobre o inimigo (F. Martins, 2010).

Assim, como declara o autor Luís Fiães Fernandes no seu livro através de uma citação do General Pedro Cardoso, "a inteligência tem uma função de apoio aos poderes

judicial, legislativo e executivo permitindo que “estes sejam exercidos com uma profunda e oportuna previsão das dificuldades”, acrescentando que quem tem por missão “garantir a integridade territorial e a defesa das fronteiras terrestres e marítimas e do espaço aéreo, não pode dispensar um conhecimento, o mais completo possível e oportuno, das atividades hostis e das ameaças” (Fernandes, 2014b).

Os órgãos que compõem o sistema de segurança interna são: o Conselho Superior de Segurança Interna, o Secretário-Geral do Sistema de Segurança Interna (SG-SSI) e o Gabinete Coordenador de Segurança (n.º 1 do artigo 1.º da *Lei n.º 53/2008 de 29 de Agosto, da Assembleia da República*, com respetiva atualização pela *Lei n.º 59/2015 de 24 de junho, da Assembleia da República*). Cada um destes órgãos integra outros serviços e forças de segurança como se pode observar no **Apêndice A**.

O Primeiro-Ministro é politicamente responsável pela direção e coordenação das estratégias da política de segurança interna, bem como lhe compete convocar e presidir às reuniões do Conselho Superior de Segurança Interna. Este deve, também, manter informando o Presidente da República sobre todos os assuntos respeitantes à condução da política de segurança interna (*Lei n.º 53/2008 de 29 de Agosto, da Assembleia da República*).

Na Lei de Segurança Interna, o SG-SSI, é equiparado, para efeitos legais, a um Secretário de Estado, e funciona na dependência direta do Primeiro-Ministro. Neste mesmo diploma designa-lhe competências de coordenação, direção, controlo e comando operacional das forças e dos serviços de segurança. Compete-lhe, ainda, a coordenação da Unidade de Coordenação Antiterrorismo – UCAT (*Lei n.º 53/2008 de 29 de Agosto, da Assembleia da República*, com a respetiva atualização da *Lei n.º 59/2015 de 24 de junho, da Assembleia da República*).

A UCAT é o órgão de coordenação e partilha de informações, no âmbito do terrorismo, entre os serviços que a integram. Compete-lhe “*a coordenação dos planos de execução das ações previstas na Estratégia Nacional de Combate ao Terrorismo e, no plano da coordenação internacional, a articulação e coordenação entre os pontos de contacto para as diversas áreas de intervenção em matéria de terrorismo*” (*Lei n.º 59/2015 de 24 de junho, da Assembleia da República*).

Deste modo, um dos principais objetivos do sistema de segurança interna é a prevenção e neutralização das ameaças, e os riscos que incumbem sobre a sociedade e os indivíduos da mesma. Essa análise e a avaliação das ameaças e dos riscos recai sobre as atividades das polícias e dos serviços de inteligência (Fernandes, 2014b).

3.2 Segurança Informática

A *Internet* quando foi desenvolvida não teve o intuito de ser segura. Com o crescimento da rede de computadores e, posteriormente, da comercialização é que se começou a denotar que a *Internet* era um local inseguro e, por conseguinte, trazia um sentimento de insegurança a quem tinha de lidar diariamente com a mesma, por diversas situações.

Este "salto" de preocupação tal como conhecemos hoje em dia só aconteceu devido a diversos setores económicos e governamentais dependerem de sistemas eletrónicos para o seu funcionamento quotidiano, em que a conceção da ideia de um ataque informático a estas infraestruturas era impensável (Pimentel, 2014).

Como vamos observar mais à frente, os problemas dos computadores são originados por falhas, acidentes ou ataques, sendo que muitos destes últimos são causados pela exploração de falhas (humanas e por engenharia social) nos sistemas. Estas falhas exploradas pelos criminosos são o foco principal da cibersegurança, uma vez que conseguem, muitas vezes, ter total controlo dos sistemas computorizados (P. Torres, 2014).

Atualmente, ainda existe alguma ambiguidade quando nos referimos aos conceitos de segurança da informação e de segurança informática. Estes dois termos apesar de serem complementares entre si, têm objetivos diferentes. A segurança informática responsabiliza-se ao nível da proteção dos sistemas informáticos, onde a informação é, comummente, armazenada e difundida. Por outro lado, a segurança da informação tem ao seu encargo a proteção da informação guardada digitalmente em computadores, sendo também responsável pela informação armazenada de distintas formas entre os diferentes canais (A. Torres, 2014).

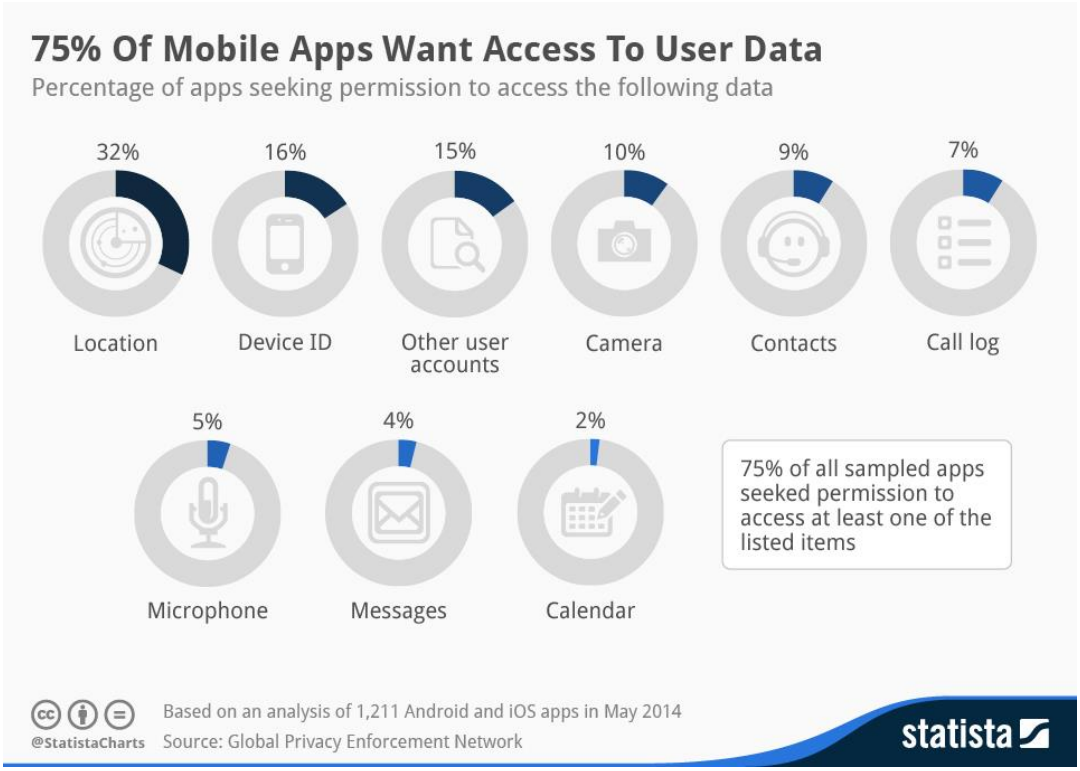
Resumidamente, podemos definir o conceito de segurança informática, ou usualmente denominada de cibersegurança, como a "*capacidade de proteger as redes e sistemas informáticos, bem como os dados que nestes circulam, de forma a assegurar a respetiva disponibilidade, autenticidade, integridade e confidencialidade*" (Casimiro, 2014). A norma internacional ISO/IEC 13335-1, de 2004, remete, ainda, que a segurança informática é um termo relacionado com a "*implementação e manutenção da confidencialidade, integridade, disponibilidade, irrefutabilidade, responsabilidade, autenticidade e confiabilidade dos recursos da informação*" (A. Torres, 2014).

Sendo que, atualmente, a *Internet* tornou-se um local onde as pessoas se transformam e deixam de ter privacidade, isto é, quando se ligam à *Internet* tornam-se informações ou mesmo códigos. As informações são fornecidas por exemplo através do *upload* de imagens ou através de um dado da pessoa. As informações fornecidas são

como um “poder”, podendo ser utilizadas tanto para o “bem” como para o “mal”. Por outras palavras, podem ser usadas apenas para ligação à rede ou podem ser utilizadas para controlar, como por exemplo, o rastreamento da localização, a alimentação diária, as pesquisas feitas, os *sites* acedidos, etc. (Kochavi, 2016a).

Os “Termos de Utilização” de um determinado serviço são exemplo disso, quando a maioria das pessoas aceitam, não os leem mas colocam o “*check*” em como leram, apenas para poder utilizar aquele serviço, esquecendo-se que existe uma enorme quantidade de informação que está a ser armazenada (**Figura 3.2**) e parte desta são as próprias pessoas que as carregam propositadamente, como acontece no caso das redes sociais (por exemplo, Facebook).

Figura 3.2 Estatísticas do acesso requerido pelas aplicações móveis, referentes a 2014.



Fonte: Richter, 2014

Essas informações são armazenadas por empresas que podem vender a alguém que as quiser comprar. Pois, a informação de uma determinada pessoa pode valer algo para alguém. E, nada impede a essas empresas (que armazenam informação) de venderem os nossos dados a alguém. Um grande exemplo disso é a Google, que rastreia as nossas pesquisas para vender essa informação.

"Informação leva ao conhecimento e conhecimento é poder!"
(Autor Desconhecido)

Outro fator normalmente esquecido na publicação de alguma informação, como por exemplo fotos, é que eliminar não significa propriamente que estas desapareceram do mundo digital. Tal acontece devido às permissões dadas, pelo utilizador, para o uso das imagens publicadas, mesmo que estas sejam eliminadas do seu perfil, pois podem estar noutros *sites*, devido a serem armazenadas por outros.

Depois da definição do conceito de segurança informática, têm de ter em atenção os cinco princípios da mesma: Confidencialidade, Integridade, Disponibilidade, Registo, Fiabilidade e Segurança (CCM, 2015; S. Mamede, 2006).

A confidencialidade baseia-se em assegurar que apenas as pessoas autorizadas têm acesso aos recursos trocados, ou seja, a informação fica ininteligível para todas as pessoas que não sejam os atores da transação (CCM, 2015; S. Mamede, 2006).

A integridade consiste em garantir que os dados são mesmo aqueles que acreditamos que são, isto é, determinar que os dados não foram alterados durante qualquer comunicação, quer de forma propositada ou acidental (CCM, 2015; S. Mamede, 2006).

A disponibilidade permite o bom funcionamento do sistema de informação, ou seja, que os recursos estão disponíveis no exato momento que são necessários (CCM, 2015; S. Mamede, 2006).

O registo baseia-se na recolha de informação sobre a utilização dos sistemas e seus recursos, garantindo a existência de dados, para a realização de auditorias. Por outras palavras, o sistema garante a identidade do utilizador, através de uma senha que deve ser codificada (CCM, 2015; S. Mamede, 2006).

A fiabilidade e a segurança garantem que os sistemas não introduzem alterações nos dados e que a utilização dos recursos deixa sempres estes e os sistemas em estados íntegros (S. Mamede, 2006).

3.2.1 Ciclo de segurança

Generalizando, a segurança diz respeito à proteção de bens, em que se subentende o conhecimento destes, bem como o respetivo valor. A partir deste conhecimento consegue tomar diferentes tipos de ação, exemplificados na **Figura 3.3** (S. Mamede, 2006).

Figura 3.3: Esquema ilustrativo do ciclo de segurança dos sistemas informáticos

Fonte: S. Mamede, 2006

Na prevenção determinamos o valor de cada bem e os riscos associados, como forma de os minimizar ou eliminar. A fase da deteção tem como objetivo responder, com o maior rigor, a certas questões (Quando? Como? Quem?), através da monitorização e acompanhamentos permanentes. Por último, a reação engloba as ações tomadas para repor a situação antes do incidente, e fazendo, em simultâneo, suprimir o risco de algo exatamente igual voltar a acontecer (S. Mamede, 2006).

Um caso prático da utilização deste ciclo de segurança é, por exemplo, o caso de utilização fraudulenta de um cartão de crédito, no qual o número foi apanhado numa transação na *Internet*. A prevenção por parte do titular consiste na utilização de uma cifra[1] na sessão de colocação de uma encomenda, em confiar em quem vende e este efetuar a validação do cartão de crédito, antes de autorizar a transação, ou não utilizar o número do cartão de crédito para efetuar as compras por este meio, escolhendo realizar o pagamento de modo mais tradicional e seguro. A deteção acontece quando o titular do cartão de crédito repara que no extrato existe uma transação que não foi efetuada por si. A reação passa, então, pelo titular pedir um novo cartão de crédito, com um novo número, e o acionar o eventual seguro associado ao mesmo (S. Mamede, 2006).

3.2.2 Dimensão do ataque

Analisando o nível de organização dos ataques informáticos podemos agrupá-los, da seguinte forma (IDN-CESEDEN, 2013):

[1] Por «cifra» entende-se "*função matemática utilizada para transformar uma mensagem em texto claro numa forma em que não pode ser percebida a menos que seja decifrada*" (S. Mamede, 2006).

- Ataques simples: O impacto destes ataques é médio-baixo, uma vez que são ataques sem coordenação ou com um nível de organização muito reduzido. Estes são executados por uma ou várias pessoas, mas sem formar uma organização propriamente dita;
- Ataques organizados: O seu impacto é, normalmente, médio, todavia depende do tipo de objetivos a atingir, podendo tornar-se superior. Estes ataques são executados e coordenados por um grupo organizado, constituído por um número considerável de pessoas;
- Ameaças Persistentes Avançadas (APT – *Advanced Persistent Threats*): O impacto destas ameaças pode ser bastante forte e têm uma probabilidade de ocorrência elevada. A concretização deste tipo de ameaças exige um grupo de pessoas, com um perfil de elevada perícia tecnológica, que permanecem particularmente focados num alvo específico;
- Ataques coordenados de grande escala: O seu impacto pode ser elevado ou muito elevado. Este tipo de ataques mostra um elevado nível de coordenação, uma vez que são executados e dirigidos por uma organização ou por uma nação, envolvendo, deste modo, um elevado número de atores, que podem pertencer ou não à organização/nação;
- Ciberataques coordenados com ataques físicos: Este tipo de ataques apresenta um impacto extremamente elevado, devido a requerer um nível de coordenação muito elevado. A combinação de ataques informáticos com ataques em diferentes dimensões físicas (terra, mar e ar) exige um planeamento e uma execução com grande precisão.

Uma reflexão que tem vindo a ser colocada é a "*extensão do impacto que os ciberataques têm na segurança nacional*". A segurança nacional não diz apenas respeito às infraestruturas críticas, que estejam dependentes das novas tecnologias de informação e comunicação, nem a afetação que tal terá sobre a economia, sobre o funcionamento do próprio Estado, mas esta segurança começa também na casa de cada cidadão do país (Caldas & Freire, 2013).

Os ataques informáticos contra a Estónia[2] (2007), Geórgia[3] (2008), Ucrânia[4] (2015) e Irlanda[5] (2016) foram ataques sofisticados e de larga escala, que provaram a necessidade de proteger e garantir o fluxo de informação vital entre as infraestruturas críticas para a sobrevivência do Estado. Quer tenham ou não a opinião de que nos encontramos na iminência de um ciberataque de grande escala, não podem desconsiderar a crescente ameaça de ataques informáticos na nossa sociedade. E, como tal, a análise e gestão do risco, no âmbito do ciberespaço, deve ser tido em conta para a soberania do Estado (Nunes, 2016).

Em suma, a segurança de informação ou a segurança informática têm diversos problemas, mas na sua grande maioria são causados por intenções ou ações de pessoas maliciosas que tentam obter benefício, ou chamar à atenção ou até mesmo prejudicar alguém (Azevedo, 2010).

[2] Em 2007, *sites* de jornais, emissoras de televisão e quase todos os *sites* governamentais foram atacados e ficaram temporariamente fora do ar. Este ataque foi o primeiro que colocou em causa a segurança de uma nação.

[3] Na sua maioria, os ataques foram contra os *sites* governamentais, Conseguindo quase parar a totalidade dos serviços via *internet*.

[4] Na última semana de 2015, uma central elétrica da Ucrânia foi alvo de um ciberataque, utilizando um *malware* que já tinha sido identificado no Ocidente, em 2014.

[5] Em Janeiro de 2016, diversos *sites* e computadores do Governo da Irlanda ficaram inoperacionais durante 24h, devido a uma série de ataques do tipo Negação de Serviço Distribuído – DDoS.

4 CIBERSEGURANÇA E CIBERDEFESA

Neste capítulo iremos centrarmo-nos em duas vertentes que estão intimamente ligadas entre si: a cibersegurança e a ciberdefesa.

Se ouvirmos o computador, tem um zumbido, que podemos associar a uma batida de coração ou a um pulso. Tal como nós, seres humanos, a tecnologia também vive, morre e, mais que tudo, evolui. Esta tem vindo a evoluir exponencialmente (como referimos no capítulo anterior) de tal modo que temos aceitado cada nova versão que surge mais rápido que a versão anterior, tornando-se uma dependência/um vício, como uma extensão de nós mesmos (Kochavi, 2016b).

Toda a informação sobre nós, que se encontra nos nossos dispositivos ou *online* numa *cloud* (nuvem) pode ser facilmente acedida por alguém que esteja interessado, devido à nossa falta de segurança. Ao transpormos esta realidade para um País ou Estado, tal coloca em causa a soberania do mesmo. Como tal, o País ou Estado tem de garantir a sua segurança *online,* bem como a segurança dos seus cidadãos na *Internet* (Militão, 2014).

> *A Internet converteu-se num instrumento indispensável aos Estados da Organização dos Estados Americanos (OEA), porém, lamentavelmente, esta também gerou novas ameaças que colocam em perigo toda a comunidade que a utiliza (adaptado de Souza & Medeiros, 2011).*

Assim, com o constante avanço da tecnologia tal “obriga” a que a sociedade esteja em permanente mutação que, por consequência, “obriga” a que os Estados revejam as suas capacidades e modelos de governação, explorando as Tecnologias de Informação e Comunicação (TIC). Portugal não é uma exceção (P. F. V. Nunes, 2012), apesar de, atualmente, não existir um número elevado de casos deste tipo em comparação a outros crimes.

Por outras palavras, o Estado tem de salvaguardar tanto a cibersegurança como a ciberdefesa. Estes dois conceitos são significativamente diferentes pois atuam em diferentes esferas no ciberespaço, contudo dependendo do ataque sofrido, a diferença é muito ténue.

A cibersegurança, como referimos anteriormente, é a capacidade de proteção das redes e sistemas informáticos, bem como os dados que nestes circulam através de um conjunto de medidas que procuram garantir o bem-estar e o regular funcionamento

da ação de um Estado e das suas populações no ciberespaço e fora dele (Casimiro, 2014; Militão, 2014). Por sua vez, a ciberdefesa garante a realização de missões de segurança e defesa nacional, através de atividades de monitorização, prevenção e de respostas a ameaças que coloquem em risco a soberania e segurança nacional (ciberguerra), cuja responsabilidade de resposta recai sobre as Forças Armadas (Militão, 2014; Ralo, 2013).

A cibersegurança não se cinge apenas aos profissionais da área de informática, esta também deve ser tida em conta por todos os cidadãos, uma vez que a segurança de um Estado depende diretamente de todos, ou seja, para um Estado ser seguro virtualmente, todos os seus cidadãos devem ser instruídos para tal, pois cada vez mais as ameaças existentes só se tornam reais através dos seus descuidos.

Podem-se enumerar algumas causas de insegurança, normalmente, divididas em dois tipos: o estado ativo e passivo da insegurança. No caso do estado ativo de insegurança, estamos a pronunciar-nos acerca do não conhecimento das funcionalidades do sistema por parte do utilizador, podendo estas ser prejudiciais para o mesmo. Por outro lado, o estado passivo de insegurança recai sobre a ignorância dos meios de segurança implementados, como por exemplo, o administrador de um sistema não conhecer os dispositivos de segurança que tem (CCM, 2015).

Podemos caraterizar este ambiente virtual em duas vertentes: o ataque e a defesa (**Tabela 4.1**).

Tabela 4.1: Caracterização do ambiente, quanto ao ataque e à defesa

Ataque	Defesa

• Muito atrativo
• Baixo custo
  - Subornar
  - Criar informações falsas
  - Manipular informação
  - Utilização de armas lógicas
• Lançada de qualquer parte do mundo
• Não deixa rasto
• Tecnologia gratuita na *Internet*
	• Amplos recursos para desenvolver:
	  - Ferramentas
	  - Processos
	  - Procedimentos
	• Custo elevado
	• Limites Tecnológicos
	• Limites Humanos
	• Não se consegue antecipar tudo
	• A ameaça interna

Fonte: Sobral, 2010

Pelo facto de existirem diversas ameaças no ciberespaço[6] – como, por exemplo, espionagem, vigilância, roubo de informações comerciais, ciberativismo (ou até

[6] O ciberespaço, num âmbito mais técnico, significa "*um conjunto de redes e sistemas de comunicação que estão interligados, entre si, de forma direta ou indireta*", tendo em atenção as vulnerabilidades inerentes ao seu acesso e às ameaças que podem afetar os utilizadores desse ambiente (IDN-CESEDEN, 2013).

hacktivismo), terrorismo e mesmo a possibilidade de conflito – precisamos de caraterizar as ameaças de acordo com as implicações que estas têm para a segurança dos indivíduos e para a segurança nacional (Pimentel, 2014).

4.1 Atores do Ciberespaço

Após análise de vários autores sobre este assunto podemos contextualizar que os atores que integram o ciberespaço são: os Internautas, os ativismos, as empresas, as instituições, os serviços de informação, as Forças Armadas, os *Hackers* e, por fim, os cibercriminosos.

Os internautas compreendem todas as pessoas que utilizam a *Internet* como forma de socializar, lazer e trabalho. Pelo fato de existirem inúmeros internautas que sentem uma atração pela conetividade, tal pode tornar-se um vício e, como consequência, uma vulnerabilidade que pode ser explorada.

Os ativismos centram as suas ações na promoção das suas causas, contestando e defendendo as suas opiniões, através da *Internet* por apresentar baixos custos e pela publicitação de informações não ser filtrada, como acontece em jornais ou revistas (P. Santos, Bessa, & Pimentel, 2008). Podemos, ainda, dividir os ativismos em dois grupos: os pacíficos e os radicais. No primeiro, estes aproveitam-se da lei vigente para fazer-se ouvir. Os segundos de forma a promoverem as suas ideias causam perturbação da ordem pública.

As empresas cada vez mais utilizam a *Internet* como um meio de aumentar a visibilidade do seu negócio.

As instituições, como as empresas, viram a utilização da *Internet* como um meio de disponibilização de informação sobre as atividades do Estado e para a disponibilização de serviços, isto é, os cidadãos deixam de perder horas numa fila por causa de um documento, quando o podem ter em cinco minutos, apenas acedendo à *Internet*.

Os serviços de informação através do ciberespaço, designadamente fontes abertas, têm acesso às informações necessárias a um baixo custo.

As Forças Armadas atuam no ciberespaço, apenas, quando todos os outros mecanismos ou entidades falham.

Os *hackers* são indivíduos capazes e disponíveis para penetrar, explorar ou contornar as barreiras de segurança, de modo a atingir um determinado fim, associando à sua imensa força de vontade e dedicação ao estudo (L. Santos, 2011; Vieira, 2006a). Estes sujeitos, frequentemente, são caraterizados como indivíduos que procuram falhas

de segurança nos sistemas para causar “caos”, como exemplo, temos os criadores do vírus “Melissa” ou do “I Love You” quando provaram enormes falhas de segurança nos sistemas da *Microsoft*, em que houve mais malefícios do que benefícios. Porém, nem todos os *hackers* são assim. E, como tal, criaram novos termos para os caraterizar, consoante as suas motivações, recorrendo ao termo *hat*[7] (Rodrigues, 2010).

Assim, consequentemente, surgiu a divisão dos *hackers* em *White hat*, *Black hat* e *Gray hat*. O *White hat* é um *hacker* ético, interessado na segurança, em que usa os seus conhecimentos para explorar e detetar possíveis erros de conceção dos sistemas, dentro da lei. A sua atitude baseia-se, quando encontra possíveis erros, em contactar os responsáveis pelo sistema informando-os de tal, para que possam corrigir e tomar medidas preventivas. Os *Black hat* é, como se pode prever, um *hacker* criminoso sem ética, em que o seu objetivo é descobrir falhas de segurança num sistema e explorá-las, com a finalidade de obterem lucro financeiro ou simplesmente por que gostam do que estão a fazer. Por fim, o *Gray hat* é um misto dos outros dois tipos. Este indivíduo tem os conhecimentos e atitudes de um *White hat*, porém, às vezes, usam esses conhecimentos com os propósitos dos *Black hat*, devido a trabalharem tanto na defesa como no ataque: “*Defendem que é aceitável invadir sistemas desde que não se cometa roubo, vandalismo ou se infrinja a confidencialidade*” (Rodrigues, 2010).

Concluindo, o tipo de *hacker* que o sujeito é, dependerá das suas atitudes e propósitos quando cometer um delito.

Por fim, não menos importante, temos os cibercriminosos são indivíduos que infringem a lei tendo benefícios com isso, como por exemplo, temos os indivíduos que distribuem e divulgam pornografia infantil.

4.2 Espectro das ameaças

> *"As pessoas são surpreendidas pela maldade porque não a previram e não se protegeram contra ela.” (Clark, 2003)*

A crescente utilização e dependência das TIC no funcionamento quotidiano de diversos sectores económicos e governamentais faz com que a possibilidade de um ataque cibernético nestas estruturas, coloque o país num estado de “xeque-mate”, uma vez que estas são consideradas como infraestruturas críticas (Pimentel, 2014).

[7] Esta ideia teve origem nos filmes de *Western*, onde a cor do chapéu indicava o lado (o bem ou o mal) que estava o indivíduo (Rodrigues, 2010).

O conceito "infraestrutura crítica" nacional diz respeito, segundo o *Decreto-Lei n.º 62/2011 de 9 de Maio, do Ministério da Defesa Nacional*, a um "*componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo*". Enquadra-se nesta definição o setor das comunicações, os serviços de emergência, o setor energético, o setor financeiro, o setor alimentar, o Estado propriamente dito, o setor da saúde, o setor dos transportes e o setor da água (Sobral, 2014).

Por outras palavras, estas novas tecnologias não são 100% seguras e como tal acarretam vulnerabilidades, que criam riscos materiais e sociais. Estas tecnologias tanto podem trazer vantagens como desvantagens para os utilizadores. Por um lado, o benefício que trazem à sociedade, e por outro a dependência e a quantidade de informação armazenada e em circulação, que acarretam riscos ao exporem o Estado, as empresas e os cidadãos (*Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho, Presidência do Conselho de Ministros*).

Deste modo, o termo «ameaça» consiste num acontecimento ou atitude indesejável, podendo ser classificada como acidental ou intencional, que pode degradar o potencial existente ou alterar um determinado *status quo* (Azevedo, 2010; Fernandes, 2014b).

Para as Nações Unidas, a comunidade internacional deve preocupar-se com seis grupos de ameaças: ameaças económicas e sociais (onde inclui a pobreza, doenças infeciosas e a degradação ambiental), o conflito entre estados, conflitos internos (incluindo a guerra civil, o genocídio e outras atrocidades em grande escala), as armas de destruição massiva, o terrorismo e o crime organizado transnacional (Garcia, 2006).

Em suma, muito primitivamente, o grau da ameaça está dependente da função das intenções manifestadas por um ou vários atores e das suas capacidades ou das possibilidades (**Figura 4.1**) dos mesmos de transformar as intenções em ações contra o alvo (Fernandes, 2014b).

