NAVEGAÇÃO WEB ANÓNIMA E SEGURA

Nuno Ricardo Mateus Coelho

Dissertação para obtenção do Grau de Mestre em Engenharia Informática, Área de Especialização em Sistemas Gráficos e Multimédia

Júri:

Presidente:

Professor Doutor Nuno Alexandre Pinto Silva, ISEP

Vogais:

Professor Doutor António Abel Vieira de Castro, ISEP

Professor José Joaquim Magalhães Moreira, ISLA-IPGT

Doutor Nuno Miguel Gomes Bettencourt, ISEP

Porto, Outubro 2015

À minha filha Maria Clara e à minha Esposa Maria João Pecegueiro pelas minhas ausências.

Ao meu irmão que não me pôde ter como exemplo, com saudade.

À minha mãe que deu o que tinha por mim,

Sou apenas o reflexo da sua dedicação.

Agradecimentos

O percurso académico de um aluno é feito de trabalho e dedicação. Este trabalho não é único dos alunos pois eles mais nada são do que recetáculos do conhecimento dos professores. Não poderia deixar de registar neste documento todos aqueles que contribuíram para a realização desta dissertação.

- Agradeço em particular ao meu orientador Prof. Doutor António Vieira de Castro docente no Instituto Superior de Engenharia do Porto (ISEP) e investigador do grupo *Games Interaction and Learning* (GILT), pela sua sempre disponível ajuda e orientação. Pela dedicação espartana que aplica ao transmitir conhecimentos nas suas aulas e pelo apoio na orientação deste trabalho.
- Agradeço ao meu coorientador, o Mestre José Joaquim Moreira (Docente e Diretor do curso do 1º ciclo em Sistemas Multimédia do Instituto Politécnico de Gestão e Tecnologia, (IPGT) pela sua dedicação e incentivo na procura por maior conhecimento académico.
- Aos meus colegas de curso e, em particular, ao Emanuel Fonseca que desde o início foi meu "*colega de carteira"* e sempre me apoiou ao longo do curso de Mestrado.
- À minha família, e acima de tudo à minha esposa Maria João Pecegueiro que pacientemente compreendeu as minhas longas horas de ausência.

A todos, reitero o meu obrigado.

Resumo

A *Web* aproximou a humanidade dos seus pares a um nível nunca antes visto. Com esta facilidade veio também o cibercrime, o terrorismo e outros fenómenos característicos de uma sociedade tecnológica, plenamente informatizada e onde as fronteiras terrestres pouco importam na limitação dos agentes ativos, nocivos ou não, deste sistema.

Recentemente descobriu-se que as grandes nações "vigiam" atentamente os seus cidadãos, desrespeitando qualquer limite moral e tecnológico, podendo escutar conversas telefónicas, monitorizar o envio e receção de *e-mails*, monitorizar o tráfego *Web* do cidadão através de poderosíssimos programas de monitorização e vigilância. Noutros cantos do globo, nações em tumulto ou envoltas num manto da censura perseguem os cidadãos negando-lhes o acesso à *Web*. Mais mundanamente, há pessoas que coagem e invadem a privacidade de conhecidos e familiares, vasculhando todos os cantos dos seus computadores e hábitos de navegação.

Neste sentido, após o estudo das tecnologias que permitem a vigilância constante dos utilizadores da *Web*, foram analisadas soluções que permitem conceder algum anónimato e segurança no tráfego *Web*. Para suportar o presente estudo, foi efetuada uma análise das plataformas que permitem uma navegação anónima e segura e um estudo das tecnologias e programas com potencial de violação de privacidade e intrusão informática usados por nações de grande notoriedade. Este trabalho teve como objetivo principal analisar as ferramentas de monitorização e de vigilância informática, identificar as tecnologias disponíveis e desenvolver uma solução na forma de uma ferramenta multimédia alicerçada em *Linux.* Foram integrados recursos no protótipo com o intuito de proporcionar ao utilizador uma forma ágil e leiga para navegar na *Web* de forma segura e anónima e segura, a partir de um sistema operativo (SO) virtualizado e previamente ajustado para o âmbito anteriormente descrito.

O protótipo foi testado e avaliado por um conjunto de cidadãos no sentido de aferir o seu potencial. Termina-se o documento com as conclusões e o trabalho a desenvolver futuramente.

Palavras-chave: segurança, navegação anónima, rede T*or*, *Linux*, violência, pirataria informática, cibercrime.

Abstract

The Web was the mean to shorten the distance between Men to an unprecedented level. With this facility also came cybercrime, terrorism and other phenomena of a moving society, fully computerized and where the land borders are of little importance in limiting the active agents, harmful or not, to this system.

Recently the world knew by the media and the WikiLeaks, that its leading nations follow closely their citizens, disregarding any moral and technological threshold, that internal and external security agencies in the United States closely follow telephone conversations, e-mail, Web traffic of their counterparts, using powerful monitoring and surveillance programs. In other corners of the globe, nations in turmoil or wrapped in the cloak of censorship persecute and deny uncontrolled Web access without armful repercussions to their citizens. Worldlier, pears coerce and invade the privacy of acquaintances and family, searching every corner of their computers and surfing habits, enforcing violence as vendetta.

This work analyzed the technologies that control the usage of Web consumers, solutions that enable and grant some anonymity and security in Web traffic. To support this study, an analysis was made of the platforms that allow for anonymous Web browsing, technologies and programs with potential computer intrusion and violation of privacy by high-profile nations. This study aimed to analyze the computer monitoring and surveillance technologies and identify the available countermeasure technologies. It scope relied on the deliver a multimedia tool developed in *Linux*, providing a LiveDVD (*Linux* OS that runs from DVD without installation). Resources were integrated in the prototype, developed in order to provide the user with a flexible and lay way to surf the Web in a safe and anonymous environment. It was prepared to operate from as a LiveDVD or inside a virtual machine. The prototype was tested and evaluated by a group of citizens to check its potentiality and effectiveness. The work was finished with the conclusions and the work to be develop in the future.

Keywords: security, private browsing, Tor network, *Linux*, open source, violence, hacking.