Figura 4.1: Definição simplificada do termo ameaça, segundo uma equação

$$Ameaça = Intenções \times Possibilidades$$

Fonte: Fernandes, 2014a

No entanto, a parte essencial de qualquer ameaça, qualquer que seja a sua natureza, não depende apenas das intenções e das possibilidades. Esta está intimamente ligada ao estudo das intenções, das possibilidades, das motivações, dos

valores em jogo e dos valores do alvo, num determinado espaço e tempo (**Figura 4.2**). Ao analisar todos os fatores que advêm podemos ter uma avaliação, do nível de risco de cada ameaça, para podemos atuar da melhor maneira na sua prevenção (Dias, 2012; Fernandes, 2014a).

Figura 4.2: Definição do termo ameaça de um determinado ator, segundo uma equação

$$Ameaça = [Intenções \times Possibilidades \times Motivações \times Valores\ em\ jogo \times Valores\ do\ alvo] \times Espaço \times Tempo$$

Fonte: Fernandes, 2014b

Através de cada uma destas caraterísticas, de que depende a ameaça, podemos decompor e definir (Fernandes, 2014b):

1) **Intenções:** são uma componente subjetiva dependente de diversos fatores, podendo servir como um motor ou um travão na ação. As intenções dependem da perceção da realidade do ator e são expressas num determinado quadro situacional;
2) **Possibilidades:** são manifestações materiais dos recursos e tecnologias disponíveis por parte do ator;
3) **Motivações:** são as razões que fazem com que o ator suporte sacrifícios e multiplique os esforços de forma a alcançar um determinado fim;
4) **Valores em jogo:** resultam de uma análise da situação por parte do autor da ameaça, onde este identifica e estabelece objetivos da ação, ou seja, os ganhos e perdas, os riscos aceitáveis e os recursos que este está disposto a usar;
5) **Valores do alvo:** estes variam consoante a natureza, os custos de recuperação e dos subsistemas a que pertence e, também, da sua utilização temporal;
6) **Espaço e Tempo:** são fatores que corporalizam a possibilidade do ator desencadear a ação e, assim, materializar, em concreto, a ameaça.

Particularizando as ameaças ao nível informático, os criminosos informáticos usam vários métodos de forma a conseguirem roubar dados financeiros de empresas ou pessoas, podendo faturar milhões através de transações fraudulentas, ou até mesmo atacar algumas infraestruturas, por puro desejo pessoal.

Por exemplo, enviar um programa malicioso (ou conhecido, em inglês, como *malware*) pela *Internet*. Quando esse programa entra no dispositivo da vítima, este silenciosamente inspeciona as defesas do mesmo, ou seja, procura portas que estejam

desprotegidas para poder invadir e, assim, procurar informações úteis. Um dos grandes problemas é que este dito programa irá alterar ou apagar arquivos, bem como enviará o mesmo por *e-mail* para todos os contactos do dispositivo atacado. Seguidamente, remeterá as informações contidas nesses dispositivos (senhas, dados financeiros, entre outras informações) para o invasor ou criador do programa.

Estes ataques, na maioria das vezes, são quase impercetíveis, podendo designar-se de ataques silenciosos.

> *"Porquanto os ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (…) podem fazer colapsar a estrutura tecnológica de uma organização social moderna" (Governo de Portugal, 2013, p. 16)*

Segundo Pedahzur (2009), existem três diferentes domínios de atuação [8] associados à segurança e defesa, no contexto do ciberespaço: o domínio de proteção simples, o domínio de prossecução criminal e o domínio da defesa do Estado (L. Santos, Bravo, & Nunes, 2012).

O domínio de proteção simples é considerado como a primeira linha de proteção das infraestruturas, dos serviços e da informação presentes no ciberespaço, englobando as componentes preventivas, reativas e de gestão da qualidade da segurança (L. Santos et al., 2012).

No domínio de prossecução criminal, o sistema judicial tem o objetivo da dissuasão da prática de crimes, em particular os cometidos contra as infraestruturas críticas nacionais, como tal o legislador teve em conta o agravamento dessas sanções (L. Santos et al., 2012).

Por último, no domínio da defesa do Estado, conforme a Constituição da República Portuguesa, as Forças Armadas são a entidade responsável pela defesa do Estado contra ameaças externas e devem assegurar, em situações de exceção, o regular funcionamento das instituições democráticas e o exercício das funções de soberania do Estado (L. Santos et al., 2012).

Em suma, na **Figura 4.3** encontramos como os três domínios caracterizam os ciberataques, os seus objetivos, os aspetos legais e constitucionais e os atores.

[8] O termo "domínios de atuação", usado neste trabalho, refere-se ao conjunto dos atores, quer seja humanos ou técnicos, bem como ao enquadramento legal, envolvidos no prosseguimento de um conjunto de objetivos, os quais, em parte, são definidos por uma perspetiva relativamente à ciberconflitualidade (L. Santos, Bravo, & Nunes, 2012).

Figura 4.3: Domínios de atuação na proteção do ciberespaço

	Protecção Simples	Prossecução criminal	Defesa do Estado
Caracterização	Os ciberataques são vistos como ameaças à disponibilidade, integridade e confidencialidade da informação e de outros activos.	Os ciberataques são vistos como actos criminalmente relevantes.	Os ciberataques são vistos como um acto de Guerra, pondo em risco a existência do Estado.
Objectivos	Proteger potenciais alvos contra ciberataques.	Prevenir crimes e identificar e condenar os responsáveis.	Eliminar uma ameaça que coloque em causa a Soberania Nacional ou ganhar uma vantagem competitiva sobre outro Estado.
Aspectos legais e constitucionais	Salvaguarda dos direitos individuais e da privacidade dos cidadãos.	Actuação dentro do quadro da legislação aplicável e segundo as regras do sistema judicial.	Actuação sujeita à Constituição da Republica, Lei do Estado de Sítio e do Estado de Guerra, bem como ao Direito Internacional dos Conflitos Armados e dos Direitos Humanos.
Actores	Técnicos de sistemas e de redes, Indústria TIC, autoridades reguladoras sectoriais, CSIRT, utilizadores TIC.	Órgãos de polícia criminal, Ministério Público e Magistrados Judiciais.	Forças Armadas e Serviços de Informações.

Retirado de Santos et al., 2012.

Os ataques e as ameaças cibernéticas têm vindo a aumentar, todavia os seus métodos baseiam-se constantemente no mesmo. Por isso, devemos compreender como estes funcionam de forma a proteger e defender deste tipo de ameaças. Podemos observar na **Tabela 4.2** uma listagem das ameaças mais comuns do ciberespaço (Torres, 2014).

Tabela 4.2: Lista de ameaças mais comuns no ciberespaço

Método	Definição
Engenharia Social	Técnica usada na obtenção de informações confidenciais, através da exploração do conhecimento ou confiança das pessoas.
Man-in-the-middle	Forma de ataque, em que é intercetada e retransmitida informação trocada entre duas partes num dado canal.

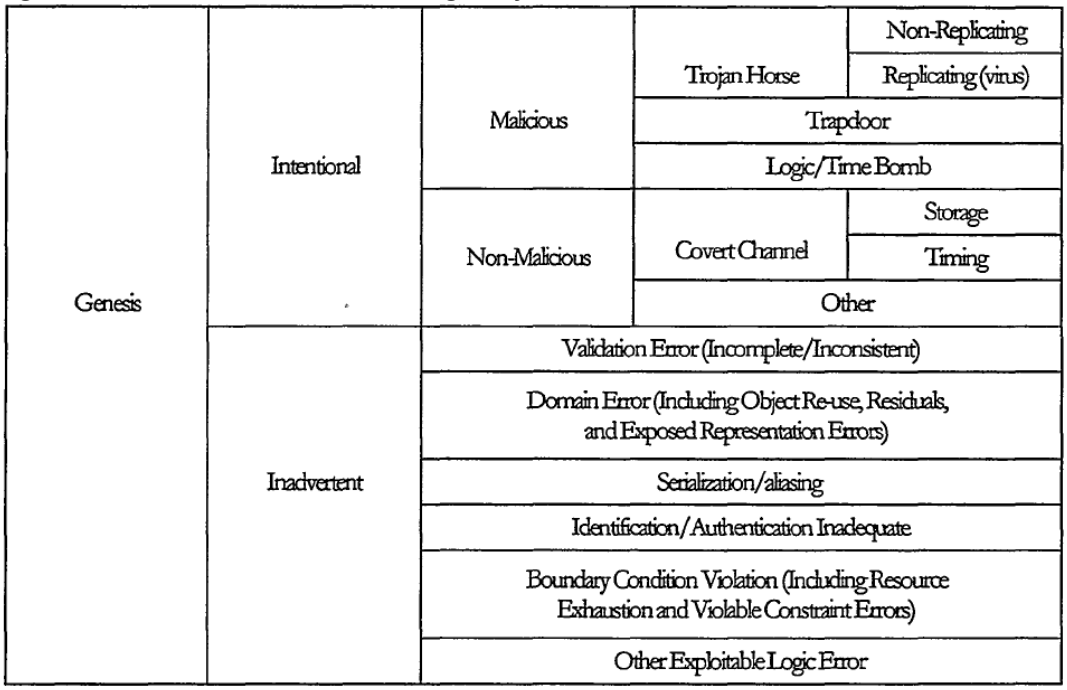
Método	Definição
Man-in-the-browser	Consiste na infeção (normalmente, um *trojan*) do computador da vítima e que é capaz de modificar as comunicações entre o cliente e o servidor de uma maneira impercetível, quer para a vítima quer para a aplicação.
Trojan	Programa malicioso introduzido num computador sem que a vítima saiba, com o objetivo de abrir uma ligação com o computador do invasor e, assim, este ter total controlo do computador da vítima.
Worms	Programa idêntico a um vírus com a capacidade de replicar-se num sistema inteiro. O objetivo pode ser, por exemplo, sabotar um sistema informático até apagar todos os dados contidos nele.
Vírus	Pedaço de *software* malicioso com a finalidade de infetar um computador e que este se espalhe por outros computadores.
Phishing	Técnica que tenta obter dados pessoais, através do envio de *e-mails* fraudulentos que tentam fazer passar-se por uma pessoa ou empresa de confiança e, deste modo, enganar a vítima.
Keylogger	Programa capaz de capturar todas as teclas marcadas pelo utilizador.
Spyware	Programa de computador que é instalado no computador da vítima e tem a capacidade de recolher informações sobre a mesma e depois envia esses dados para outra entidade.
Ransomware	Tipo de *malware* que restringe o acesso ao computador ou aos arquivos, exibindo uma mensagem em que exige um pagamento para remover a restrição, por exemplo, através de *e-mails* com anexos maliciosos ou *websites* infetados.
Botnet	Conjunto de computadores infetados que são controlados remotamente, funcionando, por exemplo, como um exército de computadores que realizam diversas tarefas como enviar *e-mails* com spam, propagação de *malware*.

Método	Definição
Clickjacking	Método que utiliza as ações de um utilizador numa determinada página *web* para realizar operações maliciosas. O atacante coloca um *iframe* num elemento clicável, por exemplo, um botão, de forma a conseguir que a vítima clique nesse *iframe* e o invasor, sem o conhecimento da vítima, realize uma operação por si definida.
Negação de Serviço	É um ataque que consiste em fazer diversas tentativas ao computador/serviço alvo (ex. servidor *web*) para que tenham dificuldade ou mesmo sejam impedidos de executar suas tarefas, por outras palavras, sobrecarregam os sistemas. Uma variante deste ataque, muito utilizado, é o DDoS (Negação de Serviço Distribuído): é um ataque em rede, em que um computador mestre controla um certo número de computadores cliente para inundar o alvo com tráfego, através da utilização de um *software* específico para o efeito.

Fonte: S. Mamede, 2006; A. Torres, 2014

Como temos vindo a observar neste capítulo, os criminosos cibernéticos utilizam as falhas de segurança para poderem cometer a infração. Na **Figura 4.4**, podemos observar dois tipos de falhas: intencional ou acidental (Howard & Longstaff, 1998).

Figura 4.4: Taxonomia das falhas de segurança: falhas intencionais ou acidentais



Retirado de Howard & Longstaff, 1998

Em relação à classificação de incidentes, o Centro Nacional de Cibersegurança utiliza a seguinte taxonomia de incidentes da Rede Nacional de CSIRTs:

Tabela 4.3: Taxonomia para incidentes de segurança cibernética

Classe de Incidente	Tipo de Incidente
Código Malicioso	Infeção Distribuição Comando e Controlo (C&C) Outro
Disponibilidade	DoS/DDoS Sabotagem
Recolha de Informação	*Scan* *Sniffing* *Phishing*
Tentativa de Intrusão	Exploração de Vulnerabilidade Tentativa de login
Intrusão	Exploração de Vulnerabilidade Compromisso de Conta
Segurança da Informação	Acesso não autorizado Modificação/Remoção não autorizada

Classe de Incidente	Tipo de Incidente
Fraude	Utilização indevida ou não autorizada de recursos Utilização ilegítima de nome de terceiros
Conteúdo Abusivo	Spam Direitos de autor Pornografia infantil, racismo e apologia da violência

Fonte: CNCS, 2015

4.2.1 Agentes da ameaça

Saber a identidade dos autores é extremamente difícil, na medida em que estes se escondem para não serem descobertos, como o caso do ataque ao FBI por parte de um grupo denominado “Anonymous”.

Podemos traçar um perfil genérico deste tipo de criminosos, mas não é 100% fiável devido à frequente utilização da *Internet*, o que basicamente começa a generalizar este tipo de perfil, alargando a qualquer pessoa (Vieira, 2006a):

1) Idades compreendidas entre os 15 e os 40 anos;
2) Sem antecedentes criminais (em média 96%);
3) Com pais divorciados ou separados (± 45%, em média);
4) Introvertido e socialmente isolado, incluindo atitudes agressivas ou arrogantes;
5) Frequenta o ensino superior, com notas escolares medianas (75%);
6) Competentes e bons trabalhadores.

Contudo, podemos classificar estes agentes, agrupando-os segundo as motivações e fatores limitativos que iremos referir mais à frente. Os potenciais agentes de ameaça são: “*Intelligence*” estrangeira; Forças militares estrangeiras; Criminais; Políticas; Ideológicos; Económicos; Educacionais; *Hackers*; e, Terroristas (P. Santos et al., 2008).

4.2.1.1 Motivações

As motivações destes sujeitos são variadas desde ganhos pessoais, destruição ou dano, vingança ou reconhecimento público, motivações políticas e económicas, vantagens táticas ou empresariais, curiosidade e procura de desafios, bem como desafios intelectuais (Militão, 2014).

A seguinte **Tabela 4.4** demonstra alguns exemplos das motivações que impulsionam estes sujeitos.

Tabela 4.4: Tabela demonstrativa de alguns exemplos das motivações dos agentes de ameaça

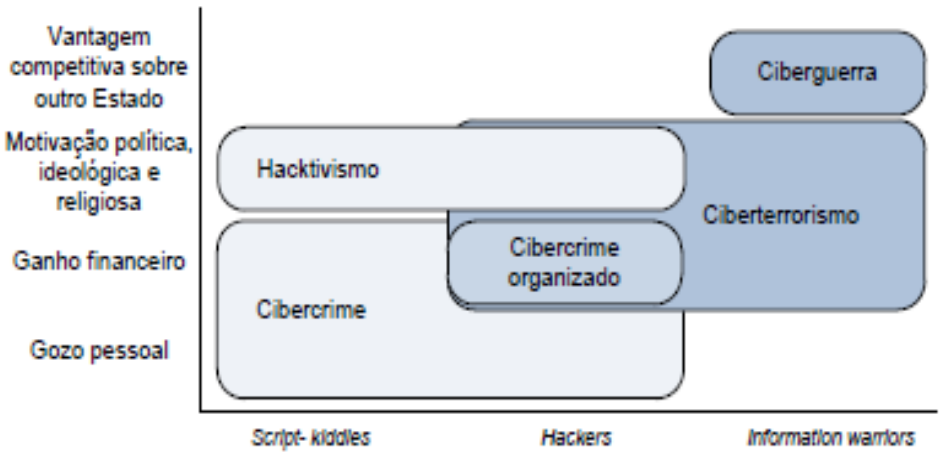
Motivações	Exemplos
Ganhos Pessoais	Vantagem competitiva; Progressão na carreira; Ganhos financeiros; Reconhecimento.
Vingança	Expetativas profissionais defraudadas; Incompatibilidade com a hierarquia; Diferenças ideológicas e políticas.
Curiosidade e Procura de Desafios	Desejo em ser um *hacker;* Procura de aventura; Saber "como funciona"; Perspetiva de poder; Afirmação pessoal.
Desafios intelectuais	Paixão em aprender; Necessidade de ser aceite pela comunidade *hackers;* Sentimento de controlo; Ultrapassar limites.
Propósitos morais ou ideologias	Convicções religiosas; Radicalismos filosóficos ou culturais; Agitação regional e internacional; Heroísmos.
Motivações Táticas	Informação em tempo real sobre o adversário; Ações de sabotagem e controlo; Acesso a informação estratégica; Potenciar ações de destruição.
Motivações Políticas e Económicas	Obter informação política e empresarial; Ganhar vantagem na condução de negociações; Obter informações tecnológicas valiosas, que seriam muito dispendiosas de obter se fosse por conta própria.
"Business Intelligence"	Atingir vantagens competitivas; Obter segredos de mercado;

Motivações	Exemplos
	Obter especificações de produtos de mercado; Obter informações valiosas resultantes de investigação.
Terror	Criar situações que atentem à vida; Destabilizar o equilíbrio das forças; Fomentar o sentimento de insegurança; Criar medo; Fragilizar a cultura e valores.
Ignorância	Segurança deficiente de Sistemas de informação, que permite, por desconhecimento e curiosidade, sejam provocados danos profundos com grande impacto nos sistemas e no funcionamento das organizações.

Fonte: Correia, 2015; P. Santos et al., 2008

Assim, podemos através das motivações dos ataques chegar a um espectro de ameaças que existem sobre o ciberespaço, podendo dividir-se em várias categorias: cibercrime, *hacktivismo*, ciberterrorismo e ciberguerra (**Figura 4.5**). Contudo, cada uma destas categorias, não acaba onde começa a outra, apresentando, assim, limites difusos podendo até existir sobreposição entre as categorias (Santos, 2011).

Figura 4.5: Espetro das motivações dos ataques



Retirado de Santos, 2011

4.2.1.2 Restrições ou Limitações

Antes de um sujeito perpetuar a ameaça, este tem de ter em conta o que precisa para a concretizar. Muitas vezes, os fatores impulsionadores dessa ameaça não são possíveis devido a restrições ou limitações.

As restrições ou limitações podem ser (Militão, 2014; P. Santos et al., 2008):

- Motivação – Como já referido anteriormente, o interesse, a perceção do sujeito quanto à probabilidade de sucesso ou à probabilidade de ser apanhado;
- Intenções/Compromissos – Valores morais e culturais, bem como a perceção da probabilidade de punição e perceção de insucesso;
- Oportunidade – "*Awareness*" e Acessibilidade aos alvos;
- Recursos – Financeiros, a disponibilidade tecnológica, o tempo e a informação;
- Capacidades – Habilidade/destreza, conhecimento, experiência, treino e formação.

4.2.1.3 Fatores de risco

Como referido anteriormente no subcapítulo «Agentes da Ameaça» iremos, na **Tabela 4.5**, referir de acordo com os potenciais agentes de ameaça, os fatores de risco.

Tabela 4.5: Tabela ilustrativa dos fatores de risco tendo em conta os potenciais agentes de ameaça

Potenciais agentes de ameaça	Definição de fatores de risco
***Intelligence* estrangeira**	Provenientes de aliados, países neutros e países inimigos; Ameaça constante.
Forças militares estrangeiras	Provenientes de aliados, países neutros e países inimigos; Ações militares diretas e indiretas; Posse de "*Intelligence*"; Hostilidades previsíveis ou imprevisíveis.
Criminais	Exploração de oportunidades; Obter valores derivados de crimes de suporte; Acessibilidade dos alvos;

Potenciais agentes de ameaça	Definição de fatores de risco
	Aprendizagem criminal; Facilidade de acesso à informação.
Políticas	Impacto dos temas políticos (eleições, etc.); Impacto de notícias provenientes dos *media*; Permanente ambiente de mudança: nacional e internacional.
Ideológicos	Relacionados e confinados a princípios ideológicos.
Económicos	Novas dinâmicas e exigências de competitividade económica; Mundialização da economia; Inexistência de estratégias.
Educacionais	Existência de informações críticas de projetos científicos.
Hackers	Motivações imprevisíveis; Grande domínio das tecnologias de informação; Probabilidade de recrutamento por forças subversivas e militares; Ameaça permanente (24x7x365).
Terrorismo	Capacidade de intervenção em qualquer lugar, em qualquer altura; Posse e capacidade de operacionalização de "*Intelligence*"; Ações imprevisíveis e ubíquas.

Fonte: Correia, 2015; P. Santos et al., 2008

4.2.1.4 Recursos e vulnerabilidades

Um incidente, quando envolve uma violação de segurança, pode comprometer a confidencialidade, a integridade e a disponibilidade da informação. Por outras palavras, a exploração de vulnerabilidades origina os incidentes de segurança (Azevedo, 2010).

Em 1988, surgiu o primeiro vírus, o "*Morris worm*", que conseguiu infetar 5 a 10% dos computadores ligados na *Internet*, que na altura seriam cerca de 60 mil (A. Torres, 2014).

Uma outra ameaça muito simples foi o *hacker* escocês, Gary Mckinnon, que segundo afirmações do mesmo *"Foi ridiculamente fácil (…) Eu não sou uma mente criminosa muito esperta que trabalhou uma estratégia. Eu fiz uma expedição pelas palavras-passe administrativas – que nunca tinham sido mudadas – e foi incrivelmente surpreendente quantas eu descobri mesmo ao mais alto nível"* (Sobral, 2010).

A ameaça só causa danos quando um recurso é vulnerável e essa vulnerabilidade é explorada. A seguinte tabela descreve os principais grupos de recursos dos sistemas de informação e algumas das suas vulnerabilidades (P. Santos et al., 2008).

Tabela 4.6: Listagem dos principais grupos de recursos dos sistemas de informação e das suas vulnerabilidades mais relevantes

Recursos dos sistemas de informação	Vulnerabilidades
Pessoal	Acesso a informação, equipamentos e aplicações críticas; Nível de formação e de conhecimentos; Probabilidade de erro humano; Falta de aptidão, compromisso e ética; Frustrações no trabalho.
Instalações	Quebra de segurança física; Segurança não implementada de raiz com as instalações; Limitações ou localização inapropriada das instalações.
***Hardware* de Rede**	Configurações físicas mal executadas; Acessos inseguros; Ferramentas de administração deficientes; Más políticas de segurança; Falta de planos de contingência; Falta de renovação de equipamentos; *Hardware* não testado; Deficiente *firmware*; "*Bugs*" ou configurações deficientes; Políticas de integração deficientes; Interrupções de energia; Danos físicos.

Recursos dos sistemas de informação	Vulnerabilidades
***Software* de Rede**	Manter a configuração base; Palavras-passe de origem não alteradas; Protocolos inseguros; "*Bugs*"; Má administração e exploração do *software*; Heterogeneidade de *software*; Falta de análise de registos (*logs*); Simetrias de confiança (*Trust Symmetry*); Simetrias transitivas (*Trust Transitivity*); Políticas de integração deficientes; *Software* não testado.
Dispositivos Periféricos	Localização; Segurança física deficiente; Políticas de segurança e de pessoal deficientes; Conexões não autorizadas ou fantasma; Dispositivos não testados.
Dispositivos de armazenamento	Gestão ineficiente; Inexistentes ou más políticas de segurança; Falta de políticas de acesso; Falha de equipamentos; Dispositivos em ambientes não controlado; Dados residuais.
Sistemas Operativos ***Software* de nível do sistema** **Aplicações de nível de sistema**	Palavras-passe de origem não alteradas; "*Bugs*"; Caraterísticas de Segurança fora de uso; Más especificações; Não atualização de "*releases*" e de "*updates*"; Má gestão das configurações de segurança; Indefinição ou deficiente aplicação das políticas de segurança.
Dados operacionais	Deficientes políticas de *backup* e de *recovery*; Falta de planos de contingência; Corrupção de dados.

Fonte: Correia, 2015; P. Santos et al., 2008

4.3 Cibercrime

Como analisado anteriormente no subcapítulo “Criminalidade informática”, o crime informático é descrito como “*todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo desse ato*” (Portugal, 2015a).

Contudo, podemos dividir o crime informático em dois tipos: puro e misto. O crime informático puro existe quando o ataque é direto, ou seja, atacar outros computadores, por exemplo a sua invasão ou a difusão de vírus. Por outro lado, o crime informático misto remete para o uso do sistema informático como um meio necessário para cometer o delito, isto é, usar o computador para cometer crimes convencionais, por exemplo pornografia infantil, fraudes bancárias ou *ciberbullyin*g (Awatare, 2014; Sousa, 2015).

Os crimes mais conhecidos desta natureza, por serem mais frequentes, são o *phishing* e o *carding*, a pornografia infantil e a pirataria informática (Dias, 2012). O *phishing* consiste no roubo de identidade *online*, utilizando como meio o correio eletrónico e *websites* fraudulentos. Tendo como propósito roubar dados e informações pessoais, tais como números de cartões de crédito, palavras-passe, dados de conta, entre outras informações (A. Torres, 2014; UOL, 2013). O *carding* é o termo usado para o processo de verificar a validade dos dados do cartão roubado (Lee, 2009, p. 45).

Com o evoluir da tecnologia, os autores do cibercrime têm-se associado aos grupos terroristas e ao crime organizado, atacando ao nível financeiro. Os ataques, mais comuns, dos cibercriminosos são através da utilização de um tipo de *malware* enviado por *Internet*, de forma a permitir a sua entrada num dispositivo, de modo a aceder a informações pessoais, dos cidadãos, ou a nível de infraestruturas críticas, que podem causar danos elevados (IDN-CESEDEN, 2013).

Contudo, existem mais crimes, uma vez que estão constantemente em evolução, devido às novas tecnologias progredirem (Dias, 2012). Estes crimes têm vindo a aumentar significativamente e a sua tendência é continuar, segundo um relatório relativamente recente, as vítimas perdem cerca de 290 milhões de euros por ano, em todo o mundo, tornando o cibercrime mais rentável do que, no seu conjunto, o comércio mundial de marijuana, cocaína e heroína (EUROPOL, 2014).

O crime informático não requer proximidade física entre a vítima e o autor do crime, ou seja, o autor pode estar num país e a vítima noutro e nem sequer se conhecerem, bastando apenas ao criminoso ter um computador (Natário, 2013; SIS, n.d.). Esta associação da criminalidade existente a uma componente informática constitui uma tarefa difícil para as forças policiais na identificação da sua origem, dos

criminosos e na recolha de provas, pois os criminosos ao utilizarem a tecnologia a seu favor podem criar identidades falsas ou até fazerem-se passar por cidadãos inocentes (Natário, 2013; Pereira, 2012; SIS, n.d.; Vieira, 2006b).

4.4 Hacktivismo

Antes de falar propriamente no conceito *hacktivismo*, convém referir o que é o ativismo. O ativismo são as atividades desenvolvidas por um grupo ou comunidade que pretende influenciar a política externa de determinado país (P. Santos et al., 2008).

Com a *Internet* tornou-se possível os ativistas utilizarem, frequentemente, campanhas de *e-mail* e listas de discussão, bem como *sites*, *blogs* ou fóruns de discussão, de modo a influenciarem as diversas organizações do Governo responsáveis pelas decisões políticas (P. Santos et al., 2008).

Portanto, o termo *hacktivismo* é uma junção de dois conceitos "*hacker*" e "ativismo" resultando no "*uso não-violento de ferramentas digitais ilegais ou legalmente ambíguas para a persecução de fins políticos*" aumentando, assim, a sua visibilidade de capacidade de intervenção e influência (Guimarães, 2013; P. Santos et al., 2008).

Um exemplo de *hacktivismo* é o grupo autodenominado de "Anonymous". A tática, mais utilizada, deste grupo é a negação de serviço de forma a impossibilitar o acesso dos utilizadores a um servidor de *Internet*, por outras palavras, a tática deste grupo é sobrecarregar um determinado *site*, o que leva à queda do servidor e, por conseguinte, a página *web* que sofreu o ataque deixa de poder ser acedida (Guimarães, 2013).

4.5 Ciberterrorismo

O terrorismo define-se como "*uma técnica de ação usada – por indivíduos, por grupos ou organizações – contra alvos humanos, seletivos ou indiscriminados, através de meios especialmente violentos, ou a efetiva ameaça do seu uso, ou, ainda, contra alvos não humanos, como infraestruturas físicas, críticas ou simbólicas, instalando um clima de terror e de insegurança que afeta não só os alvos primários, as suas vítimas diretas, como também os seus alvos potenciais, coagindo direta ou indiretamente a ação de governos ou organizações e influenciando a opinião pública a favor da prossecução de objetivos políticos, ideológicos, religiosos ou criminais (…)* " (Matos, 2012, p. 128, 2015).

Assim, com o passar dos anos, os grupos terroristas começaram a ver a *Internet* como um meio para atingirem os seus fins, quer fosse na forma de ameaças, quer no apoio às suas operações/atividades: difusão de propaganda *jihadista*, recrutamento, levantamento de informações sobre um alvo e como ferramenta de comunicação (L. Santos, 2013; SIS, n.d.). Esta nova ferramenta também possibilitou que os seus alvos pudessem passar a ser atacados via *online*, pois a cada dia que passa, tornam-se mais protegidos ou controlados. Portanto, os atacantes necessitam dos computadores para poderem saber mais sobre quem pretendem atacar (Saraiva, 2011).

Deste modo, surgiu o termo «Ciberterrorismo» que é definido, por Dorothy Denning, como "*ataques criminosos e a ameaças de ataques contra computadores, redes e informação armazenada no seu interior, quando realizados com o objectivo de intimidar ou coagir um governo ou a sua população, procurando atingir objectivos políticos. Para que possa ser qualificado como ciberterrorista, um ataque deverá resultar em violência contra pessoas ou propriedade ou, pelo menos, causar danos suficientes para poder gerar medo*" (P. V. Nunes, 2004).

De acordo com esta definição, um ciberataque para ser considerado uma ameaça de ciberterrorismo, este deve satisfazer dois critérios: motivação política e um resultado destrutivo, que seja fisicamente visível (P. V. Nunes, 2004).

4.6 Ciberguerra

Como temos vindo a observar, a informação é "*um elemento estratégico e táctico valioso*", no âmbito do ofensor ou do defensor. Com as vulnerabilidades de segurança das infraestruturas governamentais, os agressores conseguem provocar danos similares aos que poderiam provocar caso utilizassem um armamento militar (P. Santos et al., 2008).

Deste modo, surge o conceito «ciberguerra», que diferentemente do ciberterrorismo, consiste na corporalização de ações de defesa ou de ataque contra todo o género de estruturas de informação e redes de computadores, onde o campo de batalha é o ciberespaço. Estas ações podem ser, por exemplo, acessos ilegítimos a redes de computadores ou ataques de negação de serviço, tendo como objetivo influenciar ou manipular os processos de gestão de informação dos adversários (P. Santos et al., 2008).

Um grande exemplo de ciberguerra foi o ataque informático, referido anteriormente, à Estónia, em Maio de 2007, em que todo o tipo de infraestruturas digitais do país sofreu, durante semanas, inúmeros ataques de negação de serviço. Este ataque

terá sido desencadeado pelo motivo do governo da Estónia ter mudado de local a estátua, que marcava a vitória russa sobre os nazis (P. Santos et al., 2008).

5 CENTRO NACIONAL DE CIBERSEGURANÇA

Como tem vindo a ser referido nos outros capítulos, a tecnologia tem vindo a evoluir e como consequência deste evoluir é inevitável colocar-se algumas questões (Portugal, 2015b):

- Quais as implicações desta nova realidade na qual a normalidade da vida quotidiana depende do funcionamento de milhões de máquinas e sistemas interligados que garantem as necessidades básicas, nomeadamente a produção e distribuição de energia e água?

- Qual o custo se estas máquinas programadas, ligadas à *Internet*, para comunicar e receber dados e comandos de um *software* orquestrador entrarem em colapso, mesmo que temporariamente?

- Que normas de segurança, fiabilidade e continuidade terão que ser exigidas às tecnologias que constituem a *Internet* caso, por exemplo, o sistema de controlo de um veículo ou até mesmo um *bypass* cardíaco passar a estar ligado a uma rede aberta e ser controlado por acesso remoto, através de um *software*?

Podendo também colocar-se a questão acerca do prejuízo que um ataque cibernético, comunicado às forças de segurança, tem para o Estado.

Principalmente, num presente em que um antivírus instalado, e atualizado diariamente, e uma simples *firewall* não bastam como se pensava até à relativamente pouco tempo (J. C. Martins, 2015).

Deste modo, foram criadas medidas de segurança e estratégias de cibersegurança, uma vez que, as ameaças tanto existem no mundo real como no mundo virtual, colocando em causa a soberania do Estado.

Tornando-se, assim, uma necessidade o desenvolvimento de uma estratégia nacional de cibersegurança que seja "*concertada, integradora e mobilizadora de sinergias nacionais*", bem como a capacidade de reduzir o risco social e potenciar a utilização do ciberespaço (P. F. V. Nunes, 2012).

Quaisquer estratégias de segurança informática têm primeiramente de passar pela avaliação dos riscos existentes, mapear as obrigações legais e regulamentares aplicáveis, para posteriormente ter-se uma estratégia ao nível da política interna, que inclua a proteção de dados pessoais (Casimiro, 2014).

Deste modo, antes de qualquer ataque informático cada país deverá ter um plano (integrado), cumprindo as obrigações relacionadas com a segurança, resiliência das redes, sistemas de informação e as obrigações da proteção de dados pessoais (Casimiro, 2014).

Durante um ataque cibernético consoante o tipo de violação seguirá para a competência das respetivas entidades envolvidas a nível nacional, sendo articuladas através do Centro Nacional de Cibersegurança (CNCS). Os tipos de violações são (Casimiro, 2014):

1) Violação de segurança ou perda de integridade com impacto significativo;
2) Violação de dados pessoais *e-privacy*;
3) Violação de dados pessoais noutros setores;
4) Incidente com impacto significativo na segurança dos serviços essenciais que fornecem.

Por fim, após a resolução de um ataque cibernético são apuradas responsabilidades a nível civil, contraordenacional, disciplinar e criminal (Casimiro, 2014).

Segundo esta linha de pensamento foi atribuído ao Gabinete Nacional de Segurança (GNS), conforme a Resolução do Conselho de Ministros n.º 12/2012, de 7 de Fevereiro, a missão de coordenação com todas as entidades relevantes para o assunto, a definição de uma estratégia nacional de segurança da informação (ENSI), compreendendo a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (Sobral, 2014).

Em 2012, com a Resolução do Conselho de Ministros n.º 42/2012, de 13 de abril, foi criada uma Comissão Instaladora do Centro Nacional de Cibersegurança, que apresentou uma proposta de Estratégia Nacional de Cibersegurança, ao Governo. Mas só, em 2014, foi estabelecido os termos de funcionamento desta entidade com o Decreto-Lei n.º 69/2014, de 9 de maio.

Desde já a sua missão passa pela contribuição nacional da utilização do ciberespaço de forma *"livre, confiável e segura"*, com a inclusão de uma cooperação internacional em conjunto com as autoridades competentes, bem como a implementação de medidas e instrumentos que antecipem, detetem, reajam e recuperem de situações que coloquem em perigo o funcionamento das infraestruturas críticas e a salvaguarda dos interesses nacionais (Sobral, 2014).

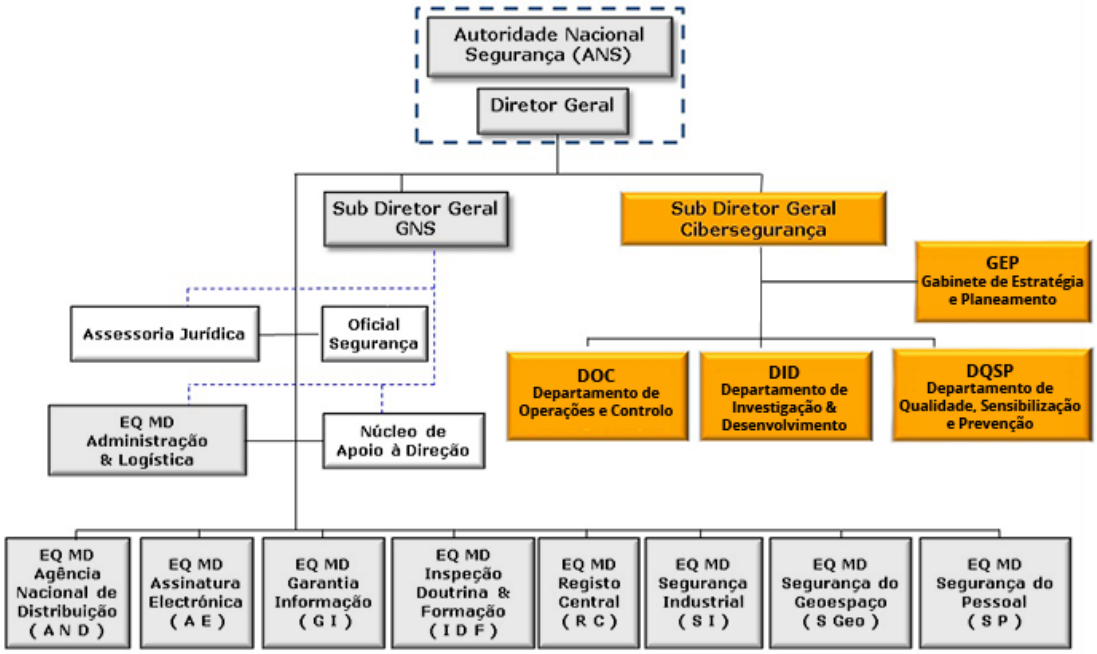
Citando o Decreto-Lei n.º 69/2014, de 9 de Maio da Presidência do Conselho de Ministros, temos que o CNCS no exercício, da sua missão, tem como competências:

1) Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques;

2) Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;
3) Exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais;
4) Contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais;
5) Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área de cibersegurança;
6) Assegurar a produção de referenciais normativos em matéria de cibersegurança;
7) Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança;
8) Assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência, no quadro definido pelo Decreto-Lei n.º 73/2013, de 31 de Maio;
9) Coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros;
10) Exercer as demais competências que lhe sejam atribuídas por lei.

Na **Figura 5.1**, podemos observar a organização do GNS, em particular do CNCS, em que a direção deste último contém um gabinete de estratégia e planeamento, bem como um Departamento de Operações e Controlo, Departamento de Investigação e Desenvolvimento e um Departamento de Qualidade, Sensibilização e Prevenção (GNS, n.d.).

Figura 5.1: Organograma da Estrutura do GNS



Retirado de GNS, n.d.

Porém, ainda há muito a fazer em Portugal quanto a este assunto. Em especial, consciencializar, sensibilizar e formar, acerca do ciberespaço, a sociedade de forma a alertar numa ótica de segurança (para os riscos e ameaças) e numa ótica de justiça, cidadania e democracia (J. C. Martins, 2015).

5.1 Estratégia Nacional de Cibersegurança

Como a sociedade, a economia e o Estado estão dependentes das TIC foi necessário criar legislação de acordo com a lei da União Europeia, salvaguardando os Direitos do Homem, para a proteção e defesa das infraestruturas críticas e dos principais serviços de informação. De modo a que todos os cidadãos, empresas e entidades, públicas e privadas, possam utilizar de forma segura, eficaz e eficiente o ciberespaço (*Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho, Presidência do Conselho de Ministros*).

A Estratégia Nacional de Cibersegurança foi criada nos termos da Resolução do Conselho de Ministros n.º 36/2015, de 12 junho, assentando em cinco pilares: subsidiariedade, complementaridade, cooperação, proporcionalidade e sensibilização. Por outras palavras, a estratégia procura sensibilizar para a segurança, mas a responsabilidade do que acontece no ciberespaço depende de cada um, cidadão ou entidade.

O principal desafio desta estratégia é a estimulação para uma *"utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos"* e em conjunto assegurar a *"proteção e defesa"* das infraestruturas críticas ou vitais (Sobral, 2014).

Deste modo, os objetivos principais da Estratégia Nacional de Cibersegurança são (*Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho, Presidência do Conselho de Ministros*; Sobral, 2014):

1) Garantir a segurança do ciberespaço;
2) Defender os interesses nacionais e a liberdade de ação no ciberespaço;
3) Fortalecer a segurança e defesa do ciberespaço das infraestruturas críticas nacionais;
4) Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.

A partir dos objetivos estratégicos foram criados seis eixos de intervenção, para reforçar o potencial estratégico nacional do ciberespaço, tais como (*Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho, Presidência do Conselho de Ministros*):

1) Estrutura de segurança do ciberespaço;
2) Combate ao cibercrime;
3) Proteção do ciberespaço e das infraestruturas;
4) Educação, sensibilização e prevenção;
5) Investigação e desenvolvimento;
6) Cooperação.

Concluindo, com a evolução das ameaças, das vulnerabilidades, dos processos e das infraestruturas é obrigatório a sua revisão regular e periódica, podendo esta ser feita de modo extraordinário, sempre que as circunstâncias o exigem, dentro dos seguintes modos: revisão no prazo máximo de três anos e a verificação anual dos objetivos estratégicos e das linhas de ação, adequando os mesmos à evolução das circunstâncias (*Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho, Presidência do Conselho de Ministros*).

6 RESULTADOS E DISCUSSÃO DOS MESMOS

A amostra corresponde a 111 respostas completas do inquérito, contudo houveram mais 31 respostas, mas encontravam-se incompletas pelo que não foram contabilizadas para o estudo. A única exigência pretendida no inquérito era habitar em Portugal e fazer utilização da *Internet*, mesmo que fosse esporadicamente.

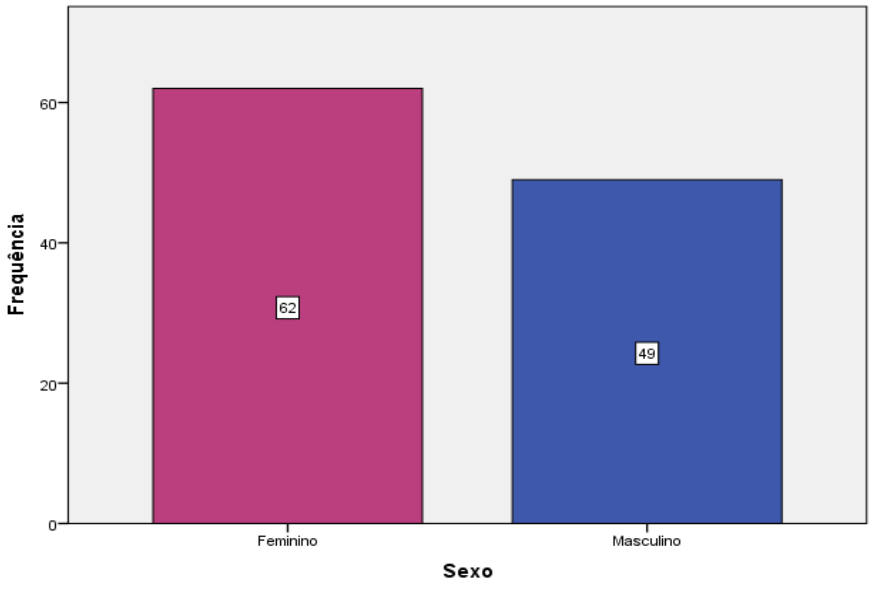
O inquérito encontrava-se dividido em nove partes que correspondem: aos Dados Pessoais; à caracterização a utilização pessoal de dispositivos de navegação na *Internet*; às Redes Sociais; a perceção acerca da utilização e da segurança informática; à privacidade, proteção e segurança na Internet; às *passwords*; à criminalidade informática; e, por fim, facultativo, comentários e sugestões em relação ao inquérito.

Todos os dados recolhidos foram tratados, inicialmente, no LimeSurvey, *software* onde o inquérito se encontrava hospedado *online*, e, posteriormente, analisados através de uma aplicação informática designada de IBM® SPSS® Statistics 22.

6.1 Dados Pessoais

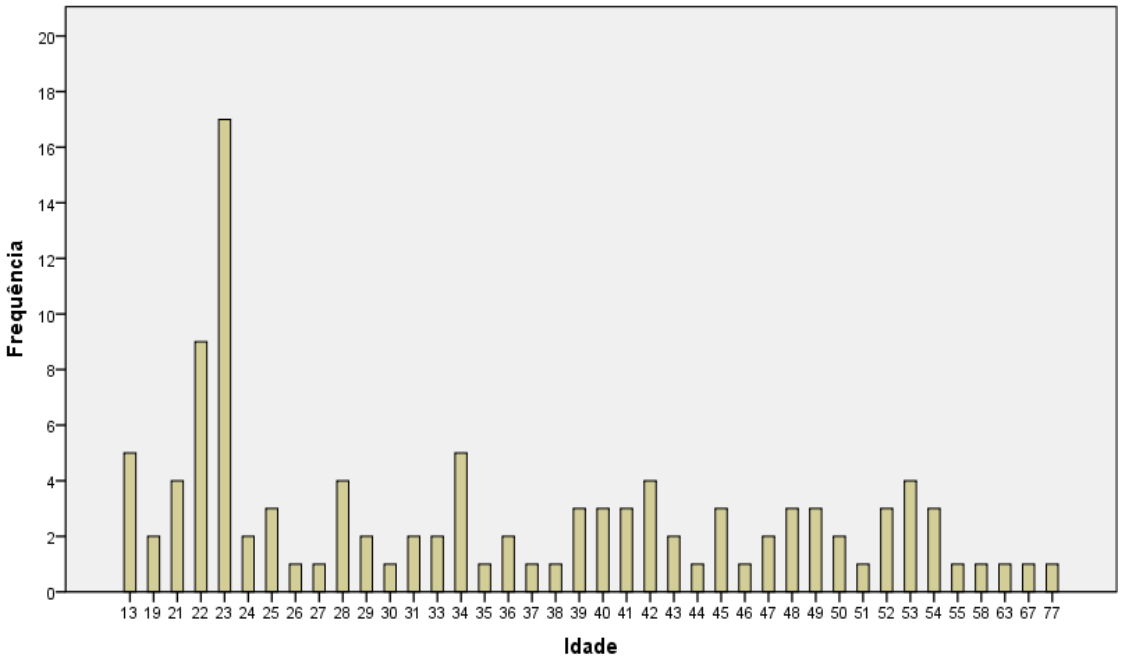
A amostra, como se pode comprovar pelas tabelas e gráficos a seguir, é de 111 pessoas com uma idade compreendida entre 13 e 77 anos, sendo que destas 62 são do sexo feminino e 49 do sexo masculino.

Gráfico 6.1: Gráfico ilustrativo do parâmetro «Sexo» do inquérito



Como referido anteriormente, em relação ao parâmetro «Idade», a idade das respostas obtidas estão entre os 13 e os 77 anos, existindo uma maior influência nos 23 anos (com 17 respostas).

Gráfico 6.2: Gráfico ilustrativo do parâmetro «Idade» do inquérito



Esmiuçando estes dois parâmetros, podemos constatar que 62 respostas do sexo feminino, a média de idades são de, aproximadamente, 30 anos (com um erro padrão de cerca de dois anos). O mínimo de idade é de 13 anos e o máximo é 67 anos. Em comparação, com as 49 respostas do sexo masculino, a média de idades são, de aproximadamente, 39 anos (com um erro padrão de dois anos). E, o mínimo de idade é, como na amostra do sexo feminino, 13 anos enquanto que, o máximo é 77 anos.

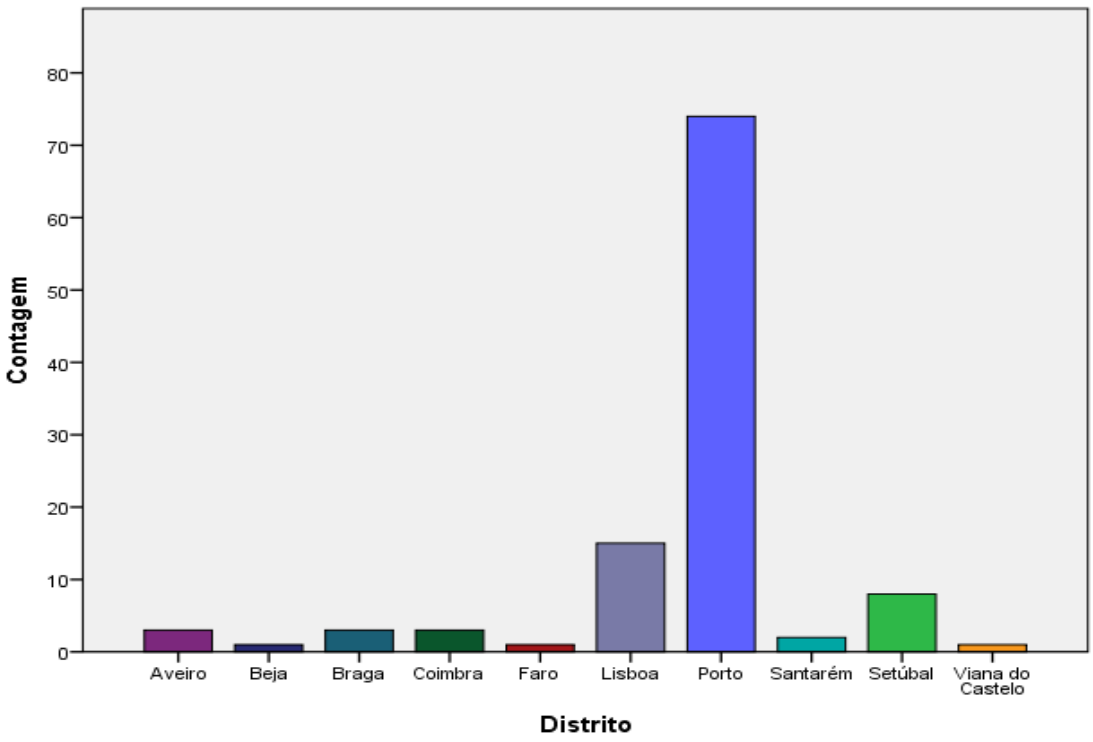
Tabela 6.1: Tabela descritiva da estatística referente aos dados relativos da Idade em função do Sexo

	Sexo			***Estatística***	***Erro Padrão***
Idade	Feminino	Média		30,73	1,624
		95% Intervalo de Confiança para Média	Limite inferior	27,48	
			Limite superior	33,97	
		Mediana		24,00	
		Desvio Padrão		12,787	
		Mínimo		13	
		Máximo		67	

	Masculino	Média		39,84	1,770
		95% Intervalo de Confiança para Média	Limite inferior	36,28	
			Limite superior	43,39	
		Mediana		41,00	
		Desvio Padrão		12,387	
		Mínimo		13	
		Máximo		77	

O Distrito com maior amostragem foi o Porto (com 74 respostas), contando com apenas 15 respostas de Lisboa e oito respostas de Setúbal. Os restantes distritos não atingiram mais do que três respostas, como se pode verificar pelo gráfico abaixo.

Gráfico 6.3: Gráfico ilustrativo do número de respostas de cada Distrito

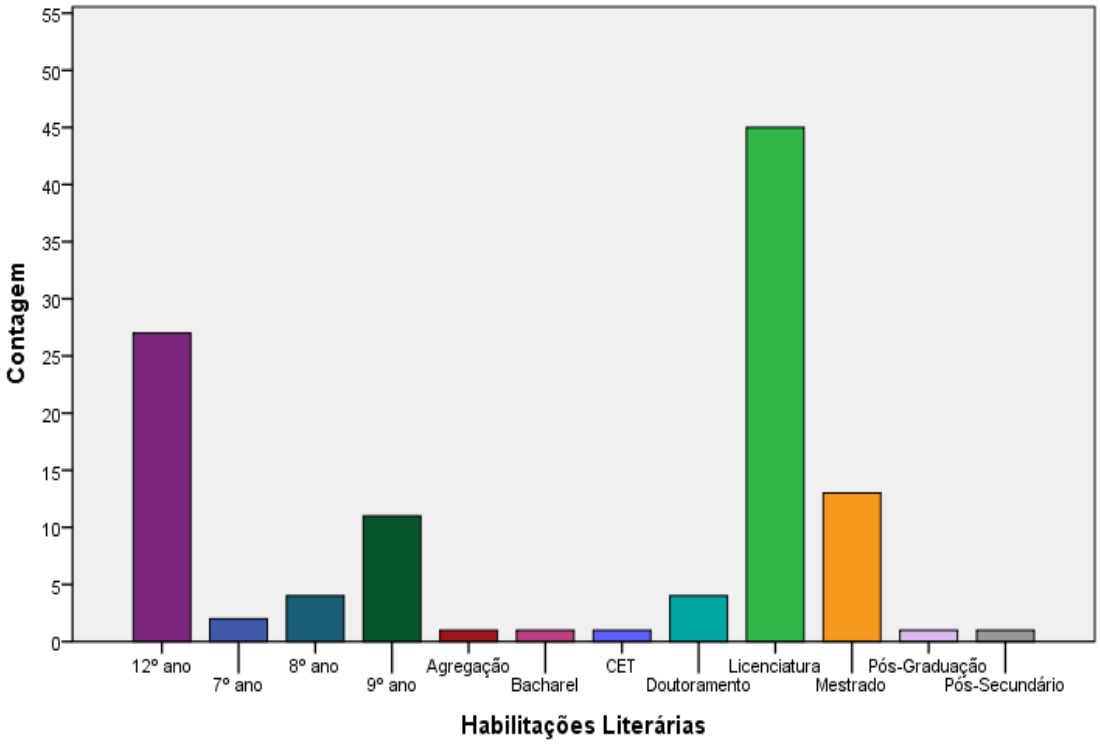


Em relação à nacionalidade das respostas desta amostra foram na sua totalidade 111 de origem portuguesa.

No parâmetro relativo às «Habilitações literárias (completas)», a maioria responderam Licenciatura (45 respostas) e 12º Ano (27 respostas). Com esta pergunta podemos observar um alargado mundo de respostas, o que implica que a utilização da *Internet* não tem nada que ver com as habilitações académicas. Mais à frente, poderemos confirmar que a segurança informática também não, por outras palavras, as

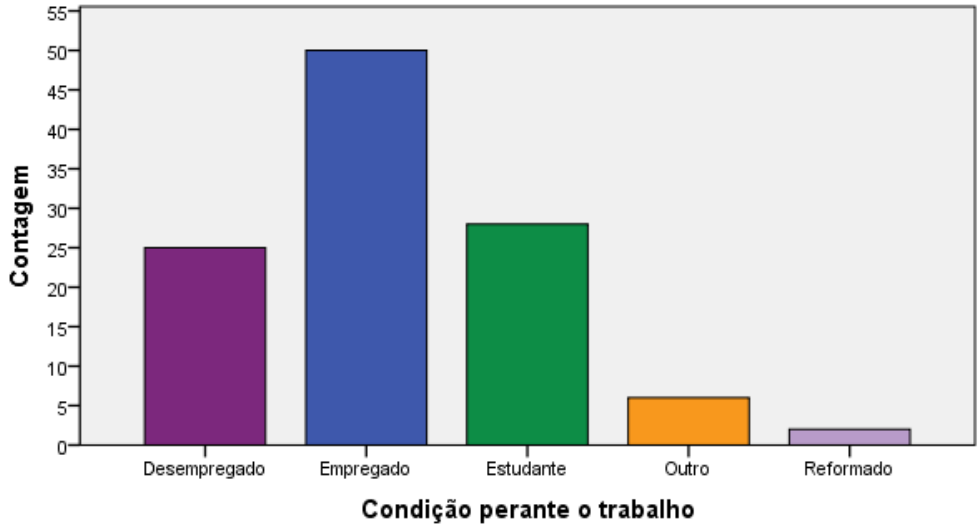
habilitações literárias não implica um maior conhecimento da proteção e segurança na *Internet*.