Índice

Lista de Figuras

Lista de Tabelas

Notações, Glossário e Acrónimos

Backdoor	Porta traseira na sua tradução literária. Significa uma porta oculta para acesso a um programa ou equipamento.
Browser	Aplicação que permite ao utilizador navegar na World Wide Web. O Microsoft Internet Explorer, Mozilla Firefox, Opera, Safari, Chrome.
Bug	Erro de programação num software.
Chat	Conversação via Web
Cloud Computing	Computação em nuvem - utilização da memória e das capacidades de armazenamento e cálculo de computadores e servidores partilhados e interligados através da Internet, seguindo o princípio da computação em rede. Clouds conhecidas: iCloud, DropBox, OndeDrive
Commercial Off-the-shelf	Software pronto a usar comprador por norma em espaços comerciais
Cracker	Denominação de pessoas que criam e modificam software e hardware de computadores com o intuito de destruir informação e utilizá-la em proveito próprio, procurando reconhecimento, informação privilegiada ou mesmo compensações monetárias.
Datacenter	Centro de computação, por exemplo um local que possui servidores de alojamento Web ou armazenamento de dados.
Demo	Demonstração do software ou disponibilização de uma parte limitada de um programa de software
DHCP	Dynamic Host Configuration Protocol é um protocolo usado em redes de computadores que permite que sejam atribuídos endereços IP automaticamente aquando da conceção dos hosts à rede.
DMZ	Demilitarized Zone significa uma zona lógica de uma rede usada para colocar serviços de acesso direto ao exterior, nos quais o grau de exigência para a segurança é menor, permitindo também resguardar o sistema interno, separando-o dos restantes serviços.
DNS	Domain Name System é uma sigla que representa um servidor de nomes que traduz endereços de nomes em endereços IP.
DoS	Denial of servisse é um tipo de ataque no qual se pretende bloquear o sistema fazendo um número de conexões de tal forma elevado que o

	sistema fique bloqueado
Download	Descarregar dados de um PC para outro através da rede ou sistema
Eavesdropping	Significa literalmente estar à escuta de forma escondida.
Exploit	Aproveitamento de uma vulnerabilidade de um software ou equipamento.
Facebook	Rede Social
Firewall	É um dispositivo de uma rede de computadores que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão e/ou receção de dados nocivos ou não autorizados de uma rede para outra.
Front-end	Parte do sistema de um software que interage diretamente com o utilizador
FTP	File Transfer Protocol. Protocolo de transferência de ficheiros em redes.
Hacker	É um termo atribuído a pessoas que criam e modificam software e hardware de computadores com o intuito de adquirir informação. Dependendo do tipo de hacker, pode utilizar a informação que detém para informar organizações de vulnerabilidades inerentes ou utilizá-la em proveito próprio, procurando reconhecimento, informação privilegiada ou mesmo compensações monetárias.
Hardware	Componentes físicos do um dispositivo ou sistema informático
HTML	HyperText Markup Language (Linguagem de Marcação de Hipertexto). Linguagem utilizada na criação de páginas Web
HTTP	Hypertext Transfer Protocol (Protocolo de Transferência de Hipertexto). Protocolo utilizado para transferências de páginas Web de hipertexto
HTTPS	HyperText Markup Language Secure. Protocolo de transferência com encriptação SSL.
Input	Entrada de informação no sistema informático. Tal entrada irá provocar uma mudança que ativa ou modifica um processo.
Internautas	Navegadores da Web
Internet ou NET	Conjunto de redes informáticas interligadas através do protocolo IP
IP	Internet Protocol ou protocolo de Internet
Javascript	Linguagem de programação criada em 1995 pela Netscape
Layout	Organização espacial de todos os elementos que compõem uma página

Link	Hiperligação ou simplesmente uma ligação a um documento
Malware	O malware é um programa concebido para causar danos ou para aceder ilegalmente a informação em sistemas informáticos.
MySQL	É um sistema de gestão de bases de dados (SGBD), que utiliza a linguagem SQL como interface
Open Source	Expressão que representa "código aberto", i.e., liberdade de visualização e modificação de um conteúdo, particularmente relacionado com código fonte de aplicações.
Password	Palavra passe que é usada em conjunto com um username para aceder a conteúdos privados ou sistemas privilegiados.
Plain Text	Expressão que representa texto puro, "às claras", passível de ser diretamente lido por terceiros
Plugin ou plug-in	Pequeno software que serve normalmente para adicionar funções a outros programas maiores, adicionando-lhe algumas funcionalidades específicas.
Post	Publicações cronológicas em websites/Blogs
Script	Programação em linguagem interpretada para ser executada no/ou do interior de programas, podendo ser executadas em vários ambientes
SGBD	Sistema de Gestão de Bases de Dados
Site	Sítio na Web. É constituído por um conjunto de páginas Web, ligadas umas às outras através de hiperligações, alojadas num servidor da Web
Smartphone	Telefone, com funcionalidades avançadas que podem ser estendidas por meio de programas executados por seu sistema operativo
Software	Sistema operativo Programas, ficheiros, é a parte lógica de um sistema informático
Spyware	Programas que normalmente estão relacionados com publicidade e troca de informações do computador do cliente para um servidor, sem o conhecimento do mesmo. São uma espécie de vírus não destrutiva e por vezes não são detetáveis por aplicações antivírus, mas sim por novas aplicações denominadas "anti-spyware".
SSL	Secure Sockets Layer. Protocolo de segurança que permite encriptar informação para evitar a sua leitura por terceiros.
Trojan	Trojan ou Cavalo de Tróia, um malware que age tal como na história do

	Cavalo de Troia, entrando no computador e criando uma porta para uma possível invasão
UDP	User Datagram Protocol é um protocolo simples da camada de transporte, permitindo que um determinado programa escreva um pacote de dados encapsulado em IPV4 ou IPV6.
Up-front invest	Investimento inicial
URL	Abreviação de Universal Resource Locator, Localizador de Recursos Universal
Usabilidade	Facilidade de uso das interfaces gráficas
Username	Nome do utilizador, comummente refere-se ao campo numa caixa de login, ao espaço onde se coloca o nome.
Virtual Server	Um servidor virtual permite obter toda a funcionalidade de um servidor físico, sem recorrer a uma máquina física independente. O servidor virtual tira partido do hardware da máquina host (servidor de serviços), utilizando-o como seu. Apesar da perda de substancial de desempenho, esta técnica permite ter vários servidores independentes dentro de uma só máquina.
Vírus	Programa que é executado numa máquina com ou sem conhecimento do utilizador e que tem como alvo a integridade, disponibilidade ou confidencialidade da informação.
VPN	Virtual Private Network. É uma rede simulada para utilização em comunicações privadas entre organizações. É construída em sobre uma rede de comunicações pública.
Web	Termo utilizado para representar World Wide Web, também designada como WWW
Webserver	PC prestador de serviços Web
Website	Sítio na Web.
Workflow	Fluxo de e sequência de passos necessários para que se possa atingir a automação de processo de acordo com um conjunto de regras definidas
Worm	Tipo de programa que se aloja na máquina-cliente e executa um determinado número sequêncial de operações. Normalmente, este conceito está associado ao furto de informação e não à atividade destrutiva, ao contrário dos vírus.

AOL	America On-Line
API	Application Programming Interface
CIA	Central Intelligence Agency
CMS	Content Management System
FCCN	Fundação para a Computação Científica Nacional
GNU	General Public License
HS	Homeland Security
HTML	HyperText Markup Language
IA	Inteligência Artificial
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
ISPs	Internet System Providers
LUKS	Linux Unified Key Setup
NSA	National Security Agency - USA
NYT	New York Times
OSP	Open Source Portfolio.
PC	Personal Computer
SI	Sistema Informação
SO	Sistema Operativo
TI	Tecnologias de Informação
TCP/IP	Transmission Control Protocol/Internet Protocol
TIC	Tecnologias de Informação e Comunicação
W. P.	Washington Post
WWW	World Wide Web

1 Introdução

"É mais divertido ser um pirata que um marinheiro"

Steve Jobs

Neste capítulo é realizado a contextualização prévia que refere alguns conceitos fundamentais a perceber. É apresentado o enquadramento relativo ao tema da segurança informática com ênfase em questões intrínsecas aos mecanismos de segurança e efetividade dos mesmos, ataques comuns, evolução e crescimento tecnológico. Identificam-se a problemática relativa ao percurso ascendente das tecnologias de informação e os impactos dos desafios que à sociedade são colocados diariamente e identificam-se concretamente as principais dificuldades e problemas existentes. São identificados os objetivos e contributos espectáveis pela proposta de trabalho a desenvolver e é elaborada a identificação conceptual do protótipo e tecnologias empregues neste, a motivação que originou a escolha do tema e, por fim, a estrutura da dissertação.

1.1 Contextualização prévia

Segundo David Whitley [David S. Whitley, 2009] a comunicação humana remonta à história mais antiga, aproximadamente há trinta mil a quarenta mil anos atrás. Inicialmente, eram usados símbolos para a passagem do conhecimento, por exemplo, para identificar comportamentos ou aspetos mundanos à altura, zonas e territórios, perigos ou apenas ócio. Foi há aproximadamente 9.000 anos que o homem iniciou a árdua tarefa de escrever palavras com sentido e com o intuito de passar conhecimento ou reter o mesmo.

O sistema de escrita organizada e com conteúdo semântico apareceu também há aproximadamente apenas 6 mil anos, daí para a frente as grandes evoluções tecnológicas que se seguiram foram sempre acompanhadas pelo registo de atividades e planeamento das mesmas, sobe a forma escrita. A evolução foi de tal ordem que, na atualidade, a escrita é maioritariamente feita de forma digital através de instrumentos de multimédia e de entrada de dados nos computadores, sendo fulminantemente difundida pelos meios digitais por milhões e milhões de pessoas. Segundo Zuckerberg, [Mark Zuckerberg, 2015] em 2015, a 8 de setembro, uma em cada sete pessoas estava ligada ao mesmo tempo ao *Facebook* (rede social digital), um feito astronómico desde a altura em que o homem fazia gravuras em paredes de cavernas.

O progresso humano é verdadeiramente pautado por esta génese de evoluções, tendo na *Internet* o seu pico comunicacional. Comummente, considera-se a *Web*, o maior desenvolvimento tecnológico a seguir à roda e à capacidade de criar fogo. Tal como o fogo foi pioneiro nos primórdios da história ao capacitar o Homem de uma ferramenta que lhe permitiu aquecer-se, cozinhar os seus alimentos e defender-se contra elementos indesejáveis, foi também o ícone do futuro pois serviu como mecha que iluminou o caminho assustador, desconhecido, perigoso, abstrato e global. Por outro lado, a roda capacitou o Homem da mobilidade pessoal e logística, de regras básicas de engenharia que se aplicam à física e à astronomia. Em conjunto com a capacidade de iluminar, a roda deu lugar ao carro que circula à noite, e agora, em pleno século XXI, a tecnologia e a *Web* permitem que estes circulem autonomamente quase sem interferência humana. A *Web* tornou-se assim o verdadeiro sistema logístico informacional.

Vivemos numa época em que a sociedade é desafiada pela mudança repentina com impactos sociais, políticos, económicos e elevados custos ambientais. Esta volatilidade implica fortes consequências ao nível da (in)segurança das sociedades e das organizações. A velocidade a que se sucedem os acontecimentos, novas ofertas tecnológicas, novas tendências, produtos, problemas e soluções, criam um desnorte que tem já hoje em dia, e apesar dos esforços de quem regulamenta, um impacto virtualmente impossível de conter ou esconder.

A pesquisa e o uso massivo de informação e a partilha social da mesma foram criados pelo advento *Web* 2.0 ou 2ª geração da *Web,* termo introduzido por Tim O'Reilly [Tim O'Reilly, 2009], que associado com a nova geração *Web* 3.0, caracterizada pela *Web* semântica, termo introduzido por John Markoff [Sam Murugesan, 2009], criou uma singularidade ímpar e equiparável apenas à pegada ecológica humana. A pegada digital implica que tudo o que se partilha e expõe na *Web,* fique arquivado algures na mesma, permitindo a terceiros aceder e guardar essa informação em *clusters* computacionais com vida útil estimada impossível de calcular, ficando assim acessível a outros por muitas e muitas gerações.

Ao confiar nas plataformas *Cloud* (armazenamento de dados em nuvens computacionais virtualizadas) e ao publicar informação pessoal nas redes sociais, abriu-se a porta ao cibercrime (crimes cometidos com recurso a tecnologias de informação) que durante anos esteve localizado e orientado aos sistemas de informação das organizações.