Gráfico 6.4: Gráfico ilustrativo do parâmetro «Habilitações literárias (completas)»



Por último, no parâmetro «Condição perante o trabalho», as respostas foram diversas sendo os principais: Empregado (50 respostas), Estudante (28 respostas) e Desempregado (25 respostas). Dentro da resposta «Outro» engloba respostas como trabalhador-estudante, profissional independente, profissional liberal e não especificado.

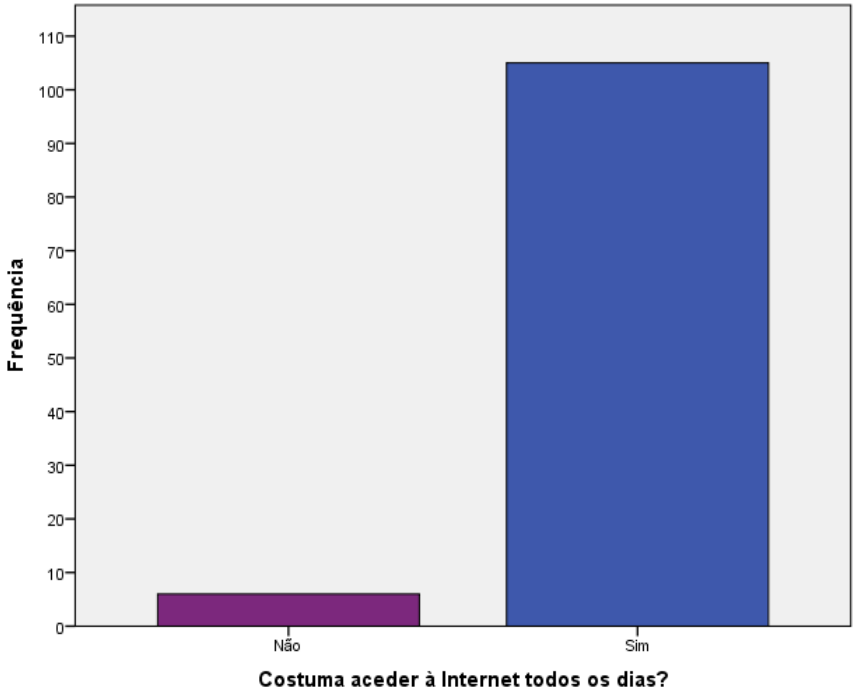
Gráfico 6.5: Gráfico ilustrativo das respostas quanto à condição perante o trabalho



6.2 Caraterização da utilização pessoal de dispositivos de navegação na Internet

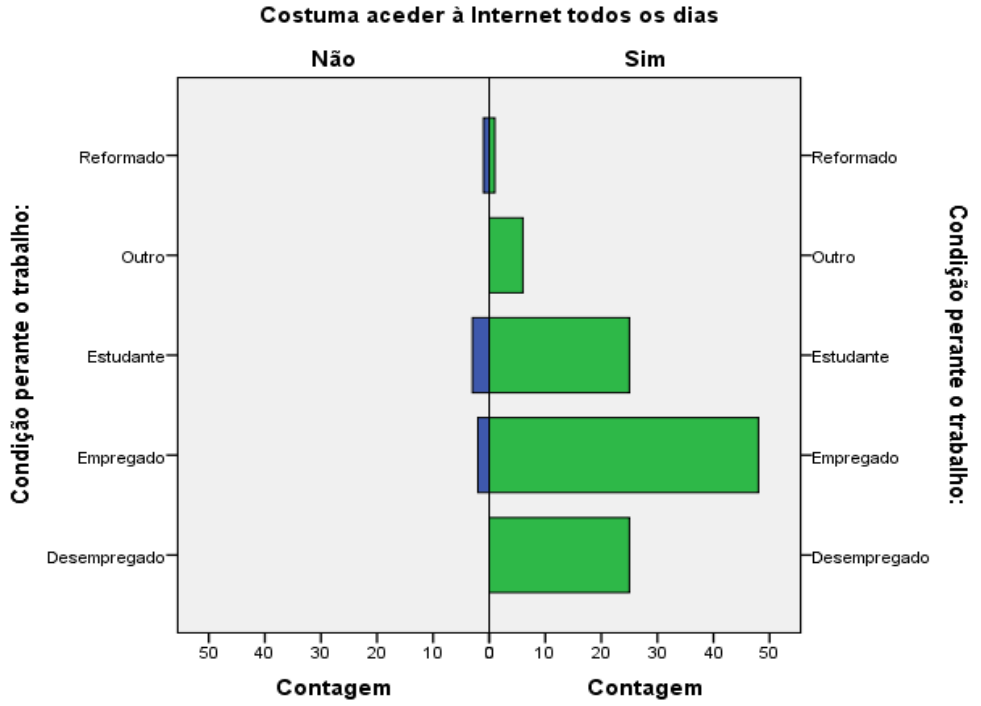
Quando se questiona os inquiridos se costumam aceder à *Internet* todos os dias, a esmagadora maioria responde que sim, sendo que apenas cerca de 5% responde negativamente.

Gráfico 6.6: Gráfico ilustrativo das respostas dos inquiridos em relação à questão «Costuma aceder à *Internet* todos os dias»



Fazendo uma comparação entre a condição dos inquiridos perante o trabalho e se acede à *Internet* todos os dias, ao contrário do que seria de esperar a maioria não são os estudantes, mas os inquiridos que se encontram empregados.

Gráfico 6.7: Gráfico de barras em Cluster referente à comparação entre duas variáveis: condição perante o trabalho e se costuma aceder à *Internet* todos os dias



Na questão «Qual o *site* que acede primeiro» a grande maioria dos inquiridos afirma ser o Google, com 39 respostas, e o Facebook, com 33 respostas.

Tabela 6.2: Tabela de frequência acerca do primeiro *site* acedido pelos inquiridos

SITE ACEDIDO	FREQ.	PERCENT. (%)	SITE ACEDIDO	FREQ.	PERCENT. (%)
Citius	1	0,9	Islagaia	1	0,9
Correio da Manhã	1	0,9	JN	1	0,9
DR	1	0,9	Nenhum em particular	1	0,9
Email	3	2,7	Observador	1	0,9
Entidade Empregadora	1	0,9	Outlook	2	1,8
Facebook	33	29,7	Pplware	1	0,9
Gmail	11	9,9	Publico	1	0,9
Google	39	35,1	Relacionados com notícias atuais	1	0,9
Google notícias	1	0,9	Sapo	2	1,8
Hotmail	3	2,7	The Guardian	1	0,9

SITE ACEDIDO	FREQ.	PERCENT. (%)	SITE ACEDIDO	FREQ.	PERCENT. (%)
Instagram	1	0,9	TV Calendar	1	0,9
Intranet do serviço (PSP)	1	0,9	TVI24	1	0,9
Youtube	1	0,9	**TOTAL**	111	100

Seguidamente, questionou-se os inquiridos acerca do tipo de dispositivo que utilizavam para a navegação na *Internet* obtendo-se os seguintes resultados (**Tabela 6.3**):

Tabela 6.3: Tabela de frequências relativa à questão «Com que dispositivo (s) costuma aceder à *Internet*»

Resposta	Frequência	Percentagem (%)
***Desktop* (Computador Fixo)**	36	32,43
Portátil	75	67,57
Smartphone	73	65,77
Outro	5	4,50

Como esta questão se tratava de uma questão de múltiplas escolhas, temos vários inquiridos a utilizar mais do que um dispositivo. Deste modo, o **Gráfico 6.8** demonstra, em quantidade, a múltipla utilização dos dispositivos por parte dos inquiridos.

Assim, de um modo geral, os dispositivos de eleição para a navegação na *Internet* são o Portátil e o *Smartphone*, com 30 respostas. Sendo que, como observável na **Tabela 6.4**, cinco das 111 respostas ainda referiram a utilização do Tablet e de um telemóvel.

Gráfico 6.8: Gráfico demonstrativo do tipo de dispositivo utilizado para a navegação na *Internet*, por parte dos inquiridos

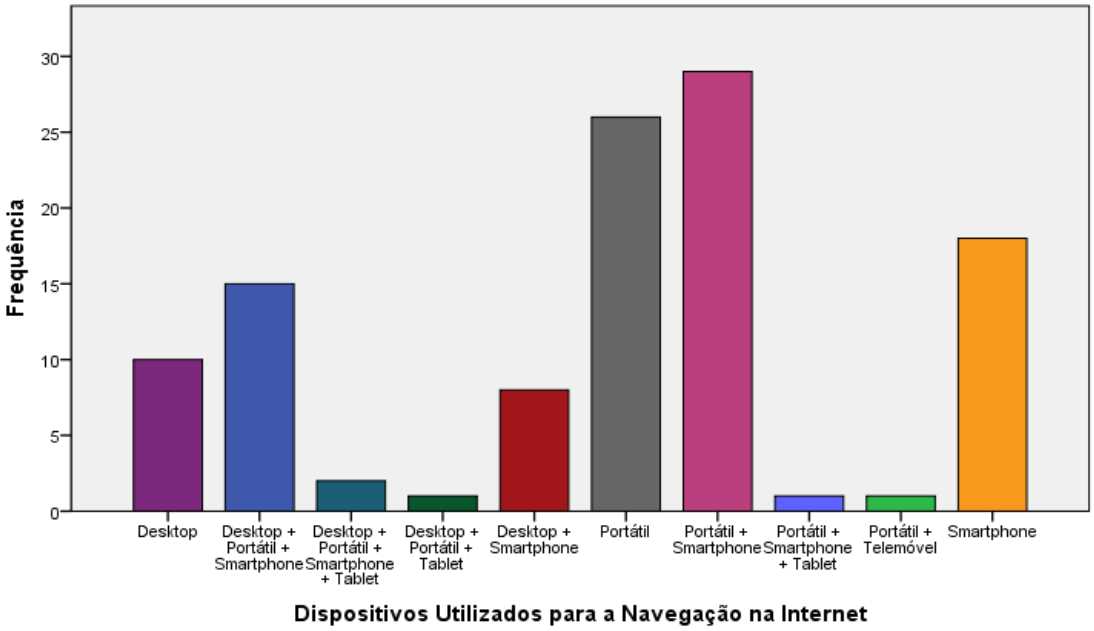


Tabela 6.4: Tabela descritiva da resposta «Outro» referente ao tipo de dispositivo utilizado para a navegação na *Internet*

Outro Dispositivo	Frequência	Percentagem (%)
Tablet	4	95,5
Telemóvel	1	3,6

Mediante a resposta da questão anterior, os inquiridos teriam algumas perguntas extras. Se os inquiridos respondessem que o dispositivo utilizado era o «Desktop» ou o «Portátil» teriam de especificar o sistema operativo que utilizavam (em caso da escolha ser «*Windows*» ainda teriam de enunciar a versão) e a frequência com que atualizavam o mesmo. Por outro lado, se os inquiridos respondessem «*Smartphone*» apenas teriam de indicar qual o sistema operativo do mesmo.

Como tal, a amostra nestas questões não será de 111 respostas. No caso das respostas «Desktop» ou «Portátil» a amostra é de 93 enquanto que, para a resposta «*Smartphone*» a amostra é de 73.

Assim, os resultados apresentados nos seguintes gráficos e tabelas elucidam que:

- 84 das 93 respostas utilizam o sistema operativo «*Windows*»;
- 67 das 93 respostas refere que atualiza o sistema operativo sempre que este avisa;
- 53 dos 84 inquiridos do sistema operativo «*Windows*» utilizam a versão mais recente, *Windows* 10;

- 60 das 73 respostas utiliza no *Smartphone* o sistema operativo «*Android*».

Gráfico 6.9: Gráfico ilustrativo das respostas dos inquiridos em relação ao Sistema Operativo do Portátil ou do *Desktop*

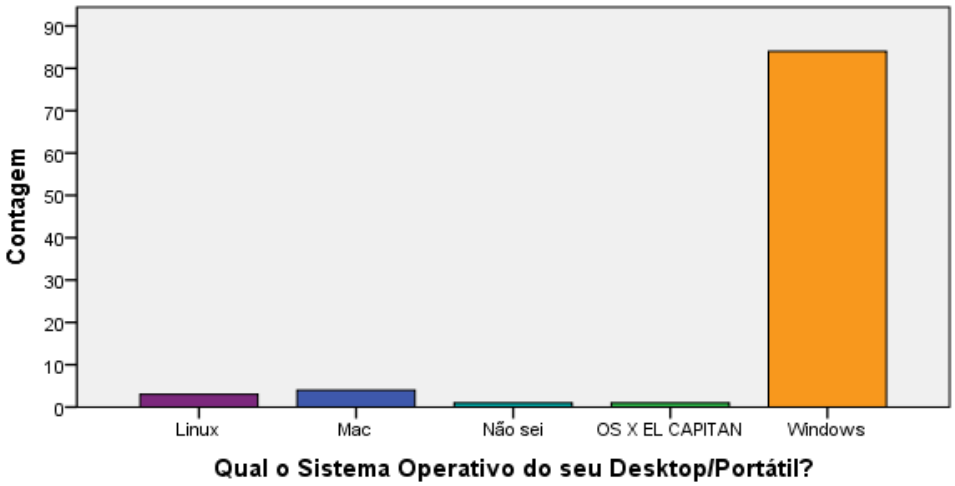


Tabela 6.5: Tabela de frequências acerca da pergunta «Com que frequência atualiza o seu sistema operativo»

Resposta	Frequência	Percentagem (%)
Esporadicamente	20	21,51
Sempre o que Sistema me avisa	67	72,04
Não atualizo	6	6,45

Gráfico 6.10: Gráfico ilustrativo da versão do Sistema Operativo *Windows* utilizado pelos inquiridos

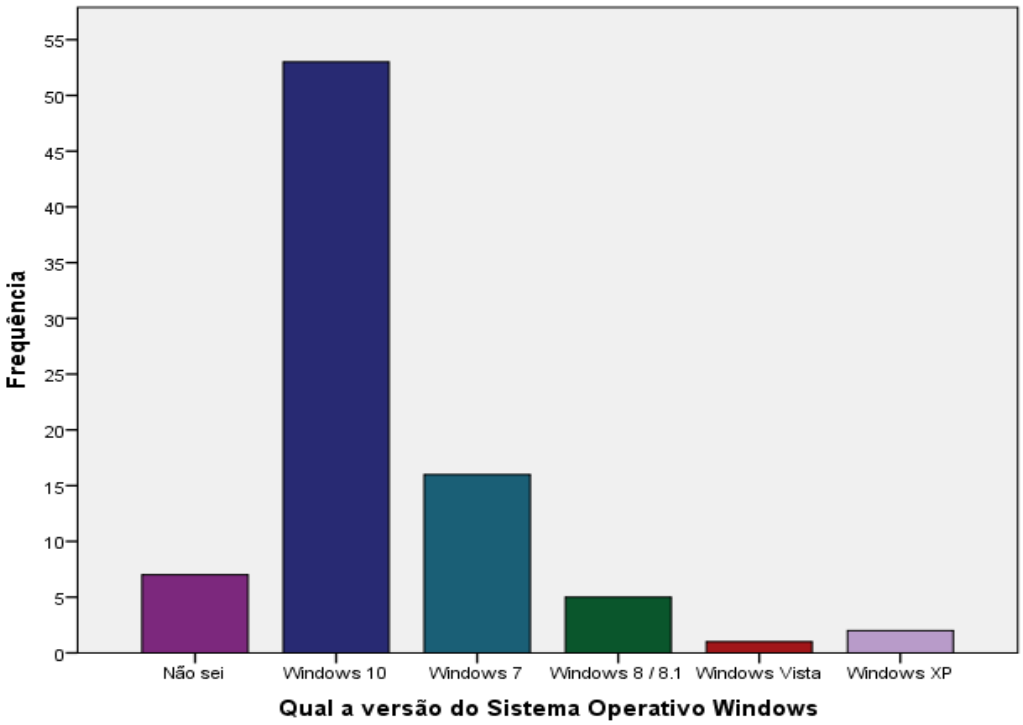
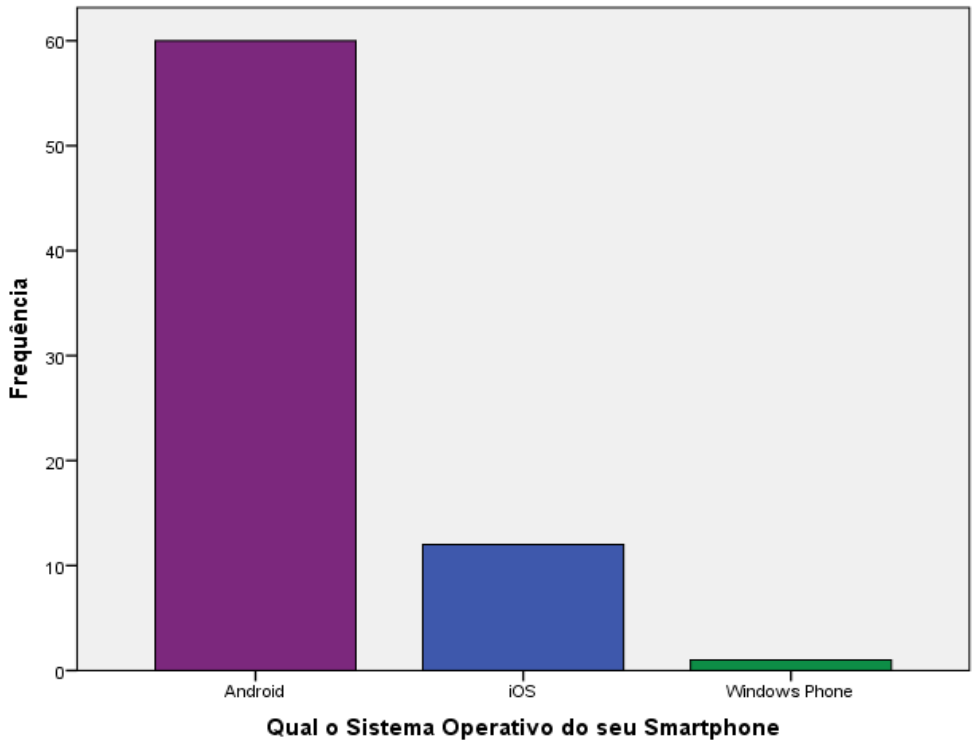


Gráfico 6.11: Gráfico relativo à questão «Qual o sistema operativo do seu *Smartphone*»



Continuamente, questionou-se os inquiridos sobre o (s) *browser* (s) que utilizavam para a navegação na *Internet* obtendo-se os seguintes resultados (**Tabela 6.6**):

Tabela 6.6: Tabela de frequências relativa à questão «Que *browser* (s) utiliza para aceder à *Internet*»

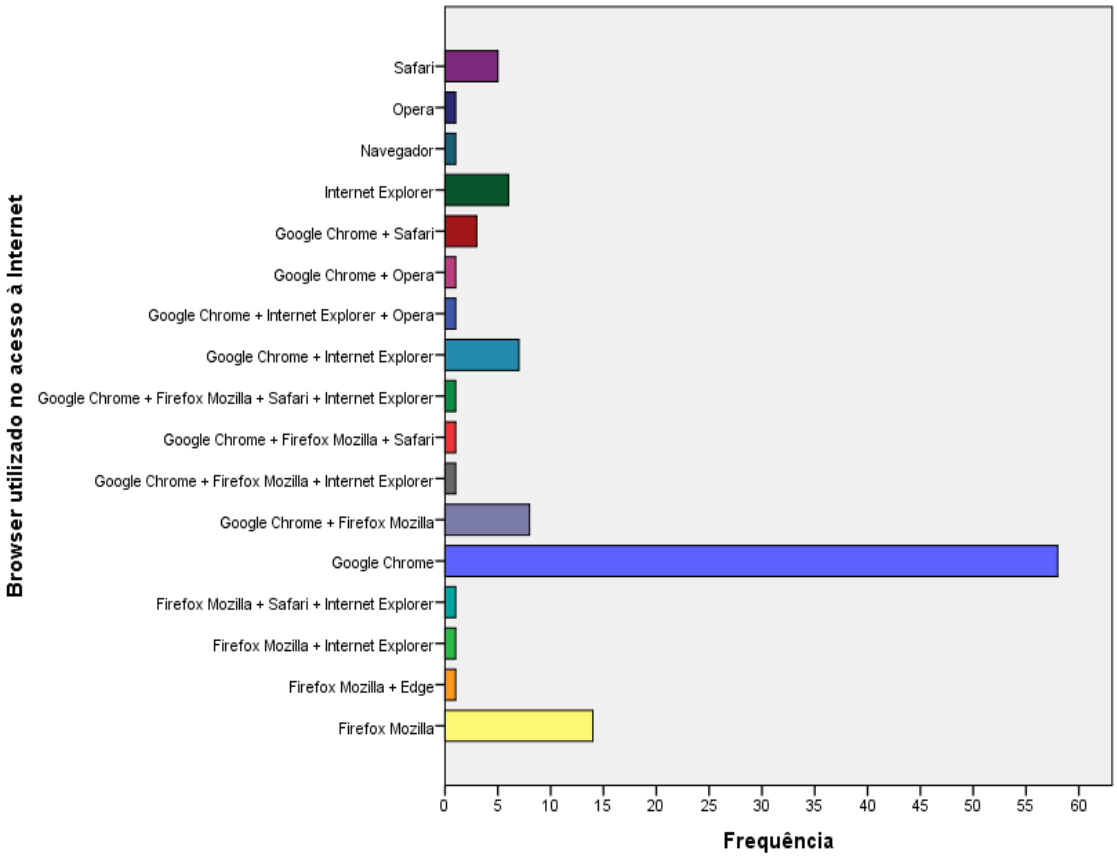
Resposta	Frequência	Percentagem (%)
Google Chrome	81	72,97
Firefox Mozilla	28	25,23
Safari	11	9,91
Internet Explorer	18	16,22
Outro	5	4,50

Na opção «Outro» as respostas do *browser* utilizado foram: Opera (com três respostas), Edge e Navegador (cada um com apenas uma resposta).

Por esta questão ser de múltiplas escolhas, existem várias pessoas que utilizam mais do que um *browser* para acederem à *Internet*. De qualquer modo, o seguinte gráfico ilustra, em quantidade, a múltipla utilização dos *browsers*.

Portanto, contrariamente ao pensado inicialmente, a maioria das pessoas não utiliza múltiplos *browsers* para aceder à *Internet*, mas sim apenas um *browser*. Dos 111 inquiridos, 58 utilizam o Google Chrome e, em segundo lugar, o Firefox Mozilla com 14 inquiridos.

Gráfico 6.12: Gráfico demonstrativo do (s) *browser* (s) utilizado (s), pelos inquiridos, para aceder à *Internet*



Na questão seguinte do inquérito, a questão volta a ser de múltipla escolha acerca do tipo de ferramenta utilizam para se protegerem enquanto navegam na *Internet*.

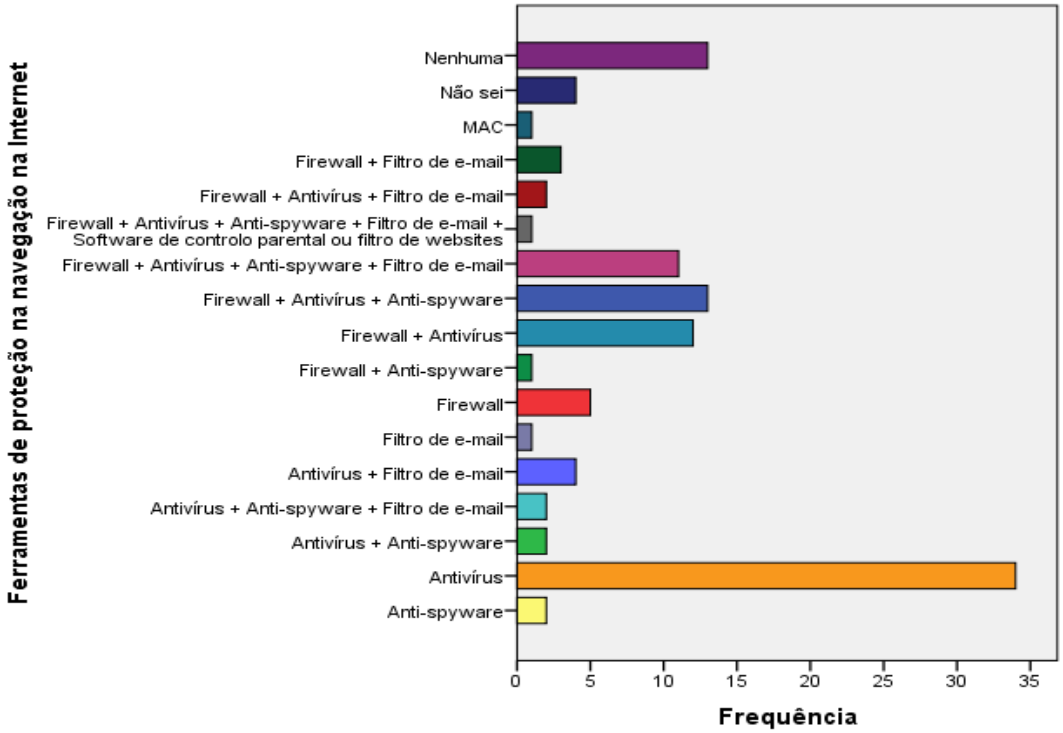
Nos resultados apresentados, através de gráficos, o tipo de resposta foi encurtado devido a ser uma resposta extensa. Contudo, as possíveis respostas nesta questão são: *Firewall*; Antivírus; *Anti-spyware* e/ou *Anti-malware*; Filtro de *e-mail* para prevenir a receção de SPAM; *Software* de controlo parental ou filtro de *websites*; Nenhuma; e, por fim, Outro.

Tabela 6.7: Tabela de frequências relativa à questão «Que ferramenta (s) utiliza para a sua proteção enquanto navega na *Internet*»

Resposta	Frequência	Percentagem (%)
Firewall	49	44,14
Antivírus	81	72,97

Resposta	Frequência	Percentagem (%)
Anti-spyware* e/ou *Anti-malware	32	28,83
Filtro de *e-mail* para prevenir a receção de SPAM	24	21,62
Software* de controlo parental ou filtro de *websites	1	0,9
Nenhuma	13	11,71
Outro	5	4,50

Gráfico 6.13: Gráfico ilustrativo das ferramentas de proteção utilizadas pelos inquiridos na navegação na *Internet*



Assim, nesta questão, podemos verificar que a maior parte das pessoas (34) utiliza apenas o antivírus para se proteger, sendo que 13 dos inquiridos refere que não utiliza nenhuma ferramenta de proteção.

Por fim, para finalizar em alguns casos, mediante as respostas na questão anterior, os inquiridos teriam algumas perguntas extra de forma a perceber qual a ferramenta utilizavam ao certo e a sua forma de utilização, ou seja, com que frequência atualizavam e se realizavam análises com algumas delas ao dispositivo que utilizavam. Como seria de esperar, a amostra nestas questões muda, não atingindo as 111 respostas.

As perguntas efetuadas foram: o antivírus utilizado (amostragem de 81 respostas), a frequência com que atualiza o antivírus e/ou o *anti-spyware* ou *anti-*

malware e frequência que realiza análises ao dispositivo de navegação com essas ferramentas (amostra de 84 respostas), e, a *firewall* utilizada (49 respostas).

Assim, os resultados apresentados nos seguintes gráficos e tabelas elucidam que:

- 30 das 81 respostas utilizam o Avast como antivírus;
- Aproximadamente 58% das 84 respostas afirmam que têm as atualizações automáticas das ferramentas: antivírus e/ou *anti-spyware*/*anti-malware*;
- Apenas uma resposta afirma que não atualiza estas ferramentas;
- 26 das 84 respostas apenas quando suspeitam de algum ficheiro é que efetuam uma análise ao dispositivo de navegação na *Internet*;
- Das 84 respostas apenas quatro nunca realizam qualquer tipo de análise ao dispositivo utilizado;
- Em relação à *firewall* utilizada, 27 das 49 respostas utilizam a *firewall* do *Windows*;
- Ainda em relação à *firewall*, podemos ver que as pessoas encontram-se bem informadas à ferramenta que utilizam uma vez que apenas três respostas foram «Não sei»;
- As respostas de outra *firewall* utilizada foram: Komodo (uma), Própria do Router (uma) e *firewall* nativa dos sistemas operativos da *Apple* (duas).

Gráfico 6.14: Gráfico ilustrativo das respostas dos inquiridos em relação ao Antivírus utilizado

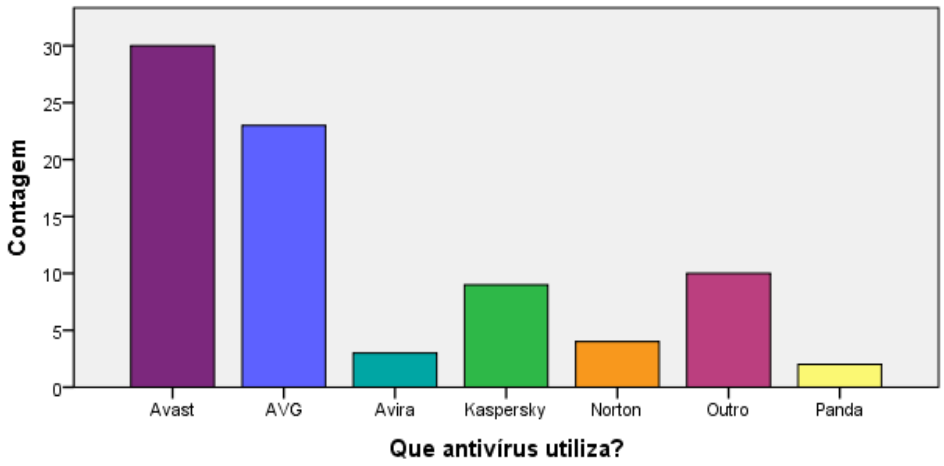


Tabela 6.8: Tabela de frequências acerca da pergunta «Com que frequência atualiza o seu antivírus e/ou *anti-spyware*/*anti-malware*»

Resposta	Frequência	Percentagem (%)
Não atualizo	1	1,19
Atualizações automáticas	49	58,33
Sempre que recebo notificações	34	40,48

Gráfico 6.15: Gráfico ilustrativo da frequência que os inquiridos realizam análises ao seu dispositivo de navegação na *Internet*

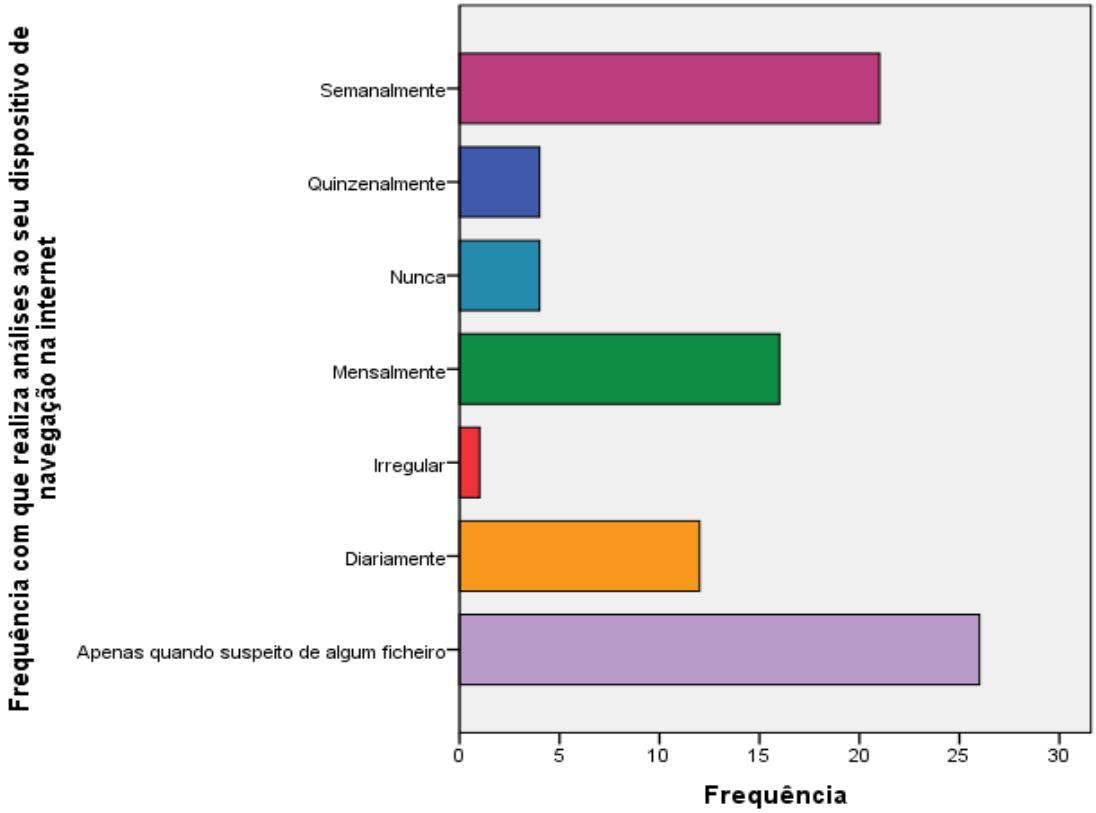
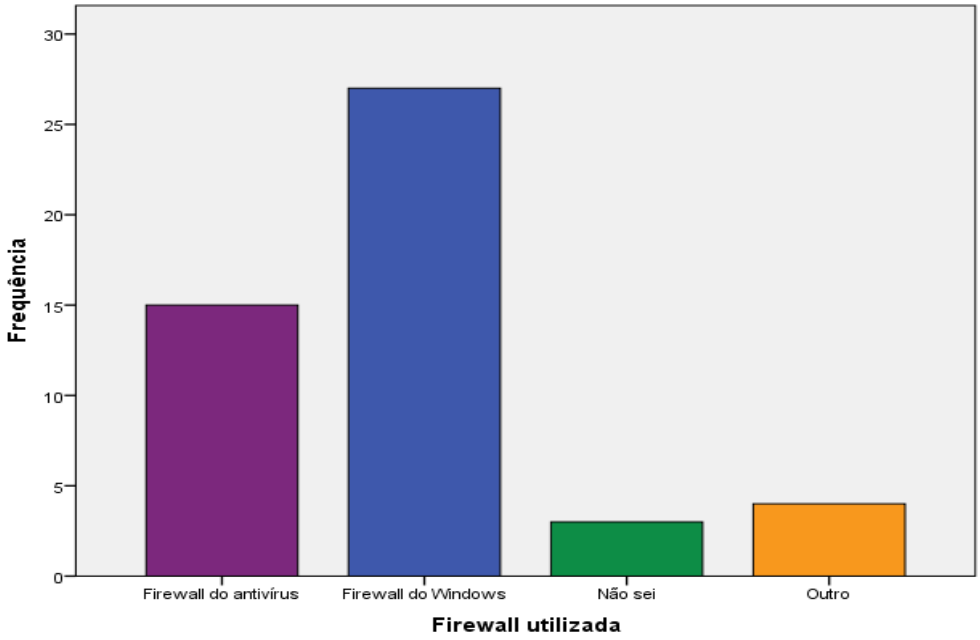


Gráfico 6.16: Gráfico demonstrativo da *firewall* utilizada pelos inquiridos

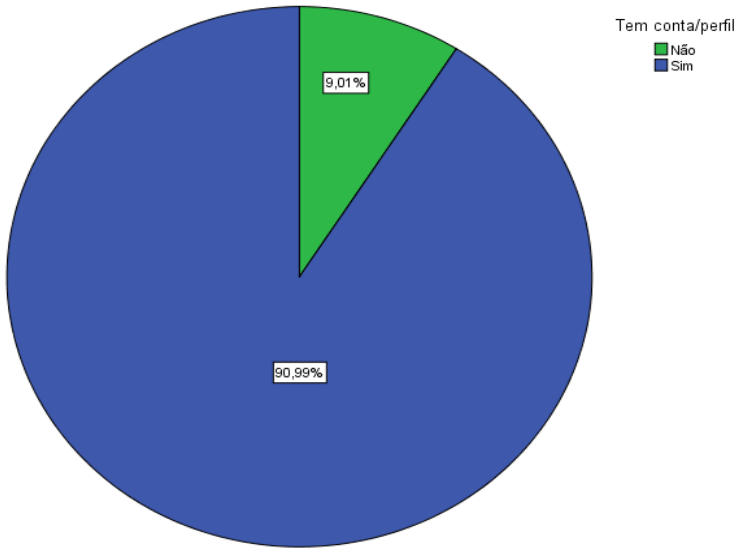


6.3 Redes Sociais

Numa terceira parte do inquérito inquiriu-se as pessoas em relação às redes sociais e quem pertencesse a uma rede social indagou-se qual seria ou quais seriam, a frequência com que a acediam, o fim para que a utilizavam, o tipo de perfil tinham e se aceitariam na sua rede de amigos alguém que não conhecessem. Os resultados da amostragem de 111 respostas pode-se observar nos seguintes gráficos e tabelas.

Em relação à questão se teriam um conta ou perfil numa rede social a esmagadora maioria (101) respondeu afirmativamente. Deste modo, nas seguintes perguntas a amostragem passa para 101 respostas.

Gráfico 6.17: Gráfico de pizza, em percentagem, relativo à questão «Tem alguma conta/perfil numa rede social?»



A tabela seguinte corresponde a uma questão de múltiplas escolhas acerca de qual rede social utilizam, adquirindo-se 99 respostas que utilizam o Facebook.

Tabela 6.9: Tabela de frequências acerca de qual ou quais rede social os inquiridos utilizam

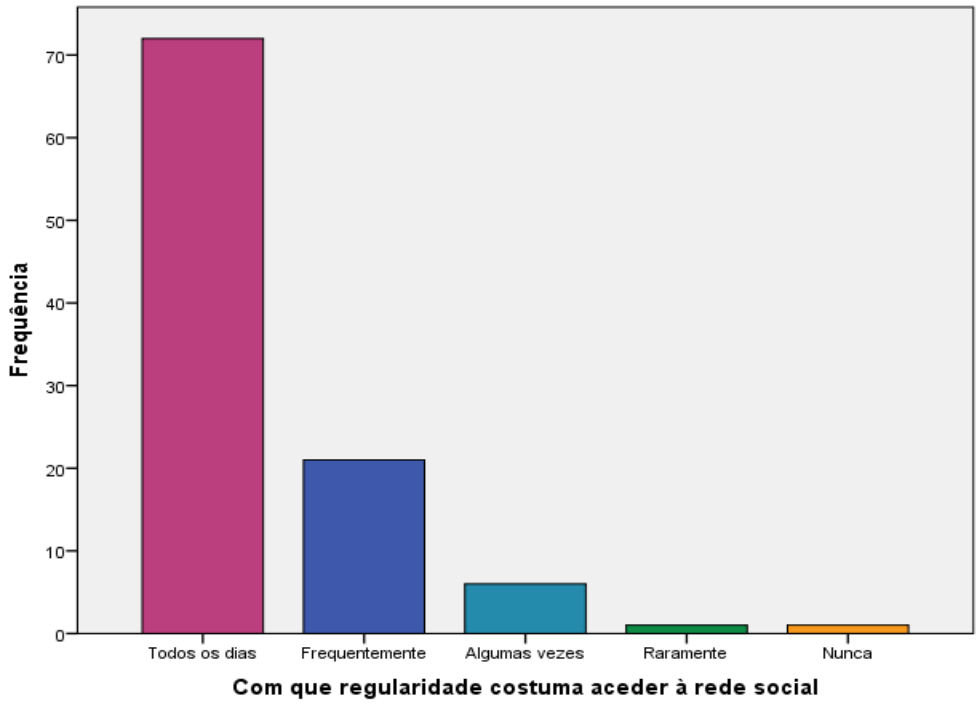
Resposta	Frequência	Percentagem (%)
Facebook	99	98,02
Google +	49	48,51
Instagram	44	43,56
LinkedIn	45	44,55
Pinterest	16	15,84
Tumblr	10	9,90
Twitter	24	23,76
Youtube	39	38,61
Outro	4	3,96

Em relação à rede social respondida em «Outro» foram: We Heart It (uma), Whatsapp (duas) e Blogspot (uma). Nesta última (Blogspot) erradamente pelo inquirido foi considerada uma rede social, contudo este não é uma rede social e sim um *blog*. Este meio não é considerado uma rede social pois o seu objetivo principal não é criar uma rede de comunicação, mas sim apenas divulgar uma ideia ou simplesmente partilhar um determinado conteúdo de uma forma simples e rápida.

De um modo generalizado, sem entrar em muito pormenor, podemos, pelo **Gráfico 8.0.1** no **Apêndice B**, comprovar que das 101 respostas, na sua maioria as redes sociais mais utilizadas em simultâneo pelos utilizadores inquiridos são o Facebook (por si só) e o Instagram e Facebook em conjunto.

Quanto à questão da regularidade em que o utilizador acede à (s) rede (s) social (sociais) a grande maioria (71%) respondeu que acedia «Todos os dias».

Gráfico 6.18: Gráfico de barras referente à questão colocada «Com que regularidade costuma aceder à rede social»



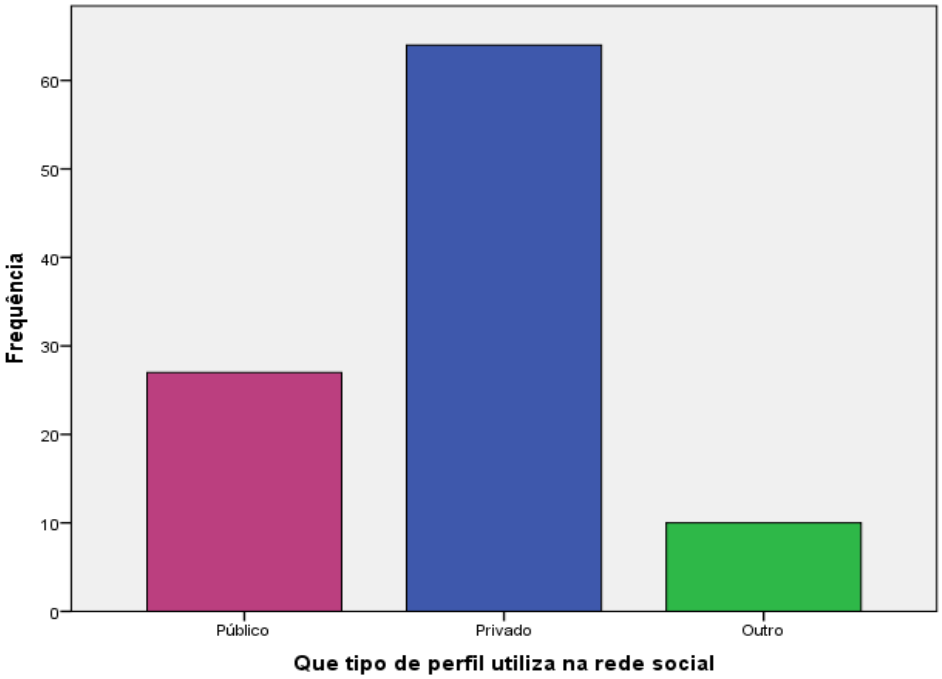
Na pergunta de resposta curta «Com que fim costuma utilizar a rede social?», as respostas foram variadas, sendo que apenas se obtiveram 100 respostas da amostra de 101 respostas. Mas, na sua grande maioria, utiliza as redes sociais para saber as notícias e se manter atualizado, para fins profissionais ou de negócio, para comunicar/socializar virtualmente com os amigos e familiares, próximos e/ou distantes de si, para entretenimento pessoal e para jogar jogos.

Na questão acerca do tipo de perfil utilizado na rede social pode-se observar, pelo **Gráfico 6.19**, que 64 das 101 respostas têm um perfil privado, 27 têm o perfil público e dez responderam «Outro».

A resposta «Outro» engloba respostas em que o perfil é só para Amigos (o que nesta pergunta se pode englobar como privado pois, por exemplo, qualquer publicação só será visualizada por amigos que a pessoa previamente aceitou); não sabe o tipo de perfil tem; a utilização de ambos, quer privado quer público; que depende da rede social; e, que no meio pessoal utiliza um perfil privado e no meio profissional utiliza um perfil público.

Com estas respostas contrariamente o que seria de imaginar no início, a população encontra-se bem informada na questão da utilização de um perfil privado para o meio pessoal da mesma.

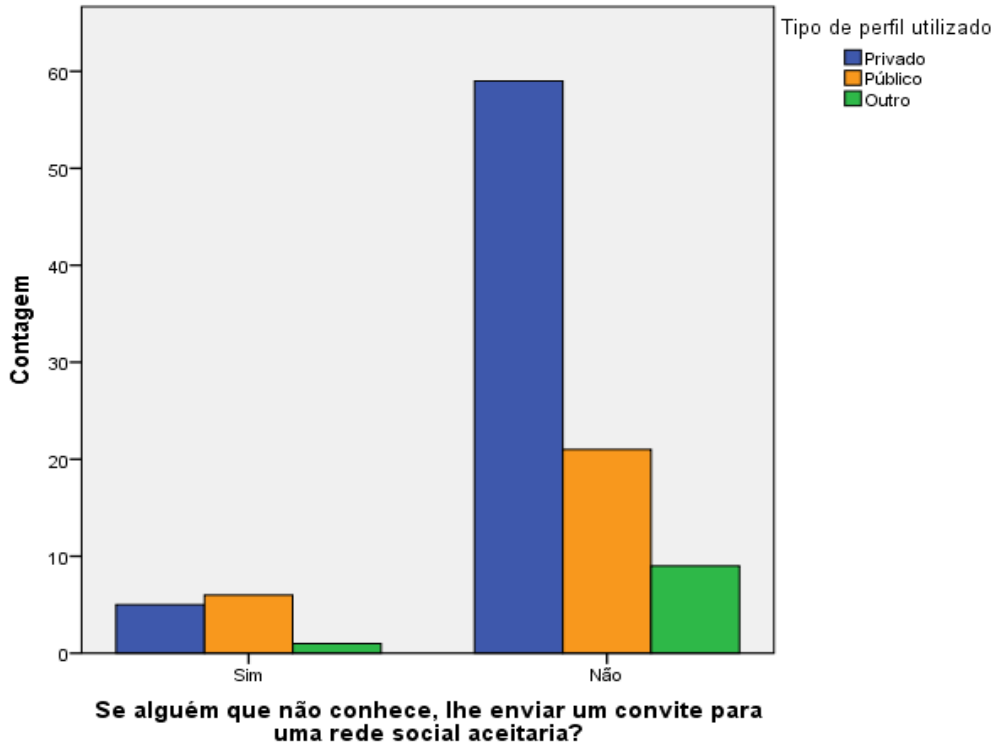
Gráfico 6.19: Gráfico de barras sobre o tipo de perfil utilizado, pelos inquiridos, na rede social



Por fim, mas sem menos valor, na questão se o inquirido aceitaria o convite, enviado para uma rede social, de alguém que não conhece, a resposta dada foi, em cerca de 88%, a recusa do convite e, apenas 12 aceitariam o convite.

Comparando o tipo de perfil com a resposta dada a esta questão podemos constatar que cinco dos 12 que aceitariam têm um perfil privado e 6 têm um perfil público. Deste modo, apesar de não ser uma amostra representativa e não se saber em que tipos de circunstâncias aceitariam o convite, podemos reconhecer que existe uma consciencialização e cuidado da parte da população portuguesa para as redes sociais.

Gráfico 6.20: Gráfico de barras, em Cluster, comparativo da resposta dada sobre o tipo de perfil utilizado na rede social e a resposta dada sobre a aceitação e não-aceitação de um convite feito por um desconhecido

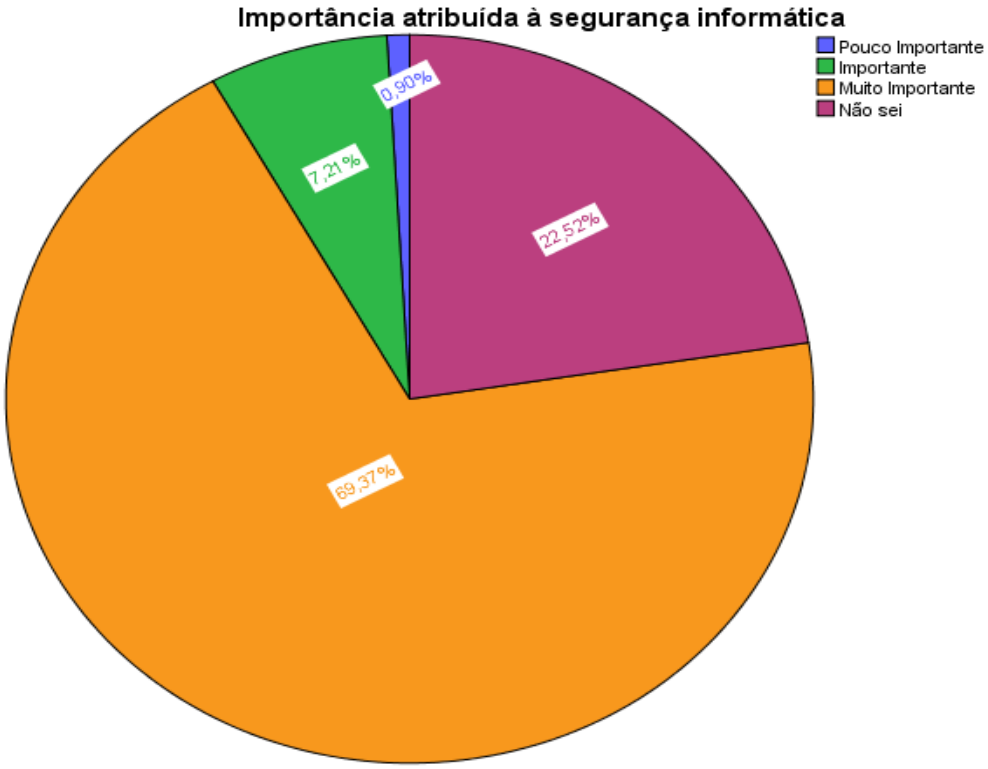


6.4 Perceção acerca da utilização e da segurança informática

Nesta parte do inquérito, tenciona-se saber a opinião dos inquiridos, enquanto utilizadores das tecnologias, quanto à importância que dão à segurança informática e o modo como utilizam a *Internet*.

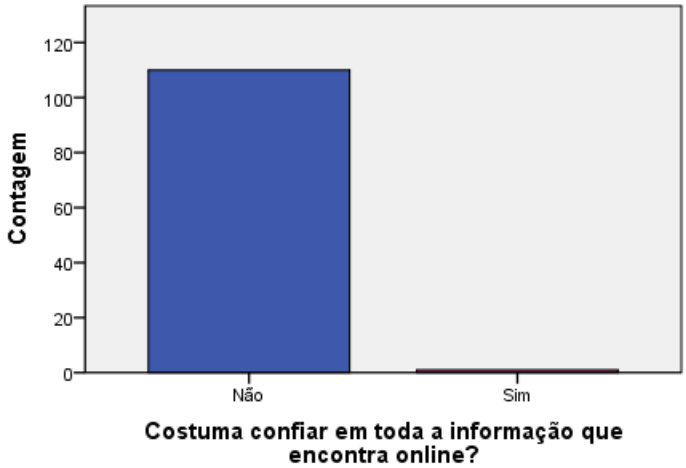
Na amostra de 111 respostas encontramos duas vertentes contrárias entre si, isto é, cerca de 69% das respostas atribuem que a segurança informática é muito importante, por outro lado, cerca de 23% responde que não sabe que importância atribuir a esta.

Gráfico 6.21: Gráfico de pizza, de percentagem, acerca da atribuição que os inquiridos dão à segurança informática



Através da seguinte questão, podemos verificar que quase toda a amostra de inquiridos compreende que nem toda a informação que existe disponivel na *Internet* deve ser considerada verdade.

Gráfico 6.22: Gráfico de barras relativo à questão «Costuma confiar em toda a informação que encontra *online*?»



Na questão relativa à informação relevante que possa ser deixada pelos inquiridos nos *sites* em que acedem, pode denotar-se que os inquiridos encontram-se

relativamente bem informados, denotando que conseguem identificar os *sites* fidedignos. Assim, pode-se na **Tabela 6.10** observar as respostas dadas.

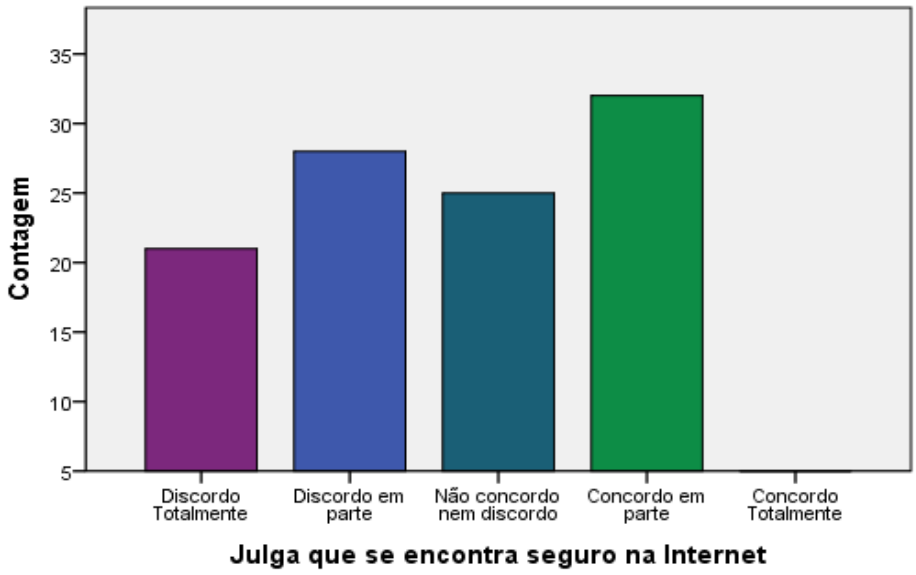
Convém ressalvar que nas respostas dadas em «Outro», um dos inquiridos encontra-se bem informado, uma vez que referiu, e muito bem, que não deixa conscientemente informações relevantes porém, "é possível que alguns *sites* obtenham informação como endereço de IP e geolocalização".