Considerando que a partilha social iniciou massivamente com o advento *Web* 2.0, na tabela seguinte apresentam-se alguns conceitos:

Tabela 1 - Alguns conceitos *Web* 2.0

Computação Social - Referente a trabalho coletivo em detrimento do individual na concretização de tarefas complexas.
Creative Commons - Sistema de licenciamento de direitos de autor. É conhecido pela sua elevada flexibilidade, orientada para a partilha de conteúdos. Muito conhecido no meio de utilizações da *Wikipédia* (enciclopédia *online*).
Conteúdo Gerado por Internautas - Dados e informação massivamente partilhada através de meios digitais. Fonte de novos produtos e serviços orientados aos conteúdos.
Dados e Informações - Dá-se especial interesse e relevância aos conteúdos (*Youtube*, *blogs*, imagens) que sejam passíveis de partilha, alteração e consequente distribuição.
***Folksonomias* ou *Tag* -** Criada por Thomas Vander Wal, consiste na classificação por meio de *Tags* (etiquetas de identificação). Permitindo recuperar as informações e partilhar as mesmas.
Mobilidade - Possibilidade de acesso a conteúdos sem estar obrigatoriamente restringido a condições espaciotemporais.
Redes Sociais - Plataformas que permitem manter relações de pessoas com interesses idênticos ou comuns, amizade, profissionais, artísticas, como por exemplo, o *Facebook, o LinkedIn, o Twitter***.**

1.2 Enquadramento

Em 1969, a DARPA (*Defense Advanced Reaserch Projects Agency*), uma agência governamental de pesquisa e desenvolvimento de projetos avançados, iniciou um projeto que se propunha a desenvolver uma rede segura e fiável para transmissão de dados. Esta agência, de génese militar estabeleceu que os pilares da rede teriam obrigatoriamente de ser robustos e assentar no paradigma de comutação de pacotes. Vivia-se à época a Guerra Fria entre os Estados Unidos e a Ex União Soviética e este era efetivamente um projeto militar [James Derian, 2009]. Esta rede foi denominada de *ARPA* e mais tarde de *ARPANET*, sendo constituída inicialmente por quatro nós. Entre o período experimental do projeto, entre 1971 e 1975 a *ARPANET* foi usada com sucesso por mais de 60 computadores e já permitia o envio de *email*s e ligações em tempo real. Após a conclusão da fase experimental, foi colocada em prática a fase operacional do projeto conduzida pelo Departamento de Defesa Norte Americano que fazia então a gestão desta rede.

Foi precisamente por esta altura que se desenvolveram grande parte dos protocolos que ainda hoje são fundamentais e basilares à *Web*, como por exemplo, *o TCP/IP* que foi

desenvolvido em 1971 para ultrapassar as dificuldades da ligação da *ARPANET* a redes privadas de *BBS*[1] (*Bulletin Board System*). Corria o ano de 1983 e a decisão de dividir a rede em duas foi iniciada. A *MILNET* (rede global de ambiente militar) e a *ARPANET* tornaram-se assim duas redes distintas. À rede global composta por estas duas denominou-se de *Internet*, tendo sido este o elemento fundamental que permitiu o crescimento e a globalização da mesma. Em 1989 a rede contava já com 80.000 máquinas ligadas de origens variadas, universidades, empresas e institutos. Em 1990, a *ARPANET* é extinta para dar lugar à *Internet,* que já tinha largo uso [Michael Woodrow, 2014].

Apenas nos anos 80 é fundada na Europa a associação de redes utilizando o protocolo *TCP/IP* com o nome de RIPE (*Réseaux IP Européens*) e nos anos 90 a rede EBONE (*European Backbone*), uma rede de escala europeia conectada à *Web*.

Apenas nos anos 90 é lançada em Portugal a RCCN (Rede para a Comunidade Cientifica Nacional), que interligava várias universidades nacionais através da rede *EBONE* gerida pela Fundação para a FCCN (Comunidade Cientifica Nacional em Portugal). Esta foi descomissionada em 1992 para dar lugar à GEANT. Atualmente a rede que sucedeu a RCCN, a RCTS (Rede de Ciência, Tecnologia e Sociedade), está conectada à *Web* através da rede europeia *GEANT2*.

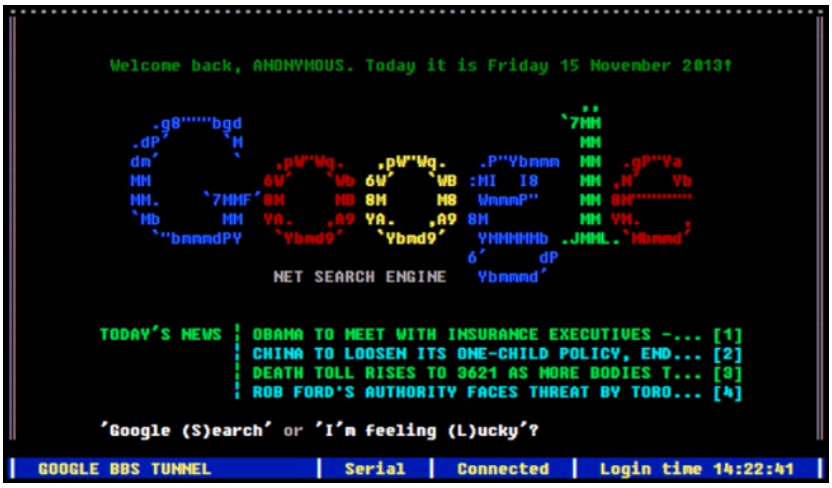

Figura 1 - Aspeto emulação da BBS da Google recriada em 2013 [2]

Em 2014, segundo a *Internet Live Stats* [Internet Live Stats, 2015], aproximadamente 3 mil milhões de utilizadores estavam ligados à *Web*[3] e partilhavam dados. A *Web* é extremamente propícia a todo o tipo de atos danosos praticados por desconhecidos e não tão desconhecidos.

[1] BBS - Bulletin board system é um sistema informático, um software, que permite a ligação (conexão) via telefone a um sistema através do seu computador e interagir com ele, tal como hoje se faz com a Internet

[2] Imagem recolhida em – http://www.masswerk.at/googleBBS/

[3] Internet Live Stats 2015 - http://www.Internetlivestats.com/Internet-users/

Por ser uma entidade viva (no sentido lato da palavra), esta globalização, esta rede que é constituída por pessoas e máquinas, é também uma fonte de desinformação orientada às nações que competem entre si, em que, quem detém primeiramente a informação validada tem de facto a liderança e para a conseguir, quer seja esta económica ou estratégica, criam-se mecanismos que preconizam a insegurança informática através da violação, descodificação, modificação e intercetação com objetivo de reter informação privada para benefício próprio.

A segurança informática é colocada à prova constantemente. Segundo Paulo Santos, [Paulo Santos, 2008] desde piratas informáticos vulgarmente conhecido por *hackers*, a entidades de espionagem governamental, todos querem um pedaço do *El Dorado*, seja este apenas uma questão de ego, proveitos económicos ou vantagem estratégica nos jogos da política internacional.

Sistemas informáticos ligados entre si por rede e, acima de tudo, pela rede ampla que é a *Web*, são usados para armazenar e manipular informação diariamente por milhões de pessoas e organizações. Segundo Herman Walker [Hermann Walker, 2009] sejam escolas, universidades, gabinetes médicos, alunos, professores médicos ou indigentes, todos estes e todas estas entidades trocam informação com recurso a redes informáticas; ora, é seguro dizer que a informação está em circulação e, logo, é crítico que esta informação esteja segura.