Tabela 6.10: Tabela de frequências sobre a informação relevante os inquiridos deixam nos *sites* que acedem

Resposta	Frequência	Percentagem (%)
Nunca, em caso algum	38	34,2
Só nos que entendo serem fidedignos	69	62,2
Só nos questionários de passatempos	1	0,9
Sim, sempre que são solicitados	0	0
Outro	3	2,7

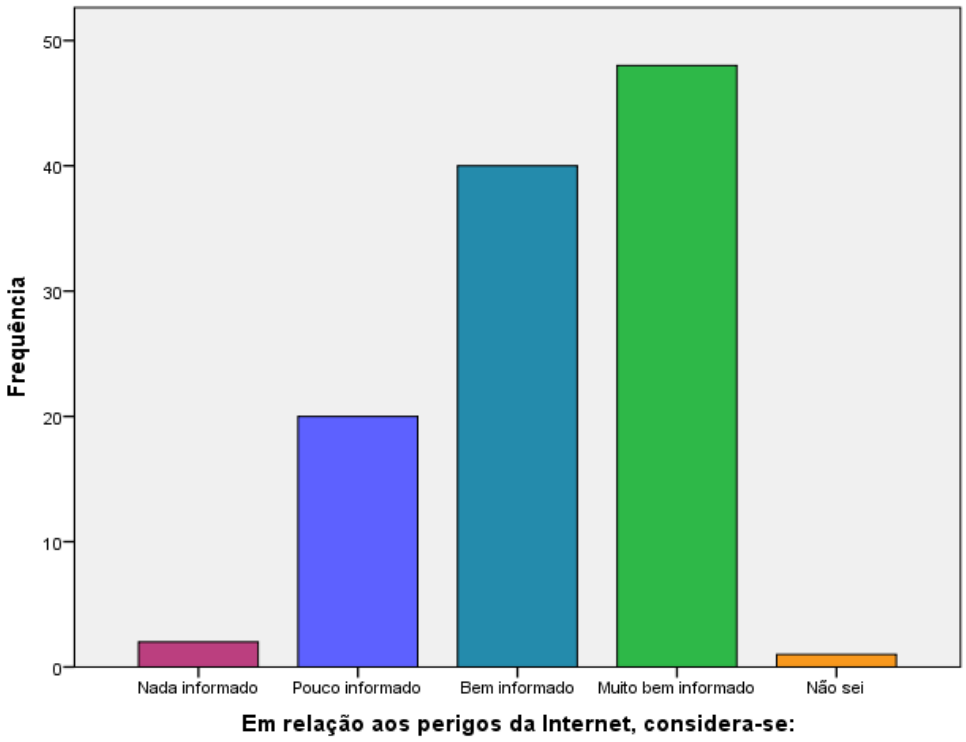
Na afirmação «Na sua opinião, julga que se encontra seguro na *Internet*?» as respostas divergem entre si, não chegando a uma resposta única com uma maioria esmagadora de respostas (como acontece em algumas questões). Apenas 4,5% respostas afirmam que concordam totalmente com esta afirmação, enquanto que, as restantes respostas divergem em concordo em parte (28,83%), não concordo nem discordo (22,52%), discordo em parte (25,23%) e discordo totalmente (18,92%).

Gráfico 6.23: Gráfico de barras, de frequência, acerca da afirmação «Na sua opinião, julga que se encontra seguro na *Internet*?»



Relativamente aos perigos existentes na *Internet*, já existe um consenso de respostas entre os inquiridos considerarem-se bem informados (36,04%) e muito bem informados (43,24%).

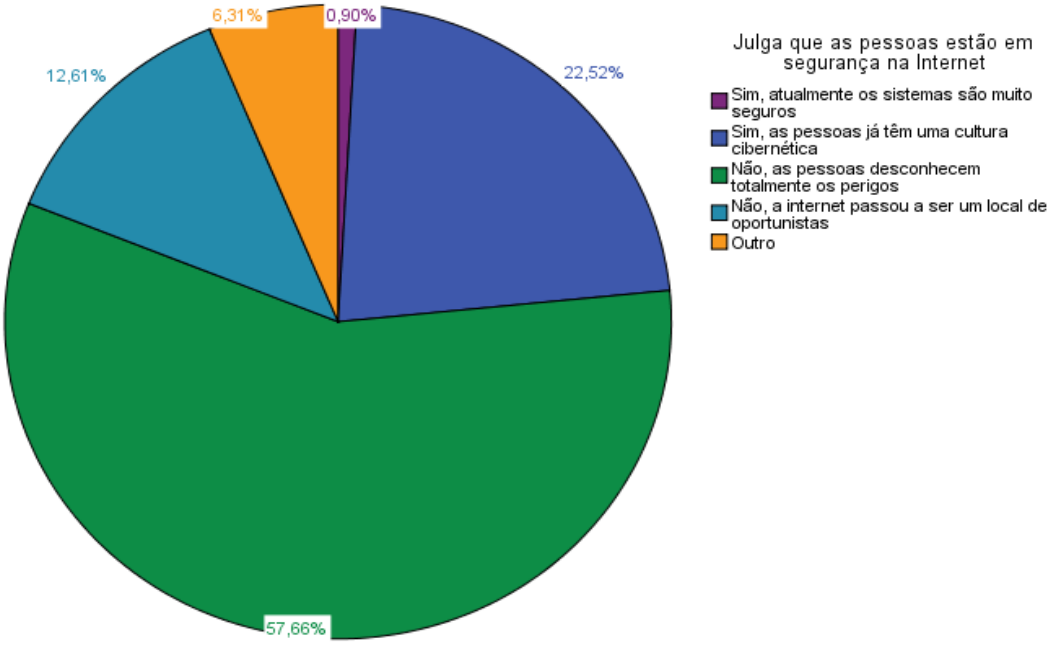
Gráfico 6.24: Gráfico de barras, de frequência, sobre como os inquiridos se consideram informados acerca dos perigos da *Internet*



Em relação à opinião dos inquiridos quanto à segurança das pessoas na *Internet*, 64 respostas declaram que as pessoas não estão seguras porque desconhecem totalmente os perigos existentes no mundo digital, enquanto que, 25 respostas afirmam o contrário – as pessoas estão seguras porque já têm um cultura cibernética.

Nas sete respostas dadas em «Outro», no geral, afirmam que a *Internet* não é um local seguro, que algumas pessoas conhecem ou estão informadas sobre os perigos existentes mas outras não o estão.

Gráfico 6.25: Gráfico de pizza, em percentagem, sobre a opinião dos inquiridos em relação se em geral as pessoas estão em segurança na *Internet*



6.5 Privacidade, Proteção e Segurança na Internet

Esta parte do inquérito iniciou com a questão se o utilizador usava complementos de segurança disponibilizados pelo (s) *browser* (s) que utiliza para navegar na *Internet*.

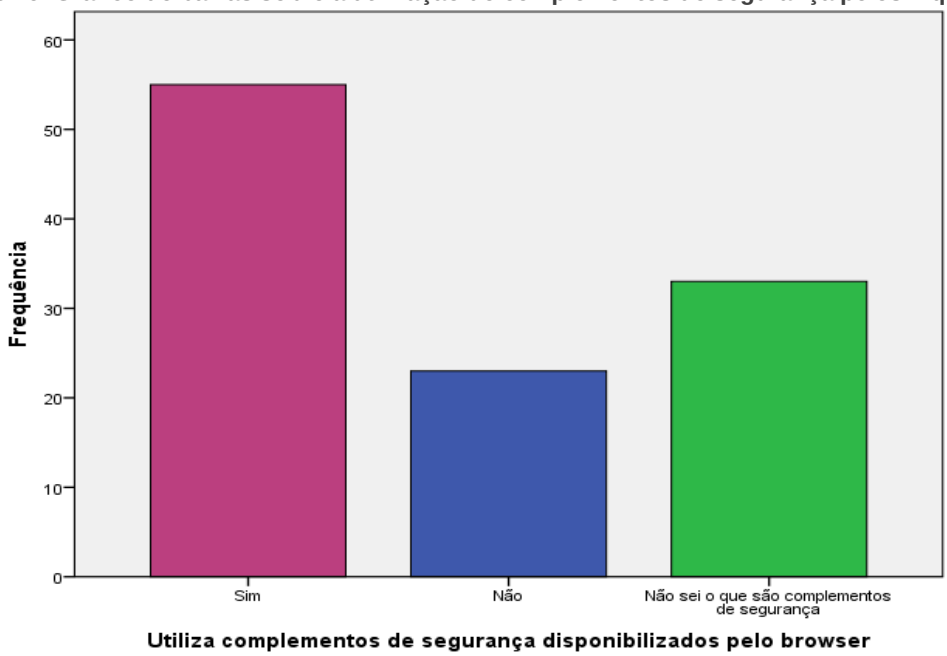
As respostas, como se pode observar pelo **Gráfico 6.26**, cerca de 50% das respostas utilizam complementos de segurança contra, aproximadamente, 21% que não utilizam. Contudo, cerca de 30% não sabe o que são complementos de segurança que são disponibilizados pelos *browsers*.

Do ponto de vista da segurança de um computador, este não necessita apenas um antivírus e um *anti-spyware/anti-malware* para se proteger de vírus, *worms*, entre outros, até porque tem vindo a ser confirmado por vários estudos que a entrada de programas maliciosos nos computadores é através do *browser*. Como tal, é essencial ter imenso cuidado com esses programas no *browser*, uma vez que através deste acedemos a vários serviços, podendo gerar imensos prejuízos, como por exemplo, acesso ao *homebanking* se formos um utilizador que guarde os acessos no *browser* para futuramente não ter de voltar a inseri-los. Assim, os *browsers* de forma a proteger os seus utilizadores disponibilizam uma série de extensões ou complementos, gratuitos ou a pagar, de forma a tornar a navegação dos utilizadores mais segura (Daquino, 2010).

Alguns exemplos de extensões ou complementos de segurança gratuitos disponibilizados são: o **Adblock Plus** – permite bloquear a publicidade *online*, bem

como o bloqueio automático de todos os domínios conhecidos de *malware* –, **WOT** – serviço de análise da reputação de *sites*, que ajuda o utilizador a tomar decisão se deve confiar num *site* ou não, quando faz pesquisas, comprar ou navega *online* – e, **HTTPS Everywhere** – altera automaticamente os sites de HTTP para HTTPS, de modo a proteger o utilizador contra diversas formas de espionagem, invasão da privacidade e censura de conteúdos.

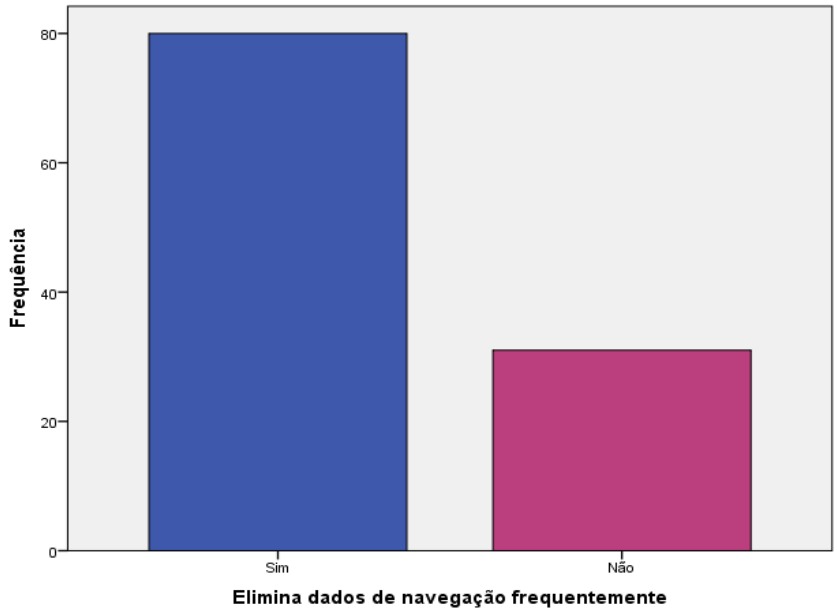
Gráfico 6.26: Gráfico de barras sobre a utilização de complementos de segurança pelos inquiridos



Quando se questionou os inquiridos, se frequentemente eliminam os dados de navegação (histórico, cookies, cache, palavras-passe guardadas e dados de preenchimento automático) as respostas foram afirmativas em cerca de 72%.

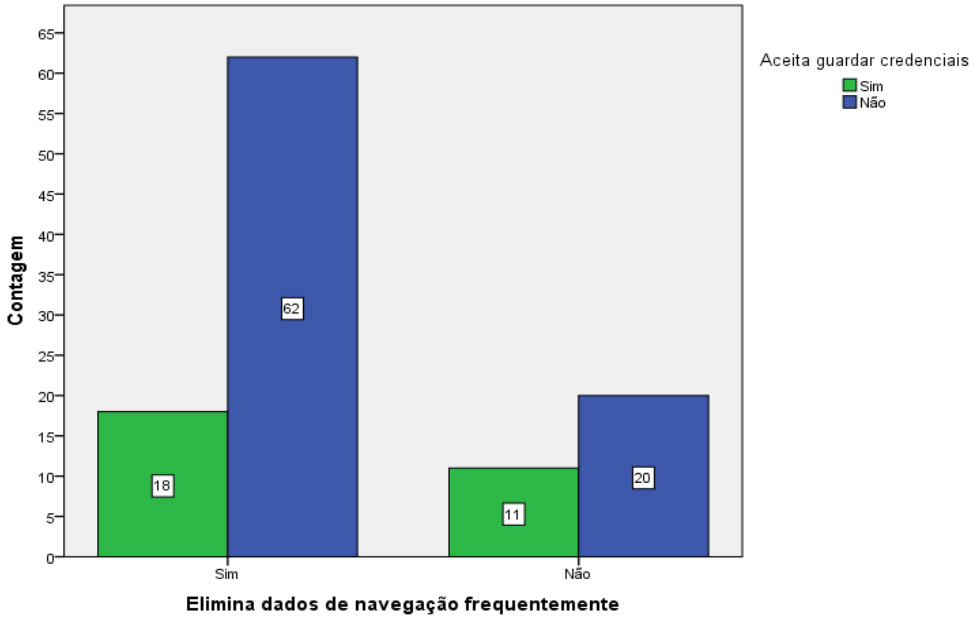
Com o mesmo intuito de perceber em que medida os utilizadores teriam os seus dados seguros em caso de o seu *browser* ser "atacado" por algum programa malicioso, questionou-se os mesmos se ao acederem a uma página/*site* em que é necessário autenticação (por exemplo, a conta de *e-mail*) e o *browser* coloca a questão se pretende guardar as credenciais (nome de utilizador e palavra-passe) para que da próxima vez que tentasse aceder não fosse necessário voltar a colocar, a resposta de 82 inquiridos foi que não autorizavam que o *browser* guardasse as suas credenciais. Porém, 31 inquiridos responderam que autorizam que guardasse as credenciais.

Gráfico 6.27: Gráfico de barras, em frequência, ilustrativo da questão colocada aos inquiridos, se estes eliminavam frequentemente os dados de navegação



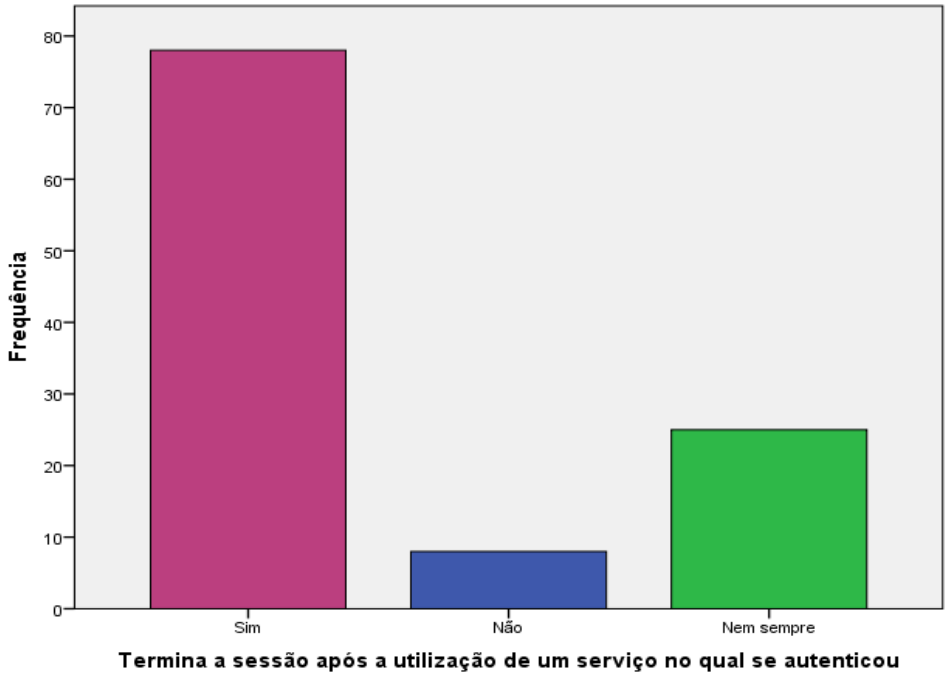
Comparando estas duas variáveis (elimina frequentemente os dados de navegação e aceita guardar as credenciais), como demonstra o **Gráfico 6.28**, podemos concluir que cerca de 56% das pessoas responderam que eliminavam frequentemente os dados de navegação e não aceitavam que o *browser* guardasse as suas credenciais. Ainda podemos denotar que, apesar de ser uma minoria, quase 10% da nossa amostra não faz frequentemente uma limpeza dos dados de navegação e aceita que as suas credenciais sejam guardadas pelo *browser*.

Gráfico 6.28: Gráfico de barras, em Cluster, comparativo da resposta dada sobre a eliminação dos dados de navegação e a aceitação das credenciais serem guardadas pelo *browser*



No continuar, do mesmo assunto, colocou-se, aos inquiridos, a questão se após entrarem num serviço, por autenticação, se terminavam a sessão após a utilização desse serviço. Favoravelmente obteve-se, na maioria, 78 respostas afirmativas e apenas oito respostas em que não terminavam a sessão do serviço.

Gráfico 6.29: Gráfico de barras referente à questão «Termina a sessão após a utilização de um serviço no qual se autenticou?»



Por, atualmente, vivermos num mundo quase todo ele informatizado, colocou-se a questão se os utilizadores utilizam o *homebanking*, obtendo-se aproximadamente 50% de respostas (56) que declaram que usam.

Mediante a resposta afirmativa a esta resposta, ou seja, a amostra passou a ser de 56 respostas, o inquirido teria duas perguntas extras para responder: se utilizava este serviço em computadores públicos e se usava conectado em redes *Wi-Fi* abertas/públicas.

Em relação à primeira questão extra, as respostas foram 55 respostas em que os inquiridos não utilizavam computadores públicos no acesso ao *homebanking*. Em relação à segunda pergunta extra, obteve-se 48 respostas que não utilizavam este serviço ligados a redes *Wi-Fi* abertas/públicas.

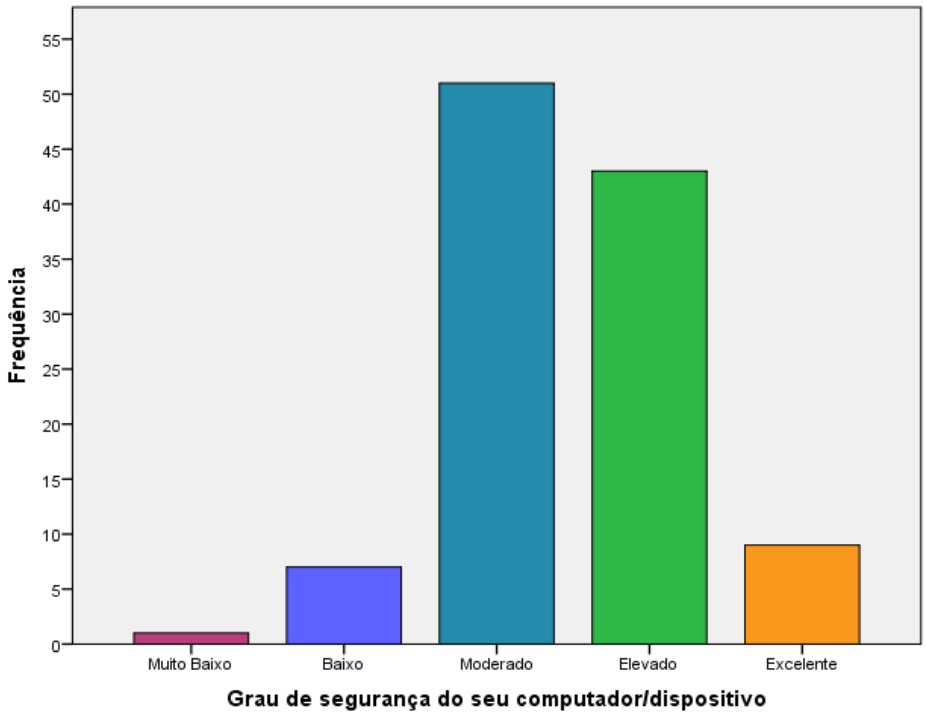
Perante estes resultados, pode-se verificar que existe uma consciencialização das pessoas para as medidas “básicas” de segurança para estes serviços. Contudo, nunca é demais enunciar algumas medidas preventivas a ter em atenção quando se acede ao serviço de *homebanking*.

As medidas de prevenção mencionadas pelo Dr. Jorge Lordello são (Lordello, n.d.):

1. Procurar ler as orientações de segurança do seu banco para a utilização do banco eletrónico;
2. Sempre que entrar no *site* do banco, digitar primeiro uma senha errada. Ao aparecer uma mensagem de erro significa que o *site* é mesmo o banco, por verificar a veracidade da senha colocada, senão pode estar diante de uma página pirata ou clonada;
3. Se a página do banco apresentar um "teclado virtual", tente minimizá-lo. Se o teclado ficar sempre fixo, não minimizar, o utilizador teve o seu computador invadido por *hackers*;
4. Sempre que entrar no *site* do banco, verifique na caixa de introdução do endereço do site aparece um ícone na forma de um cadeado. Clique uma vez com o rato sobre esse ícone, se o *site* for autêntico, aparecerá uma pequena janela com informações sobre a sua autenticidade. Nos *sites* clonados, o cadeado pode aparecer mas ao clicar sobre ele, nada acontecerá;
5. O computador mais seguro para a utilização do *homebanking* não é o da empresa em que trabalha, mas sim o de sua casa, devido a poucas pessoas terem acesso ao mesmo;
6. Alterar a palavra-passe bancária constantemente, pois quem mantém a mesma senha está propenso a mais riscos;
7. Nunca aceda ao banco eletrónico em computadores públicos ou computadores de amigos ou redes de *Wi-Fi* públicas de restaurantes ou cibercafés;
8. Se o seu computador teve algum problema (por exemplo, estar lento ou contaminação por vírus), não se esqueça que o conserto do mesmo deve ser realizado por um técnico de confiança, uma vez que ele terá acesso a todo o conteúdo do seu computador;
9. Quando receber o computador arranjado troque, imediatamente, todas as palavras-passe, em particular, das suas contas bancárias.

Após estas questões, foi pedido ao utilizador que classificasse o grau de segurança do dispositivo que utilizava, obtendo-se no total uma classificação de moderado-elevado.

Gráfico 6.30: Gráfico de barras referente à classificação que os inquiridos davam à segurança do seu computador/dispositivo

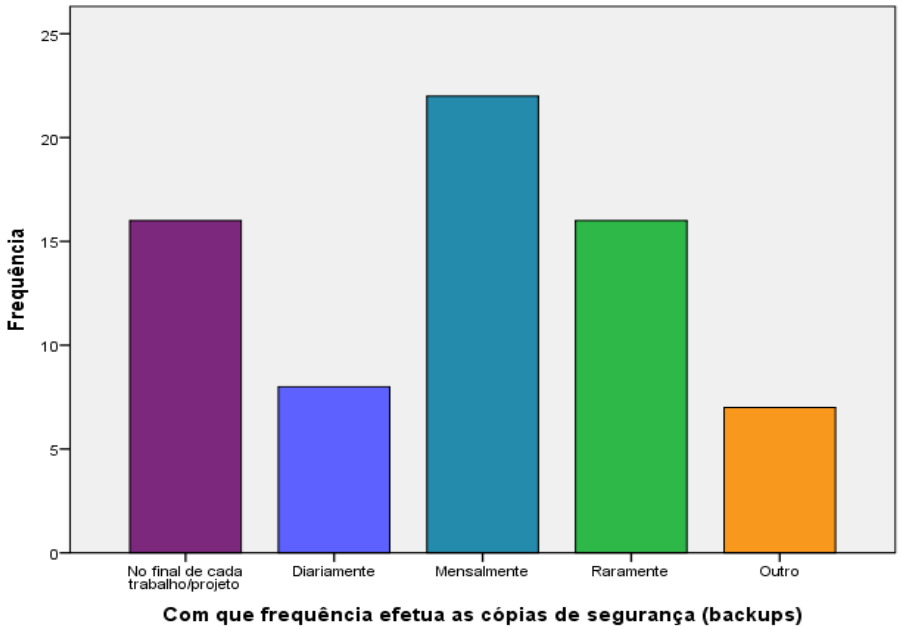


Por último nesta parte do inquérito, não menos importante, questionou-se as pessoas se realizavam cópias de segurança (*backups*) do que continham no seu computador/dispositivo. As respostas foram 69 pessoas dizendo que sim e 42 que não.

Deste modo, tentou-se saber mais em que medida estas 69 pessoas faziam estas cópias de segurança, por outras palavras, saber a periodicidade com que as faziam e que dispositivos de armazenamento utilizavam.

Em relação à frequência que os inquiridos efetuam os *backups*, na sua generalidade, é mensalmente (31,88%). Particularizando a resposta «Outro» podemos denotar pelas respostas dadas que são efetuadas semanalmente ou semestralmente ou sempre que o utilizador reconheça que tem informação importante que deve ser armazenada.

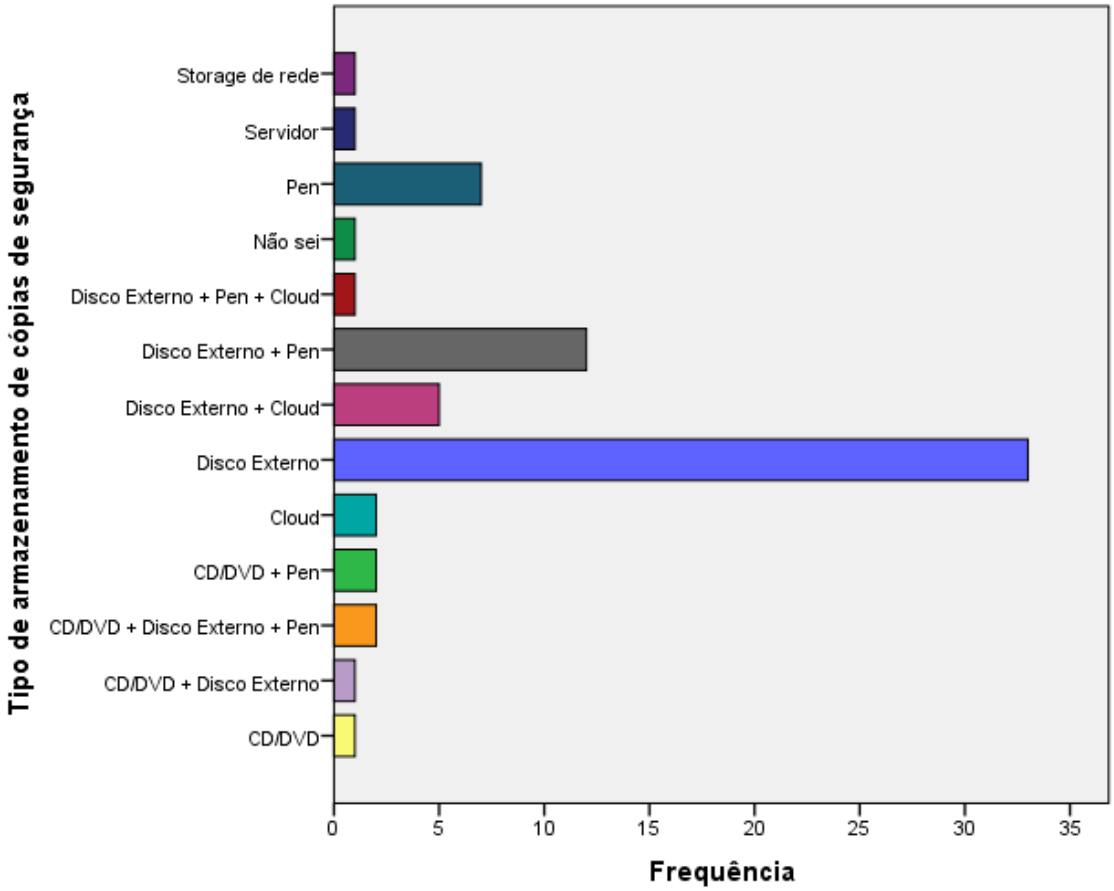
Gráfico 6.31: Gráfico de barras demonstrativo das frequência com que os inquiridos efetuam as cópias de segurança



A última pergunta referente ao tipo de dispositivo utilizado para o armazenamento dos *backups* foi uma pergunta de múltipla escolha, pelo que, de modo generalizado, a maioria (54 respostas) utilizava o disco externo para guardar as cópias de segurança.