A segurança informática é crescentemente um problema social e um problema técnico. Técnico pois a variedade de sistemas, normas, arquiteturas, metodologias como *ITIL (Information Technology Infraestructure Library)*[4], *COBIT (Control Objectives for Information and Related Technology)*[5], *TOGAF (The Open Group Architecture Framework)*[6], *SOA (Software Oriented Architecture)*[7], versões de sistemas operativos, *hardware* e seu requisitos, requisitos de *software,* entre muitos exemplos, tornam a tarefa de implementação de medidas e normas de segurança, circuitos de mitigação de risco e elaboração de planos diretores informáticos que antecipem e respondam a questões inesperadas. Uma verdadeira tarefa dantesca, culminando na impossibilidade de criação ou total abrangência de políticas de segurança eficazes. Basta adicionar à equação a ligação à *Web* de sistemas distribuídos para que realmente se torne uma missão quase impossível [Javier Lopez et al., 2015].

[4] ITIL – Information technology Infrastructure Library – Norma de boas pratica na gestão manipulação de sistemas informatizados

[5] COBIT – Control Objectives for Information and Related Technology – Guia de boas práticas para gestão e manipulação de sistemas informatizados

[6] TOGAF – The Open Group Architecture Framework – Framework de arquitetura corporativa de sistemas de informação

[7] Service Oriented Architecture – Arquitetura orientada a serviços

Problema social, pois os utilizadores não técnicos destes sistemas não possuem uma noção das necessidades e dos problemas de segurança existentes. Para estes, segundo Brian Shea [Brian Shea, 2002] é transparente todo o esforço e sistemas atrás do ecrã, e não relegam grande atenção ao detalhe pois sentem segurança por terem um antivírus, uma *firewall* que emite alertas gráficos no *GUI* (*Graphical User Interface*), aos técnicos informáticos que implementam e lhes dão suporte às dificuldades do dia-a-dia nas organizações.

Diariamente são desenvolvidas aplicações que visam o aproveitamento e a desatenção do público em geral ou dos administradores de sistemas. Também diariamente empresas de renome desenvolvem e lançam para o mercado aplicações para permitir que se consigam evitar os mecanismos que insistem em violar a privacidade informática.

Ao longo dos tempos foram sendo criadas soluções informáticas que se propunham manter a segurança da informação e dos utilizadores desta. Entidades como a *Symantec*[8] (empresa de *software* e de segurança informática) lançam diariamente atualizações aos seus programas antivírus numa tentativa de resposta às ameaças criadas. Empresas como a *Microsoft*[9] criam atualizações que disponibilizam regularmente para corrigir erros e vulnerabilidades do *software* que desenvolve e comercializam. Empresas como a *CISCO*[10] desenvolvem *appliances* (equipamentos) de rede que são passíveis de ajustes, com outras funcionalidades que não são ajustáveis, no sentido de padronizar conceitos de segurança e mecanismos de defesa [Gary Shelly and Jennifer Campbell, 2012].

Não obstante este panorama, estas medidas não são mais do que reativas aos desafios diários e lamentavelmente não são preventivas.

Segundo Paulo Santos [Paulo Santos, 2008], para a prevenção, existem políticas e mecanismos complexos de segurança que estão estabelecidas e plenamente aceites pelas entidades que desenvolvem equipamentos e *software*, mas nem sempre implementadas pelos utilizadores finais. Segundo o mesmo autor, as políticas de segurança definem o foco da segurança e o que esta deverá garantir e assegurar. Os mecanismos são a tecnologia que permite pôr em prática as políticas de segurança. Um domínio de segurança consiste num universo de recursos (máquinas e redes) e pessoas sujeitas às mesmas políticas de segurança. Estas visam garantir a confidencialidade de informação reservada, visam a proteção de informação crítica, visam a continuidade da operação ou prestação de serviço, visam a confiança na correção de

[8] https://www.symantec.com
[9] https://www.microsoft.com
[10] https://www.cisco.com

operação de sistema, visam a prova de correção ou da autoria na troca de informação e visam, entre muitas outras garantias, a capacidade de auditoria de ações passadas.

Como em tudo na vida, existirão sempre riscos pois é impossível garantir a 100% que um determinado sistema está protegido. Para a gestão de risco dentro da segurança informática, a sociedade faz esforços e convenções que aproximam entre si métodos que visam diminuir o risco de intrusão. Estas normas ou padrões são gerais e são aplicáveis tanto às sociedades como, em última instância, aos cidadãos, pois são as sociedades que os irão implementar para que os cidadãos se sirvam destes. Normas como o Padrão *ISO/IEC* 27001 [Alan Calder, 2015] fornecem aproximações adequadas para a gestão do risco em sistemas informáticos. Este padrão fornece um enquadramento de *best practices* (boas práticas) para a gestão da segurança de informação e infraestruturas informáticas.

Por tudo isto, é notório que a segurança informática e a necessidade de mecanismos que protejam efetivamente os utilizadores estejam na ordem do dia. A *Web* transporta informação pública e privada, dificultando a tarefa de separar as duas, e o tempo, esse não pára, como também não pára a evolução.

1.3 Identificação do problema

Segundo a *Symantec,* no relatório *Insecurity of Internet of Things*, em 2015 estima-se que estarão conectados à *Web* aproximadamente 4.9 mil milhões de dispositivos [Mario Barcena, 2014]. Muitos destes equipamentos serão equipamentos que concentram em si poucos mecanismos de segurança ativa e passiva, como é o exemplo dos telemóveis, *tablets* e dos *smartphones*.

Independentemente deste panorama, todos os dias milhões e milhões de utilizadores partilham informação e dados através destes equipamentos. É através destes equipamentos que as gerações mais novas, e não só, comunicam entre si, ao ponto de já fazerem chamadas de voz sobre o protoloco de *Internet*, também conhecido por *VOIP* (*Voice Over IP)* para poupar nos custos de comunicação.

Atualmente as organizações deixaram de ser o alvo direto dos que se dedicam ao furto e desvio de informação, o utilizador comum tornou-se um alvo pela quantidade de informação que partilha *online*.

Também se observam os ataques a sistemas que prestam serviços, como servidores *Web* que guardam informação sobre utilizadores, como foi o caso do alegado ataque à plataforma

online do Euromilhões, noticiado pelo w*ebsite* pplware.sapo.pt em maio de 2015 [Pplware, 2015].

Segundo estes, embora a Santa Casa o tenha negado, no *Website REDDIT* (rede social especializada em conteúdos informáticos) foi anunciado que os dados de 20.000 utilizadores tinham sido comprometidos. A forma do ataque não foi revelada, tendo sido expostos dados que poderão ser usados para futuros ataques. Os elementos expostos consistiam em *username*, *hash*[11]*, MD5 (Message Digest 5), salt*[12], *email* (correio eletrónico) e datas de aniversário. O *MD5* gera códigos de *hash* de 128*bits* de comprimento e foi desenvolvido por Ron Rivest, do *MIT* (*Massachusetts* Institute of Technology), em 1991 [Daniel Barret, 2005], encontrando-se especificado no *RFC* 1321[13]. Dado que o algoritmo tem várias fragilidades já documentadas [Daniel Barret, 2005], [André Zúquete, 2014], a sua utilização é desaconselhada, contudo, estaria a uso quando ocorreu o ataque, e considerando que esta plataforma regista dados de pagamento de apostas, a administração de sistemas poderia ter antevisto o problema. Como se pode concluir, o erro humano impera em muitas falhas de segurança pois a mesma assenta nos pressupostos que determinados ataques não ocorrem em Portugal, que este tipo de ataques não é comum, mas a *Web* é global e os servidores, *websites*, repositórios de dados entre outros, estão disponíveis globalmente.

Embora estes dados possam parecer pouco relevantes, estes elementos permitem tentativas de intrusão em contas de *email* que tenham datas de nascimento como senha, e recuperar uma nova *password* do site do Euromilhões, após usar o mecanismo de segurança que recorre perguntas adicionais de segurança, como a confirmação da data de nascimento. A partir daí a imaginação toma lugar. Como se pode concluir neste ponto, evitar o uso de datas de aniversário como palavras passe é uma norma essencial. *Websites* como os da *Google* e da *Apple* não permitem que se use estas datas como senhas.

O ano de 2013 foi rico na revelação de eventos e atividades das entidades de segurança Norte Americanas. Segundo revelações de Julien Assange [Julien Assange, 2013] na *Wikileaks* (plataforma *online* de partilha de informação), a navegação segura pela *Web* não existe e nem sequer a localização dos utilizadores está salvaguardada. Segundo este, vários países conseguiam aceder aos dados dos utilizadores e extrair informação relevante. A não utilização

[11] Um hash é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F)

[12] Salt ou Sal é parte de um código aleatório usado para criar senhas seguras. Existe para prevenir ataques com recurso a dicionários de palavras - https://en.wikipedia.org/wiki/Salt_(cryptography)

[13] RFC 1321 ou Request For Comments 1321, é uma publicação da Internet Engineering Task Force (IETF) relativa ao MD5 Message-Digest Algorithm

de senhas seguras, sistemas encriptados, *firewall*, uso de *software* não licenciado e desbloqueado com recurso a *cracks* (programas criados para ultrapassar a obrigatoriedade de licenciamento legítimo) e outros mecanismos, facilitam o trabalho destas e de entidades [Fernando Boavida et al., 2013].

A possível falta de conhecimentos dos utilizadores em questões técnicas e de segurança, levou a que 220.000 proprietários de equipamentos *Apple* ficassem vulneráveis e com eles, os sistemas da *iCloud* (plataforma de armazenamento na nuvem) da *Apple* [Thomas Hyslip, 2014]. Quem recorre a programas estilo *Cydia*[14] para fazer compras de aplicações proibidas nos equipamentos da marca, pode acabar por comprar aplicações que permitem este tipo de ataques. Não se sabe concretamente que vulnerabilidade foi usada, mas as suspeitas recaem numa *backdoor* (porta escondida de entrada num determinado sistema) no método de *jailbreak* (desbloqueio de dispositivos móveis da Apple). Este ataque teve grande notoriedade, sendo conhecido como o caso das fotografias de celebridades.

Segundo Markus Jakobsson [Markus Jakobsson, 2012] e Christopher Adams, [Christopher Adams et al., 2012] os correntes *browsers* são mais um problema do que que uma solução. No início de 2010, as batalhas pelo pódio do *browser* mais rápido passaram a estar na ordem do dia. *Google Chrome*, *Firefox, Opera* e *Internet Explorer,* todos lançavam novas versões mais rápidas com o intuito de apenas ser o mais rápido e *hipster* (na moda, em tendência). Pelo caminho ficou a segurança que independentemente dos eventos que juntavam milhares de pessoas com capacidades informáticas que receberiam um prémio por encontrar vulnerabilidades, nunca eram em quantidade suficiente face ao número de versões lançadas para o mercado.

O utilizador incauto deixou na mão de terceiros a sua segurança pois a transparência destas questões técnicas e o ruído mediático em torno delas cria uma falsa sensação de confiança. A 4 de setembro de 2015, a *Mozilla* lançou um alerta de que o seu *browser*, o *Firefox,* permitia que dados fossem desviados devido a uma vulnerabilidade num produto da companhia que permite registar erros de *software* (*Bugzilla*) [Martin Brinkmann, 2014].

Inicialmente com ataques de *Phishing*[15], o utilizador comum é agora seguido atentamente quando navega nas mais variadas páginas *Web*. É atentamente seguindo por *cookies* que visam passar informação dos hábitos de navegação às entidades gestoras das plataformas e

[14] Cydia é um software de código aberto para o sistema operacional móvel iOS da Apple, possibilitando instalação de aplicativos não oficiais em equipamentos desbloqueados

[15] Phishing é o termo usado para descrever o ataque informático de tentativa de adquirir dados pessoais de terceiros com recurso a mail fraudulentos que personificam entidades fidedignas

seus parceiros, para que lhes seja apresentada publicidade noutras páginas *Web*, a publicidade dos serviços e produtos conexos aos seus gostos. É também através dos *cookies* que vários *websites* guardam a informação de sessão (nomes e palavras passe) dos utilizadores, expondo-os a ataques que capturam informação confidencial. Esta transmissão de informação através dos *cookies* torna muito mais simples a navegação, criando uma falsa sensação de conhecimento e domínio das tecnologias, o que por sua vez conduz ao descuido e, conclusivamente, ao furto de informação no melhor de cenários.

Ainda assim os ataques a sistemas informáticos organizacionais isolados, sistemas que prestam serviços, ataques ou controlo a utilizadores comuns, existem e são de conhecimento generalizado. O ponto de partida é, na grande maioria dos casos, descuido nos métodos de segurança, desconhecimento destes ou simplesmente as soluções existentes são complexas de usar.