Particularizando as respostas, como podemos ver pelo **Gráfico 6.32**, aproximadamente, 48% dos inquiridos realmente utiliza o disco externo para guardar os *backups* porém, também utilizam em conjunto com o disco externo a *Pen* com 17,4%. Outra particularidade a ressalvar é a utilização da *Cloud* por oito pessoas, em conjunto com outros dispositivos ou como único dispositivo.

Gráfico 6.32: Gráfico de barras demonstrativo do tipo de dispositivos utilizados pelos inquiridos para armazenar os seus *backups*



6.6 Passwords

Esta parte do inquérito é fundamental para perceber em que medida os utilizadores da *Internet* têm noção de como deve ser constituída uma palavra-passe de modo a ser segura. Pois, hoje em dia, temos ouvido bastantes notícias de *hackers* que invadiram empresas ou contas do topo hierárquico de uma empresa de um modo bastante simples e rápido, pois a palavra-passe utilizada era «admin» ou «123456», entre outras.

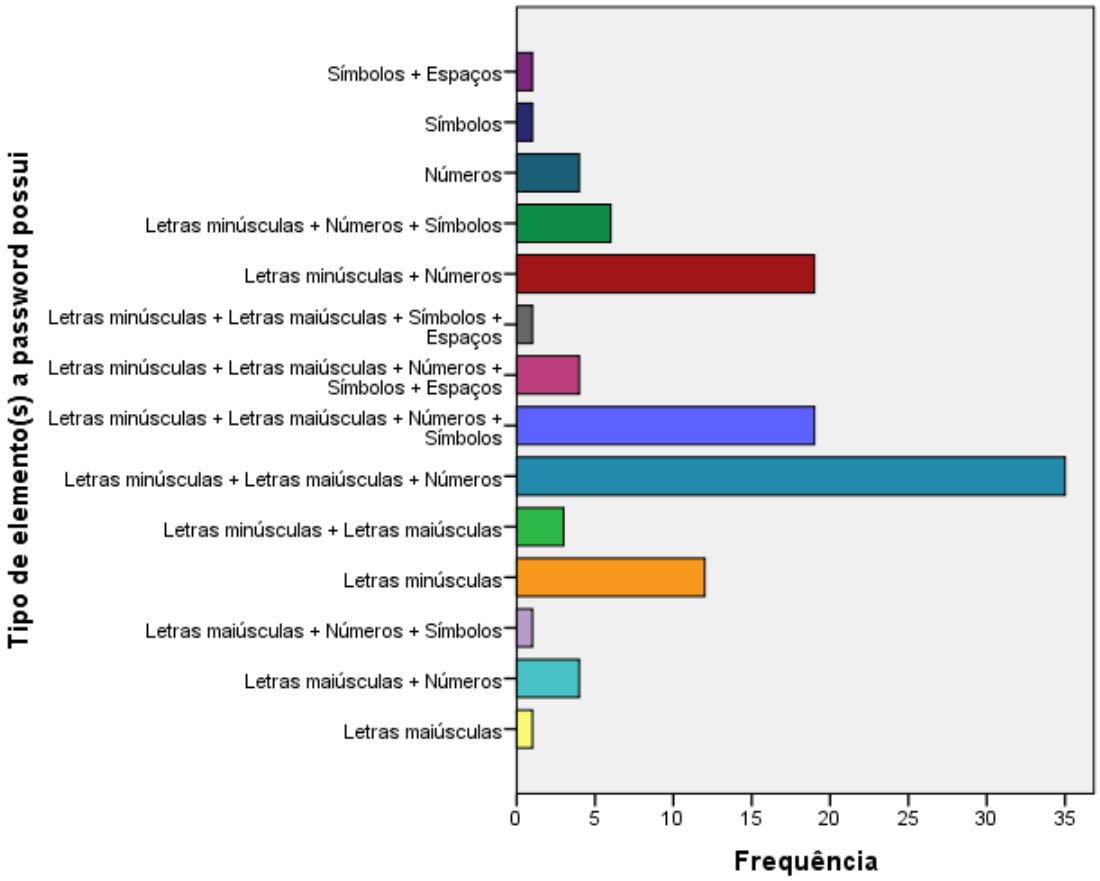
Pela **Tabela 6.11**, podemos verificar que esta amostra de 111 pessoas contém na sua maioria (52) palavras-passe com cerca de 10 a 13 caracteres, por outro lado, temos também muito próximo (46) palavras-passe com 5 a 9 caracteres. Contudo, a quantidade de caracteres não quer dizer nada por si só!

Tabela 6.11: Tabela de frequência e percentagem acerca da quantidade de caracteres que os inquiridos têm nas suas palavras-passe

Resposta	Frequência	Percentagem (%)
5 a 9	46	41,44
10 a 13	52	46,85
14 a 17	12	10,81
Mais de 17	1	0,90

Relativamente aos caracteres que compõem as senhas dos mesmos inquiridos podemos verificar que cerca de 32% utiliza em simultâneo números, letras minúsculas e maiúsculas, e adicionando a estes elementos os símbolos temos 17% das respostas. Contudo, ainda temos utilizadores (17%) que só usam uma mistura de letras minúsculas e números. Ainda, mais grave, temos cerca de 11% que utilizam apenas letras minúsculas.

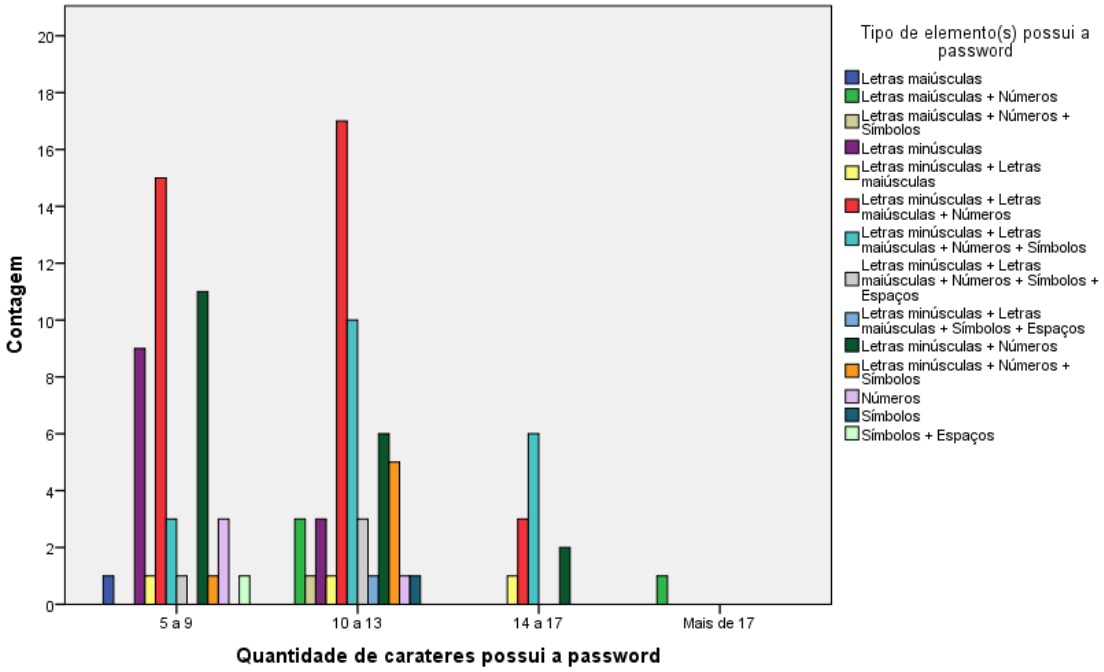
Gráfico 6.33: Gráfico de frequências relativo aos elementos usados em conjunto ou em separado nas palavras-passe de escolha dos inquiridos



Agrupando os tipos de elementos utilizados nas senhas segundo a quantidade de caracteres utilizados nas mesmas podemos denotar que:

- De cinco a nove caracteres, 15 respostas simultaneamente utilizam números, letras minúsculas e maiúsculas;
- Dentro da mesma variável, 11 respostas só utilizam na mesma palavra-passe letras minúsculas e números;
- De dez a treze caracteres, globalmente, têm consciência da utilização de vários tipos de elementos simultaneamente;
- De 14 a 17 caracteres, a maioria (seis inquiridos) utiliza concomitantemente números, símbolos, letras minúsculas e maiúsculas;
- Nas palavras-passe com mais de 17 caracteres contêm apenas letras maiúsculas e números.

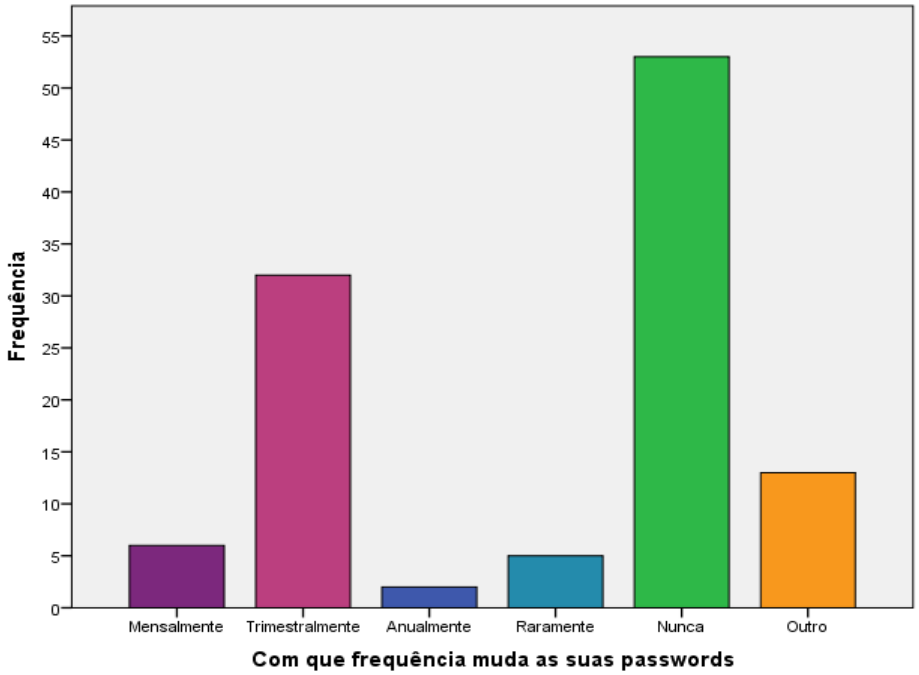
Gráfico 6.34: Gráfico da quantidade de caracteres em função do tipo de elemento (s) que as palavras-passe dos inquiridos contêm



As respostas quanto à seguinte questão («Possui passwords iguais em serviços diferentes?») 64 respostas foram afirmativas, 19 responderam que não e 28 que dependia. Com esta resposta verificamos que cerca de 58% da amostra contém palavras-passe iguais em serviços distintos, encontrando-se em risco caso em algum destes serviços a sua senha for exposta, pois o "atacante" poderá ter acesso a outros serviços.

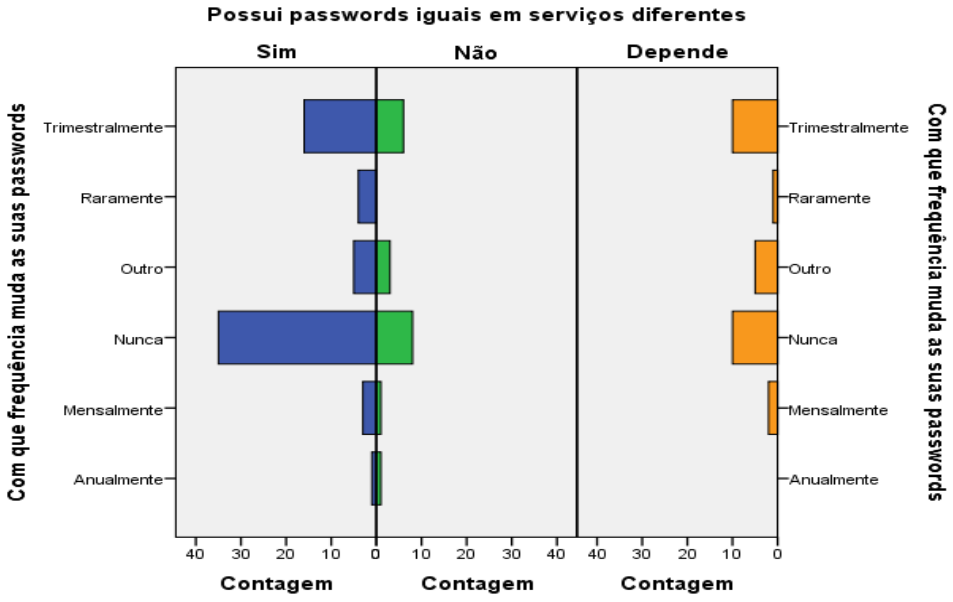
A seguinte questão colocada obteve alguns resultados preocupantes, visto que num primeiro realce, 53 respostas afirmam que nunca alteram a sua palavra-passe.

Gráfico 6.35: Gráfico da frequência que os inquiridos alteram as palavras-passe dos serviços que utilizam



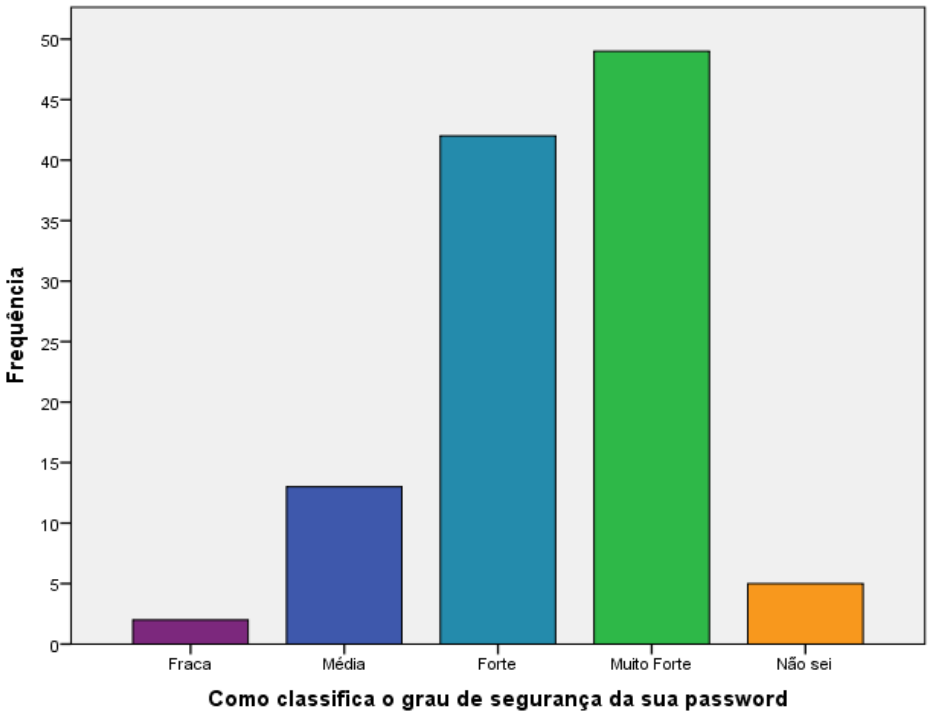
Indo ao encontro da preocupação demonstrada anteriormente, pelo seguinte gráfico, podemos denotar que de facto temos uma quantidade considerável de 35 pessoas que nunca alteram as suas palavras-passe e utilizam a mesma em serviços distintos.

Gráfico 6.36: Gráfico de barras, em Cluster, acerca dos inquiridos possuírem palavras-passe iguais em serviços diferentes em função da frequência com que alteram as mesmas



No **Gráfico 6.37**, podemos verificar como os inquiridos classificam as suas senhas, sendo que, de modo geral, classificam-nas como fortes ou muito fortes.

Gráfico 6.37: Gráfico ilustrativo de como os inquiridos classificam as suas senhas



Por fim, em relação ao método utilizado para guardar as palavras-passe, 91% dos inquiridos, e muito bem, utiliza a memorização como principal método. Mas, ressalvando que em duas respostas «Outro» afirmam que utilizam a encriptação como método para as guardar, ou seja, a utilização de ficheiros encriptados onde contêm as suas palavras-passe.

6.7 Criminalidade Informática

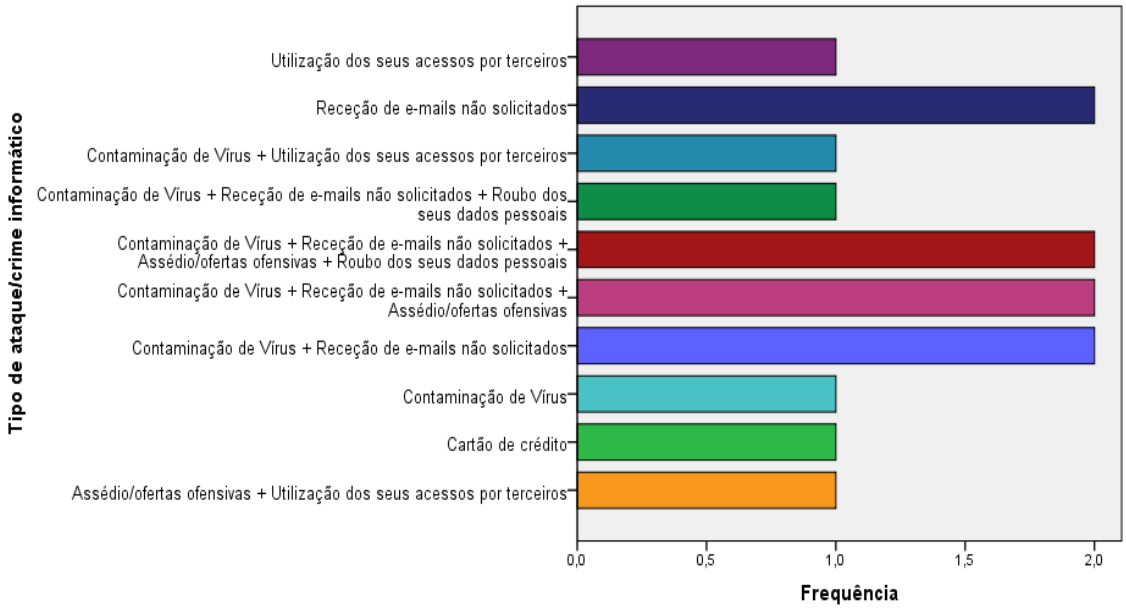
Nesta penúltima parte do inquérito, procura-se saber se os inquiridos estão a par da legislação portuguesa quanto aos crimes informáticos, bem como se foram vítimas ou se conhecem alguém que já foi vítima de ataques ou crimes informáticos. Ainda, se tenciona saber se os inquiridos acreditam no sistema judicial.

Assim, a primeira questão a ser colocada foi se alguma vez foi vítima de um crime ou ataque informático. Felizmente, só cerca de 13% da amostra afirmou que já foi vítima de um crime ou ataque informático.

Assim, as próximas questões colocadas foram apenas para as 14 pessoas que disseram que já foram vítimas.

Na questão sobre que tipo de crime ou ataque sofreu, o inquirido poderia escolher mais do que uma opção como pode ser demonstrado pelo **Gráfico 6.38**. Mas, de um modo geral, a contaminação de vírus e a receção de *e-mails* não solicitados foram a resposta mais selecionada.

Gráfico 6.38: Gráfico descritivo das respostas dadas pelos inquiridos à questão «Que tipo de crime (s)/ataque(s) sofreu?»



Quanto se face ao crime/ataque sofrido apresentou queixa às autoridades competentes, apenas um inquirido declarou que apresentou.

Deste modo, relativamente à questão colocada «Obteve resultados satisfatórios com a queixa feita às autoridades?» a resposta dada pelo inquirido que apresentou queixa não foi a melhor pois o resultado não foi satisfatório para o inquirido, uma vez que o caso foi arquivado.

Em relação à amostra que respondeu na primeira questão que não tinha sido vítima de algum tipo de crime ou ataque informático foram colocadas duas questões: «Algum familiar ou conhecido seu já foi vítima de um crime informático?» e «Se fosse vítima de fraude informática ou de crime informático faria queixa às autoridades competentes?».

Na primeira questão, a maioria (75 inquiridos) não tem qualquer familiar ou conhecido que tenha sofrido deste tipo de crime, por outro lado, 22 inquiridos têm familiares ou conhecidos que já sofreram.

Quanto à segunda pergunta, cerca de 72% afirma que apresentaria queixa às autoridades competentes e 23 inquiridos responderam que talvez o fizessem. Contudo, há que ressalvar que dois inquiridos responderam que não apresentavam queixa e outros dois inquiridos responderam que não valia a pena apresentar queixa.

Nas cinco questões do inquérito, colocadas aos 111 inquiridos, podemos de um modo geral afirmar que à medida que se começa a perguntar mais especificamente de alguns tipo de crimes/ataques informáticos, o número de inquiridos que sabe o que é cada um começa a diminuir e, consequentemente, aumenta o número de inquiridos que não sabem o que é ou, então, nunca ouviram falar.

Tabela 6.12: Tabela de frequência e percentagem acerca das questões colocadas sobre o conhecimento dos inquiridos quanto aos esquemas de *phishing, keylogger, clickjacking, rootkit* e o esquema da Nigéria

Sabe o que é	Sim	Não	Nunca ouvi falar
Esquemas de *phishing*	67 (60,36%)	23 (20,72%)	21 (18,92%)
Keylogger	44 (39,64%)	32 (28,83%)	35 (31,53%)
Clickjacking	35 (31,53%)	40 (36,04%)	36 (32,43%)
Rootkit	22 (19,82%)	44 (39,64%)	45 (40,54%)
Esquema da Nigéria	21 (18,92%)	43 (38,74%)	47 (42,34%)

Finalmente, após todas as questões colocadas, a última parte do questionário era facultativa e o inquirido poderia deixar algum comentário ou sugestão.

Os comentários/sugestões deixados foram de quatro inquiridos, em geral, a agradecer o inquérito devido a ter servido para procurarem informação sobre os assuntos abordados e a desejar um bom trabalho. Uma sugestão colocada por um dos comentários era de no final do questionário colocar um esclarecimento acerca da última matéria abordada por este. Por último, um outro comentário teve a ver com a pergunta colocada acerca da utilização de ferramentas de proteção em que este inquirido respondeu que não utilizava antivírus e como tal no final explicou o porquê de não usar: “Não uso antivírus pelo facto de o meu conhecimento na área da segurança digital ser grande mas penso que hoje em dia e muito fácil contornar qualquer situação usando a engenharia social e assim aceder aos dados de alguém informaticamente.” E, em relação ao *phishing*, o mesmo explicou que o facto de este método de criminalidade ser “bom”, não era o aspeto em si da página mas a engenharia social que era utilizada por detrás.

7 CONSIDERAÇÕES FINAIS

A cada dia que passa, a tecnologia evolui, quer a nível de *hardware* (equipamentos) quer a nível de *software* (nova versão do sistema operativo), e nós aceitamos cada versão mais rápido que a anterior, vivendo dependente desta nova tecnologia.

A *Internet*, originalmente, foi criada com o propósito de manter as comunicações, independentemente de qualquer ataque físico de um inimigo. Portanto, esta foi criada sem ter como ideia primária a segurança deste espaço de comunicação.

Naturalmente a evolução da tecnologia, bem como a própria *Internet* em si, trouxe consigo diversas vantagens mas também desvantagens. Como vantagens podemos enumerar a comunicação entre as pessoas de todo o mundo, partilhar informações, através da *Internet*, tornando mais rápido a troca de informações. Como desvantagens temos a dependência ou mesmo vício que foi criado da necessidade de querermos o último equipamento lançado (por exemplo, *smartphone*) ou até mesmo de querermos a última aplicação lançada (por exemplo, o jogo do Pokémon Go), e a falta de privacidade, uma vez que muitas pessoas ficam expostas e tornam-se vítimas de diversos golpes ou crimes. Esta falta de privacidade acontece pela falta de conhecimento dos utilizadores acerca da *Internet*, em particular das redes sociais.

A questão das redes sociais prende-se pelo que publicamos... milhares de milhões de Gigabytes de momentos/desejos armazenados em servidores, podendo-se mesmo dizer que estes servidores contêm grandes histórias armazenadas digitalmente. E como sabemos uma foto ou outro qualquer dado não pode ser facilmente eliminado após ser publicado na *Internet*, uma vez que mesmo que eliminemos do nosso perfil, esta pode ter sido guardada por outra pessoa que colocou noutro site e assim sucessivamente.

Assim deixámos de ter privacidade virtualmente. Estas informações (por exemplo, através de uma foto e/ou dos seus metadados) podem ser usadas por qualquer pessoa e podem ser utilizadas quer para o “bem” quer para o “mal”. Deste modo, o impacto que determinadas informações têm ao “cair” em mãos erradas pode prejudicar a segurança nacional.

Desde sempre houve crimes, mas com a *Internet*, houve o acrescentar da tecnologia aos crimes já tipificados na lei, por exemplo, a burla informática, e houve a criação de novos tipos de crimes, por exemplo, sabotagem informática. Deste modo, o direito penal teve e deve continuar a sofrer diversas alterações, na medida em que todos os dias os criminosos tentam explorar novas oportunidades para praticar os crimes.

Assim, é necessário entrar no campo da prevenção e "combate" destes crimes, construindo legislação, tipificando os mesmos, e criando medidas de segurança.

A realidade portuguesa não é muito diferente da realidade mundial, pois como se pode observar no RASI, o número de participações deste tipo de crime tem sofrido um significativo aumento (73,7% em comparação com o ano anterior).

As estatísticas não refletem fiavelmente acerca da realidade deste fenómeno da criminalidade informática, pois temos de ter em atenção as «cifras negras», ou seja, alguns dos crimes cometidos não são participados/registados às autoridades. Tal "silêncio" deve-se ao facto de muitas empresas pela sua reputação não afirmarem que foram alvo de um ataque informático (para não afetarem a sua credibilidade) ou, muitas vezes, por falta de experiência ou de sensibilização dos utilizadores, estas ameaças não são detetadas. Como podemos reparar nos resultados do inquérito, temos 14 pessoas que sofreram algum ataque ou crime informático, e apenas um é que afirmou que efetuou queixa às autoridades competentes, ressalvando também que algumas das pessoas que responderam que não tinham sido vítimas de algum crime ou ataque informático, já o podem ter sido mas nunca descobriram.