Existem países que pelas suas características políticas empregam um controlo apertado de acesso a conteúdos disponibilizados pela *Web*. Segundo Ronald Deibert [Ronald Deibert et al., 2008], países como a Coreia do Norte limitam o acesso ao nível físico e tecnológico, ou seja, apenas determinadas pessoas podem ter acesso a dispositivos que permitam aceder à *Web*, e quem os possui, necessita ainda de passar por barreiras impostas pelos *ISP* (*Internet Service Provider(s)* ou provedores de serviços de *Internet*, e.g. Portugal Telecom). O objetivo é impossibilitar a visualização de conteúdos de determinados *sites*, países, religiões, etc.

O caso mais notório desta realidade é a Grande *Firewall* da China, também conhecida por *Golden Shield Project*, desenvolvido pela divisão informática militar da República Popular da China. Esta avançada *firewall* consegue automaticamente e através da análise de todo o tráfego de saída e de resposta à entrada, perceber se a informação deve ser censurada ou não. Ultrapassar esta barreira é simples, mas extremamente inseguro caso seja necessário fazer operações de valor. Confiar em sistemas de *proxy* é confiar toda a informação que emitimos e recebemos por esse canal, a quem gere esse canal.

1.4 Objetivos e contributos esperados

Como é notório pelo abordado anteriormente, a segurança informática é um elemento primordial neste trabalho e ser-lhe-á dada correspondência relevante com especial pormenor e incidência aos programas e mecanismos que permitem seguir, verificar, triangular e guardar informações sobre utilizadores da *Web*.

Com o presente estudo pretende-se dissertar sobre como as principais agências de segurança americanas recolhem informação com recurso a sistemas e analistas de sistemas e analisar a vasta rede informática que coleta, captura e analisa grande parte do tráfego informático em trânsito à escala global. São analisadas entidades e programas revelados pelo Analista de Sistemas da *CIA*, Eduard Snowden e pelo soldado Bradley Manning à *Wikileaks*, ex funcionários dessas instituições, que testemunharam em primeira mão a complexidade e a extensão dessa realidade comummente reconhecida e aceite [Alexander Avakov, 2012].

Pretende-se identificar como ultrapassar algumas barreiras técnicas impostas por provedores de *Internet* pelo mundo fora sendo analisada a forma de acesso à *deepWeb*[16]. O resultado final será a compreensão destes sistemas e uma ferramenta multimédia que consiste num *LiveDVD* (sistema operativo virtual que funciona sem necessidade de instalação a partir de um suporte digital) preparado para usar anonimamente e de forma segura a *Web*. Parte da informação disponibilizada neste trabalho é fruto de uma análise ao submundo informático através da rede *Tor* (*The Onion Router)* ou rede de anonimato, recolhida em conversas durante seis meses. Aqui, foi possível reunir informação e conferenciar com quem por norma se dedica a este tipo de iniciativas.

Este projeto visou conhecer as tecnologias que a todos ameaçam e as principais alternativas que existem para as contornar e iludir. O objetivo geral é o desenvolvimento de uma ferramenta plenamente útil e funcional, que faculte várias soluções, de navegação anónima e segura e que permita aos utilizadores menos capazes configurar autonomamente este protótipo nos seus computadores. Esta solução, impossível de ser instalada num computador, deverá estar apetrechada de soluções informáticas que permitem usar de forma segura e anónima a *Web*. Deverá conter e permitir:

- Circular na *Web* de forma anónima sem revelar a posição geográfica nem *IP* de origem;
- Comunicar de forma segura através de um sistema de *chat* seguro encriptado;

[16] Deepweb é uma rede de dados informáticos privada, acessível apenas com recurso á rede Tor ou I2P

- Contornar sistemas de bloqueio de tráfego e mecanismos de censura;
- Não deixar rasto de uso no computador nem facultar a localização geográfica do utilizador e do que este faz ou fez na *Web*;
- Tecnologia de criptografia de alto nível, fácil e simples de instalar caso seja necessário;

O *LiveDVD* contém ainda uma mistura de soluções que permite os seus utilizadores obter o melhor no que respeita à segurança informática:

- Segurança informática através do anónimato;
- Segurança informática através de mecanismos ofensivos;
- Segurança informática com recurso a técnicas de isolamento;
- Uso da rede *Tor*.

Neste projeto são empregues algumas técnicas de *Air GAP* recomendadas por Bruce Schneier [Bill Blunden, 2014], um reconhecido perito em criptografia e escritor de livros sobre segurança informática e também professor na Universidade de *Harvard*, contudo não será um sistema *Air Gap*. Apenas não serão ativadas ferramentas que não sejam essenciais para o uso da navegação segura. Não estão presentes ferramentas que permitam ser exploradas via *Web* por terceiros, e assim levar à descoberta da localização do computador.

Como objetivo geral, pretende-se que este trabalho seja uma fonte de informação e de consciência de um panorama real e até de certa forma amedrontador. Longe de querer ser alarmista, mas a realidade não está ao alcance de todos pois a desinformação impera e está espalhada por toda a *Web* de forma fragmentada e até contraditória. As soluções existentes, apesar de serem sólidas, são complexas e não orientadas ao público geral.

1.5 Motivação

A segurança informática é uma das áreas da computação que mais me fascinam e interessam. Não há muito tempo, numa conversa de circunstância num evento de apoio a pessoas vítimas de violência doméstica, uma oradora queixava-se que nunca pôde usar o computador de casa ou o seu portátil sem que o seu anterior marido o vasculhasse e a agredisse física e verbalmente após "inspeção". Pessoa após pessoa, todas tinham uma coisa em comum, a falta de acesso não censurado a um computador ou represálias pelo uso e conseguinte verificação do histórico.

Nas notícias, recorrentemente falava-se na Primavera Árabe e nas dificuldades de ultrapassar a censura informática para livremente expor as atrocidades da guerra civil na Síria.

Concomitantemente, vinham a público as iniciativas da *Wikileaks*, do jornalista e ativista informático Julian Assange e de Eduard Snowden. Snowden, um analista de sistemas da *NSA* (*National Security Agency*) e da *CIA* (*Central Intelligence Agency*), fez revelações aos jornais *The Guardian* e ao *The Washington Post*, onde deu a conhecer a agenda de segurança americana e o poderoso programa de vigilância informática denominado de *PRISM*. Saber como ultrapassar estes mecanismos de censura e espionagem das liberdades de qualquer cidadão do mundo é, sem dúvida, o âmbito deste trabalho.