Portugal encontra-se num bom caminho no que diz respeito à punição do cibercrime, porém ainda há muito a fazer, em especial, quanto à obtenção da prova, uma vez que os dados de tráfego são incluídos na proteção de dados pessoais e ao fim de, aproximadamente, um ano as empresas não guardam mais esses dados, o que, por conseguinte, dificulta a investigação deste tipo de crimes.

Apesar de todos os riscos e perigos existentes na *Internet*, por muito que nos questionemos se realmente necessitamos desta, a resposta é afirmativa.

Por isso pode-se dizer, que viver sem a *Internet* é um facto impensável, devido a existirem serviços que apenas se encontram disponíveis no meio digital ou que só podem ser utilizados acedendo à *Internet*, por exemplo, os juristas e os contabilistas precisam do acesso à *Internet* para consultar os processos ou entregar documentos, entre outros serviços, pois estes apenas existem *online*. Particularizando, a nível pessoal, torna-se muito mais fácil aceder à conta bancária, entregar impostos, conversar, gratuitamente, com os amigos e familiares do outro lado do globo, entre outras possibilidades, tudo sem sair de casa ou em qualquer lugar, com acesso à *Internet*.

Com este facto, a segurança passa a ser imprescindível no mundo digital! Assim, o Estado deve assegurar que os utilizadores da *Internet* estão seguros, pois esta já faz parte do dia-a-dia dos cidadãos, bem como das entidades públicas e privadas.

Portanto, cabe à segurança interna conhecer as ameaças que advêm do mundo virtual, bem como as intenções, vulnerabilidades e capacidades de um adversário. Todavia, se todos nós, enquanto cidadãos, estivermos instruídos com regras de segurança e as seguirmos, além de proteger os dispositivos eletrónicos e a nós mesmos, num cenário generalizado, estaremos a contribuir para proteger o nosso país de ameaças de cariz informático, pois a segurança do mesmo não diz respeito apenas às infraestruturas críticas.

Podemos então concluir que para protegermos o país devemos num primeiro plano nos proteger a nós próprios! Muitas vezes deixamos de estar seguros digitalmente devido a algo que se publica na *Internet*, ou em particular nas redes sociais.

> *"A Segurança não é um sentimento, é um estado que se atinge pela adoção de medidas que permitam a consciente aceitação do risco" (Sobral, 2010).*

Não podemos negar a crescente ameaça dos ataques informáticos a diversas entidades governamentais e que estes ataques são sofisticados, contudo podemos denotar que estes ataques têm por base o mesmo tipo de ataque (negação de serviço) e que ao se estudar esses ataques podemos proteger o país de ataques semelhantes.

A *Internet* relacionando-se com a segurança interna permitiu que conflitos analisados, anteriormente, no terreno fossem tratados no ciberespaço, tendo uma maior relevância, uma vez que são utilizados para propaganda, espionagem, negação de serviços ou até mesmo a destruição de infraestruturas vitais. (Caldas & Freire, 2013).

Em geral, não existem sistemas de informação que sejam 100% seguros, nem existem soluções que acabem com todas as ameaças e vulnerabilidades existentes num sistema, mas podemos torná-los mais seguros, na medida em que estes ataques são perpetrados, na sua maioria, por pessoas ou grupos que tencionam obter benefício, prejudicar alguém ou apenas chamar à atenção.

Assim, o Estado tem de prevenir estas ameaças, através da cibersegurança e da ciberdefesa, por outras palavras proteger as redes e sistemas informáticos, os dados que neles circulam, bem como monitorizar, prevenir e dar respostas a ameaças que coloquem em causa a soberania do Estado.

De modo a colmatar as possíveis falhas existentes a nível da segurança informática no nosso país foram criadas medidas de segurança e uma estratégia de cibersegurança, em conformidade com o Centro Nacional de Cibersegurança e as entidades que detêm esta responsabilidade.

Com o estudo realizado através da resposta de um inquérito *online* pretendemos analisar se os cidadãos conhecem os perigos que a *Internet* acarreta e se, por conseguinte, se sabem proteger ou prevenir destes perigos.

De modo geral, podemos verificar que, na sua maioria, os inquiridos deste estudo são pessoas do sexo feminino, em média com 30 anos, licenciados, empregados e residentes no distrito do Porto. A amostragem encontra-se bem caraterizada para o estudo, uma vez que a sua maioria acede à *Internet* todos os dias.

Na questão da segurança informática e, por conseguinte, a privacidade, temos respostas discrepantes, isto é, metade dos inquiridos conhecem os perigos e sabem como se proteger e as ferramentas a utilizar, enquanto a outra metade é divida entre os que não se protegem e os que não conhecem as ferramentas de proteção existentes.

Uma outra questão preocupante é a nível da palavra-passe utilizada, cada vez mais ouvimos que um sistema informático imensamente seguro foi invadido através do acesso de uma palavra-chave, pois esta era simples e fácil de ser descoberta (conter poucos tipos de elementos e ter referências pessoais ou ser "ridícula", como por exemplo «admin» ou «12345»). O mesmo se pode verificar na análise da secção das «*Passwords*» do inquérito, em que os inquiridos não têm uma conjugação de tipos de elementos (letras maiúsculas e minúsculas, números, símbolos e espaços) na criação da sua palavra-passe e utilizam a mesma em diferentes serviços. E, voltando a referir o caso do *hacker* escocês, Gary Mckinnon, podemos verificar a facilidade com que se pode aceder a um sistema fazendo apenas "correr" as palavras-passe mais utilizadas e que nunca foram modificadas.

Assim, podemos observar que na amostragem do inquérito realizado, uma grande parte das pessoas se encontravam informadas sobre os perigos e sabiam como se prevenir, contudo, ainda há muito a fazer e muitas pessoas a sensibilizar, em especial, quanto à palavra-passe e à criminalidade informática.

Em suma, podemos constatar que a segurança informática e a segurança interna estão relacionadas e são fulcrais para a soberania do Estado.

REFERÊNCIAS BIBLIOGRÁFICAS

Livros e Capítulos de Livros

Almedina. (2016). *Código Penal* (6ª). Almedina.

Clark, S. H. A. (2003). *Aprender + Pcs*. (A. Faria, Trad.). Lisboa: McGraw-Hill.

Fernandes, L. F. (2014b). *Intelligence e Segurança Interna*. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

Marques, A. E. (2009). *Internet* (2ª). Centro Atlântico, Lda.

Martins, J. C. (2015). Capacitar, Mitigar, Detetar, Sensibilizar, Educar e Cooperar. Em A. Moreira, A. D. Ramos, C. M. Sarmento, H. J. de Matos, J. Portugal, J. C. Martins, … R. Duque, *Liberdade e Segurança*. Lisboa: ICPOL-ISCPSI.

Matos, H. (2010). O Sistema de Segurança Interna: O Caso Português. Em Adriano Moreira & J. P. Ramalho (Eds.), *Estratégia* (Vol. XIX, pp. 173–246). Lisboa: Instituto Português da Conjuntura Estratégica.

Matos, H. (2016). Sistemas de Segurança Interna: Terrorismo & Contraterrorismo. Casal de Cambra: Caleidoscópio.

Nunes, P. F. V. (2016). Ciberameaças e Quadro Legal dos Conflitos no Ciberespaço. Em J. V. Borges & T. F. Rodrigues (Eds.), *Ameaças e Riscos Transnacionais no novo Mundo Global*. Lisboa: Fronteira do Caos Editores Lda.

Portugal, J. (2015b). A Internet Industrial e os novos riscos: Regresso ao futuro. Em A. Moreira, A. D. Ramos, C. M. Sarmento, H. J. de Matos, J. Portugal, J. C. Martins, … R. Duque, *Liberdade e Segurança*. Lisboa: ICPOL-ISCPSI.

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

Santos, P., Bessa, R., & Pimentel, C. (2008). *Cyberwar - O Fenómeno, as Tecnologias e os Actores*. FCA - Editora de Informática.

Tanenbaum, A. S., & Wetherall, D. (2011). *Computer networks* (5ª ed.). Boston: Pearson Prentice Hall.

Tzu, S. (1993). *A Arte da Guerra* (2ª ed.). Publicações Europa-América.

Verdelho, P., Bravo, R., & Rocha, M. L. (2003). *Leis do Cibercrime* (Vol. 1). Portugal: Centro Atlântico, Lda.

Publicações científicas

Caldas, A., & Freire, V. (2013). Cibersegurança: das Preocupações à Ação. IDN. Obtido de http://www.idn.gov.pt/conteudos/documentos/Working_Paper_2_Ciberseguranca_Versao_final.pdf

Dias, V. M. (2012). A Problemática da Investigação do Cibercrime. *Data Venia*, (1), 63-88.

Howard, J. D., & Longstaff, T. A. (1998). A common language for computer security incidents. *Sandia National Laboratories*. Obtido de http://cyberunited.com/wp-content/uploads/2013/03/A-Common-Language-for-Computer-Security-Incidents.pdf

Garcia, F. P. (2006). As ameaças transnacionais e a segurança dos Estados. Subsídios para o seu estudo. *Revista Negócios Estrangeiros*, (9.1), 339–374.

IDN-CESEDEN. (2013). Estratégia da Informação e Segurança no Ciberespaço. *Cadernos dos IDN*, *12*. Obtido de http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf

Martins, F. (2010). Inteligência. *Política Internacional e Segurança*, *3*, 117–146.

Mathias, S. K. (2016). Aspectos da relação entre desenvolvimento, segurança e cooperação. *Relaciones*

Internacionales, *25*(50), 99–118.

Matos, H. (2012). Contraterrorismo Ofensivo. O «targeted killing» na eliminação de alvos terroristas: o caso dos EUA e de Israel. *JANUS.NET e-journal of International Relations*, *3*(2). Obtido de http://observare.ual.pt/janus.net/images/stories/PDF/vol3_n2/pt/pt_vol3_n2_art7.pdf

Natário, R. M. P. (2013). O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço. *Revista Militar*, (2541), 823–858.

Nunda, G. (n.d.). Angola Fortalece e Moderniza o Sistema. *PATRIA*, (3). Obtido de https://issuu.com/pedrobento3/docs/revista_p__tria_final_gabriel-1

Nunes, P. F. V. (2004). Ciberterrorismo: Aspectos de Segurança. *Revista Militar*, (2433). Obtido de https://www.revistamilitar.pt/artigopdf/428

Nunes, P. F. V. (2012). A Definição de uma Estratégia Nacional de Cibersegurança. *Instituto da Defesa Nacional - Revista Nação e Defesa*, (133), 113–127.

Santos, L., Bravo, R., & Nunes, P. V. (2012). Protecção do Ciberespaço: Visão Analítica. Em *Riscos, Segurança e Sustentabilidade* (pp. 163–176). Lisboa: Edições Salamandra. Obtido de http://comum.rcaap.pt/handle/123456789/3578

Souza, G. L. M., & Medeiros, M. de A. (2011). Da cibersegurança à ciberdefesa Americana: a diplomacia da internet como instrumento de proteção e de integração dos estados da OEA. *Proceedings of the 3rd ENABRI 2011 3 Encontro Nacional ABRI 2011*. Obtido de http://www.proceedings.scielo.br/scielo.php?pid=MSC0000000122011000200017&script=sci_arttext&tlng=pt

Valente, M. M. G. (2013). A Segurança (Interna) na Constituição da República Portuguesa de 1976. *Revista Eletrônica AD Judicia*, *1*. Obtido de http://www.oabrs.org.br/arquivos/file_527a3e21b6153.pdf

Apresentações científicas

Alves, P. (2006). *Informática e Tecnologias de Informação - Teoria da Computação*. Aula lecionada no Curso de Proteção Civil.

Azevedo, M. T. de. (2010). *Cibersegurança em sistemas de automação em plantas de tratamento de água.* (text). Escola Politécnica da Universidade de São Paulo, São Paulo. Obtido de http://www.teses.usp.br/teses/disponiveis/3/3142/tde-10012011-121525/

Borges, J. J. B. V. (2010). *A Segurança e Defesa numa perspectiva do contexto regional ibérico: os novos instrumentos de articulação de políticas e estratégias*. I Congresso Nacional de Segurança e Defesa, Lisboa. Obtido de http://icnsd.afceaportugal.pt/conteudo/congresso/ICNSD_2C_texto_pdf_joao_vieira_borges.pdf

Casimiro, S. de V. (2014). *Cibersegurança – Aspetos Legais*. Comunicação oral apresentada na Segurança da Informação e Gestão do Risco na 3a Plataforma, Lisboa. Obtido de http://www.afceaportugal.pt/2014/eventos/12h10-Vieira_de_Almeida__Associados_s.pdf

CNCS. (2015). CERT.PT - Taxonomia. Obtido de http://www.cncs.gov.pt/media/2015/06/Taxonomia_pt.pdf

Correia, F. (2015, Outubro). *Segurança da informação nas organizações*. Apresentado no Mestrado em Segurança da Informação e Direito no Ciberespaço, Lisboa. Obtido de http://www.engenheiros.pt/~rcorreia/seginforg/04-estado_informacao.pdf

Fernandes, L. F. (2014a). *Informações e Segurança*. Aulas lecionadas no Mestrado não Integrado de Ciências Policiais na especialização de Segurança Interna, Lisboa.

Governo de Portugal. (2013). *Conceito Estratégico de Defesa Nacional*. Lisboa: Resolução do Conselho de Ministros. Obtido de http://www.portugal.gov.pt/media/909457/20130405_cedn_publicacao_oficial.pdf

Guimarães, J. R. F. (2013, Março 7). *Desobediência civil eletrônica : o hacktivismo como manifestação política legítima* (Monografia). Universidade de Brasília, Faculdade de Direito, Brasília. Obtido de http://bdm.unb.br/handle/10483/4800

Lee, P. (2009). Oracle Adaptive Access Manager Reference Guide. Oracle and/or its affiliates. Obtido de http://docs.oracle.com/cd/E12057_01/doc.1014/e12054.pdf

MAI. (2015). *Relatório Anual de Segurança Interna 2014*. Portugal. Obtido de http://www.apav.pt/apav_v2/images/pdf/RASI_2014.pdf

MAI. (2016). *Relatório Anual de Segurança Interna 2015*. Portugal. Obtido de http://www.portugal.gov.pt/pt/pm/documentos/20160331-pm-rasi.aspx

Matos, H. (2014). *Sistemas de Segurança Interna*. Aulas lecionadas no Mestrado não Integrado de Ciências Policiais na especialização de Segurança Interna, ISCPSI, Lisboa.

Militão, O. P. (2014). *Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional* (Relatório Científico Final do Trabalho de Investigação Aplicada). Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa, Lisboa. Obtido de https://run.unl.pt/handle/10362/14300

Pimentel, C. (2014). *Notas analíticas sobre o conceito dissuasão aplicado ao fenômeno da Cibersegurança*. Apresentado no IX Encontro da ABCP, Brasília. Obtido de http://www.encontroabcp2014.cienciapolitica.org.br/resources/anais/14/1403551139_ARQUIVO_ABCP-VersaoFinal2.pdf

Ralo, J. (2013). Artigo de Opinião - CiberSegurança e CiberDefesa. Obtido 28 de Outubro de 2016, de http://dgpdn.blogspot.com/2013/03/artigo-de-opiniao-ciberseguranca-e.html

Rodrigues, P. E. B. (2010, Outubro). *Segurança Informática de Redes e Sistemas (Abordagem Open-Source)* (Dissertação de Mestrado). Universidade de Trás-os-Montes e Alto Douro. Obtido de http://repositorio.utad.pt//handle/10348/747

Santos, L. (2011). *Contributos para uma melhor governação da cibersegurança em Portugal* (Dissertação de Mestrado). Faculdade de Direito da Universidade Nova de Lisboa, Lisboa. Obtido de http://run.unl.pt/handle/10362/7341

Santos, L. (2013). *Cibersegurança: Visão Analítica*. Obtido de http://sm.vectweb.pt/media/43/File/EEDS_2013/IEEDS%20-%20apresenta%C3%A7%C3%A30%20-%20Ciberespa%C3%A70%20-%20Lino%20Santos.pdf

Saraiva, M. F. (2011, Agosto). *Ciberterrorismo: Terrorismo Virtual? Uma Abordagem Territorial ao Fenómeno Terrorista no Ciberespaço*. Apresentado no XI Congresso Luso Afro Brasileiro de Ciências Sociais, Salvador da Bahia. Obtido de http://www.xiconlab.eventos.dype.com.br/resources/anais/3/1307728152_ARQUIVO_Ciberterrorismo_Francisca_Saraiva_Congresso_Luso_Afro_Brasileiro.pdf

Sequeira, J. (2004). *Segurança Interna e Externa Face às Novas Realidades*. Trabalho de Investigação Individual no âmbito da Disciplina de Estratégia, do Curso do Estado-Maior 2002/2004.

Sobral, J. T. (2010). *Cibersegurança na Área da Justiça - CERT, detecção de incidentes e contra-medidas*. Apresentado no VII Encontro Anual do Conselho Superior da Magistratura, Évora. Obtido de https://www.csm.org.pt/ficheiros/eventos/7encontrocsm_torressobral.pdf

Sobral, J. T. (2014). *O Levantamento do Centro Nacional de Cibersegurança: um desígnio nacional*. Comunicação oral apresentada na Segurança da Informação e Gestão do Risco na 3ª Plataforma, Lisboa. Obtido de http://comum.rcaap.pt/handle/123456789/7657

Sousa, S. S. (2015). *Criminalidade Organizada Cibernética*. Apresentado no Seminário sobre a Criminalidade Organizada Transnacional, ISCPSI, Lisboa.

Symantec. (2016). *Internet Security Threat Report 2016* (No. 21). Obtido de https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Torres, A. (2014). *Os referenciais de segurança da informação e a melhoria contínua: um caso exploratório* (Dissertação de Mestrado). Instituto Superior de Engenharia do Porto, Porto. Obtido de http://recipp.ipp.pt/handle/10400.22/5588

Torres, P. (2014). *Portugal: o caminho entre o real e o virtual* (Dissertação de Mestrado). Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa, Lisboa. Obtido de https://run.unl.pt/handle/10362/14430

Ventura, S. (2015, Outubro). *UFCD 0771: Conexões de Rede*. Aula lecionada, Porto.

Diplomas Legais e Jurisprudência

Decreto-Lei n.º 62/2011 de 9 de Maio, do Ministério da Defesa Nacional, Pub. Diário da República n.º 89 § 1ª série (2011).

Lei n.º 53/2008 de 29 de Agosto, da Assembleia da República, Pub. Diário da República n.º 167 § 1ª série (2008).

Lei n.º 59/2015 de 24 de junho, da Assembleia da República, Pub. Diário da República n.º 121 § 1ª série (2015).

Lei n.º 109/1991, de 17 de Agosto, da Assembleia da República, Pub. Diário da República n.º 188 § 1ª série (1991).

Lei n.º 109/2009, de 15 de Setembro, da Assembleia da República, Pub. Diário da República n.º 179 § 1ª série (2009).

Portugal. (2015a, Maio 26). Tribunal da Relação do Porto. Acórdão n.º RP2015052635/07.2JACBR.P1. Relator: Maria Luísa Arantes. Obtido de http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/aa9d0fb297dcca7880257e62003a86e4?OpenDocument

Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho, Presidência do Conselho de Ministros, Pub. Diário da República n.º 113 § 1ª série (2015).

Emissão Televisiva

Kochavi, M. (2016a). Crush. *Dark Net*.

Kochavi, M. (2016b). Upgrade. *Dark Net*.

Webgrafia

Awatare, A. (2014, Março). *Cyber crimes and security*. Obtido de http://pt.slideshare.net/ashwiniawatare/cyber-crimes-and-its-security

Brandão, J. (2013). *Evolução da Internet*. Aula lecionada. Obtido de http://pt.slideshare.net/jalmeidabrandao/evoluo-da-internet-17078918

CCM. (2015). Introdução à segurança informática. Obtido 20 de Julho de 2015, de http://br.ccm.net/contents/623-introducao-a-seguranca-informatica

Daquino, F. (2010). Navegue sem medo! Extensões e complementos para reforçar a segurança dos navegadores. Obtido 28 de Maio de 2016, de http://www.tecmundo.com.br/opera/4627-navegue-sem-medo-extensoes-e-complementos-para-reforcar-a-seguranca-dos-navegadores.htm

DGPJ. (2016). Sistema de Informação das Estatísticas da Justiça. Obtido 25 de Outubro de 2016, de http://www.siej.dgpj.mj.pt/webeis/index.jsp?username=Publico&pgmWindowName=pgmWindow_636131241829218750

EUROPOL. (2014). Cybercrime: A growing global problem. Obtido 11 de Novembro de 2014, de https://www.europol.europa.eu/ec/cybercrime-growing

Francis, M. N. (2008). A história da Internet e da web, e a evolução dos padrões web. Obtido 15 de Fevereiro de 2015, de https://danillonunes.com/curriculo-dos-padroes-web/a-historia-da-internet-e-da-web-e-a-evolucao-dos-padroes-web

Flloress, C. (2010). Evolução da Internet - história sobre os *sites* de busca. Obtido 19 de Fevereiro de 2015, de https://sites.google.com/site/historiasobreossitesdebusca/evolucao-da-internet

GNS. (n.d.). Organograma do Gabinete Nacional de Segurança. Obtido 2 de Novembro de 2016, de http://www.gns.gov.pt/organograma.aspx

Hollinger, B., & Mart, N. (n.d.). Web Design. Obtido 19 de Fevereiro de 2015, de http://portfolio-mart.weebly.com/web-design.html

Lordello, J. (n.d.). Dicas para uso do Home Banking com segurança. Obtido 28 de Maio de 2016, de http://tudosobreseguranca.com.br/portal/index.php?option=com_content&task=view&id=860&Itemid=154

Muniz, F. (2012). *Origem e evolução da internet*. Picos. Obtido de http://pt.slideshare.net/laerciomesquita/origem-e-evoluo-da-internet-26392684

Pereira, F. (2012, Fevereiro 10). O Cibercrime. Obtido 12 de Novembro de 2014, de http://protejainternet.blogspot.pt/2012/02/o-cibercrime.html

Richter, F. (2014). 75% Of Mobile Apps Want Access To User Data. Obtido 15 de Julho de 2016, de https://www.statista.com/chart/2710/app-privacy/

SIS. (n.d.). Ciberameaça. Obtido 10 de Agosto de 2015, de http://www.sis.pt/ciberameaca.html

UOL. (2013). O que é phishing? Obtido 18 de Agosto de 2015, de http://seguranca.uol.com.br/antivirus/dicas/curiosidades/o-que-e-phishing.html#rmcl

Vieira, O. J. T. (2006a). Crimes Informáticos. Obtido 8 de Dezembro de 2015, de http://crimesinformaticos.no.sapo.pt/index.htm

Vieira, O. J. T. (2006b). Introdução. Obtido 19 de Fevereiro de 2015, de http://crimesinformaticos.no.sapo.pt/index.htm

APÊNDICES

Apêndice A: Sistema de Segurança Interna

Figura 8.0.1: Esquema ilustrativo das entidades que compõem o Sistema de Segurança Interna, nomeadamente o Conselho Superior de Segurança Interna, o SG-SSI e o Gabinete Coordenador de Segurança

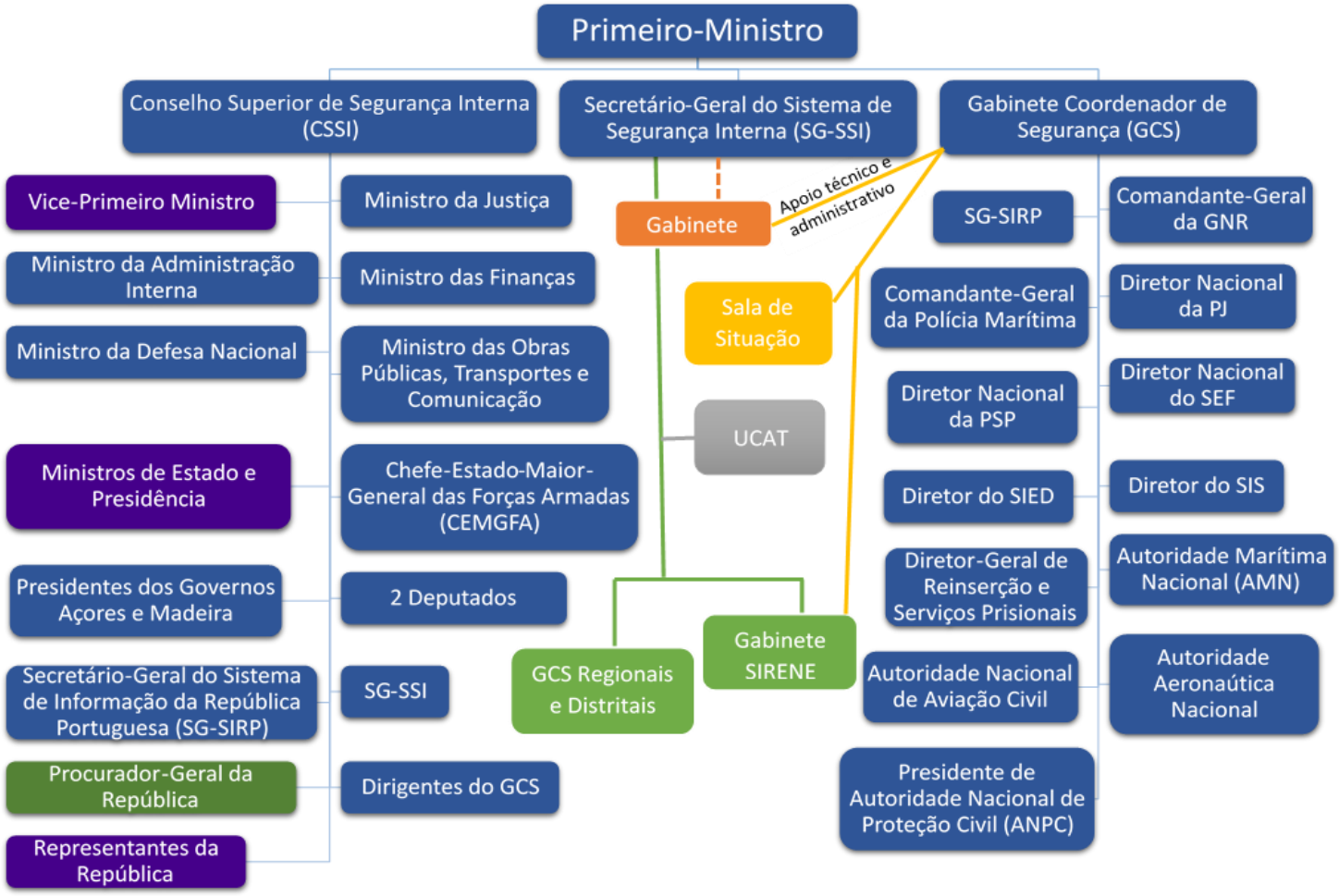


Imagem de autoria própria com recurso à Lei de Segurança Interna (*Lei n.º 53/2008 de 29 de Agosto, da Assembleia da República*, com a respetiva alteração da *Lei n.º 59/2015 de 24 de junho, da Assembleia da República*).

Apêndice B: Gráfico dos Resultados das Redes Sociais

Gráfico 8.0.1: Gráfico de área, de frequência, ilustrativo das respostas dos inquiridos quanto às redes sociais que utilizam