Antes de iniciar os estudos na área das ciências informáticas, fui estudante da área jurídica durante 5 anos em algumas instituições pioneiras no estudo do cibercrime. Foi aqui que me interessei mais pela informática do que pelas leis desta, e me dediquei à aprendizagem e análise deste fenómeno. Foi aqui que decidi que deveria um dia ser aluno do *ISEP* para poder aprender com os melhores o conhecimento que necessito e poder ser um elemento contribuidor de algo positivo na minha carreira profissional e vida pessoal. Poder contribuir para uma navegação anónima e segura, sobretudo daqueles que são mais vulneráveis e com menos conhecimentos ao nível da informática, é uma tarefa altamente aliciante e motivadora.

1.6 Estrutura da dissertação

Este trabalho está estruturado em cinco capítulos. No primeiro capítulo é desenvolvida a apresentação e evolução histórica com o respetivo enquadramento relativo ao tema, principais problemas da utilização por parte dos internautas, estabelecidos os objetivos a que se propõe o trabalho e o autor do mesmo.

No segundo capítulo é feito o levantamento do estado da arte, onde se analisam e se descreve a sua origem, composição e métodos, separando as ameaças e o *modus operandi* (forma de funcionamento das mesmas), das soluções a estes problemas. Serão identificados os mais comuns ataques que são realizados aos internautas e utilizadores de tecnologia que permitem a partilha de dados e de informação. São identificados os mais recentes alvos individuais e coletivos e o impacto que estas ameaças têm diretamente nas vítimas.

No terceiro capítulo são descritas as funcionalidades e a objetividade do protótipo e a explicação da construção do mesmo. É apresentada toda a fase de preparação e resultados final, é feita a descrição individual das principais ferramentas e do impacto que estas têm na segurança.

No quarto capítulo são analisados e apresentados os resultados estatísticos finais e a demostração da funcionalidade e eficácia do protótipo.

Por fim, no quinto capítulo é efetuada uma reflexão geral e são apresentadas as devidas conclusões e perspetivas de trabalho futuro.

2 A segurança, as ameaças e as respostas

"O homem que sabe reconhecer os limites da sua própria inteligência,
está mais perto da perfeição"
Johann Goethe

Neste capítulo, foi efetuado um enquadramento relativamente às ameaças existentes à privacidade e segurança informática no uso das tecnologias para uma navegação *Web* segura, dentro do âmbito desta dissertação. Foram abordadas as necessidades de segurança e mecanismos que permitem que esta se verifique, enquadrados nos princípios basilares da segurança da informação, integridade, autenticidade, não-repúdio, disponibilidade e confidencialidade. Foram analisadas as principais normas e padrões, políticas de segurança e as ferramentas de acesso seguro a sistemas de informação.
Foram identificadas as ameaças de maior relevo à escala global, qual o seu provável *modus operandi* e que medidas existem para ultrapassar esses obstáculos.

2.1 Enquadramento

À medida que a expansão das redes a nível mundial avança a um ritmo fulminante, a segurança informática e a privacidade começam a ser vistas de outra forma. Manter seguro os sistemas de informação e de telecomunicações assume um papel vital no dia-a-dia dos intervenientes deste panorama, sejam utilizadores, administradores de sistemas informáticos em ambiente doméstico, empresarial ou governamental.
Não obstante desta necessidade de segurança, são as infiltrações, as violações de privacidade, os esforços maliciosos e não maliciosos, que levam a que todos os sistemas operativos estejam praticamente vulneráveis, o que por sua vez leva a que sejam desenvolvidas soluções comerciais e o*pen source*, para poder manter em última instância os utilizadores e a informação destes, segura cumprindo os pilares basilares da confidencialidade, integridades, disponibilidade e autenticidade.
São as investidas de *hackers* e *crackers* que mostram ao mundo que nem tudo é simples e que a segurança não termina nem começa num antivírus [Michael Whitman, 2011].
Neste capítulo pretende-se aclarar o estado da arte, com ênfase em dois pontos cruciais, ameaças e soluções.

2.2 Necessidade e mecanismos de segurança informática

As necessidades de mecanismos de segurança em redes informáticas apresentam-se em vários níveis, crescendo de forma exponencial e simétrica à complexidade dos sistemas em atividade. Desde a proteção de sistemas de telecomunicações *VOIP*, sistemas de *email* e gestão documental, comunicações de terminal remoto, proteção contra tentativas de acesso externo não autorizado, utilizando aplicações ou *appliances* de *firewall*, a segurança não deve ser colocada em segundo lugar, atrás da usabilidade dos sistemas [Christopher Kern et al., 2007].

Os vários sistemas, políticas e mecanismos de segurança devem interferir o mínimo possível, senão quase nada, com o utilizador, mas manter uma presença que seja notável para transmitir segurança no uso do Sistema de Informação, sem perturbar o funcionamento tradicional dos serviços. Características como a encriptação transparente das comunicações, regras de mudança de *passwords*, grupos de domínio ou de *AD (Active Directory*) onde são colocados perfis de utilizador com mais ou menos privilégios e gestão automática de sessão, são de elevada importância e criticidade.

O advento universal da informática globalizou a circulação da informação e a comunicação entre partes é realmente imediata. Esta verdade criou um paradoxo que em contraciclo, colocou a experiência do utilizador em primeiro lugar e a segurança em segundo durante algum tempo. Contudo, este tipo de tendências e facilidades que expõe e ameaçam a segurança da informação e dos sistemas informáticos, está em rápido e acelerado desuso e em intenso contrarrelógio para implementar e manter mecanismos que garantam que a informação.

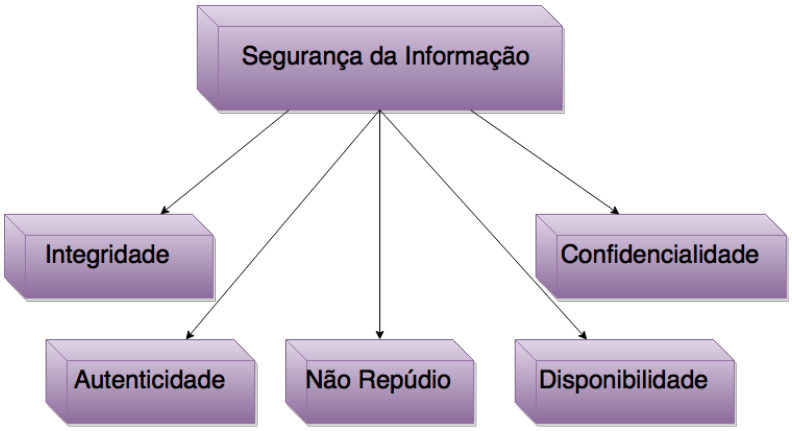

Figura 2 - Segurança da informação[17]

[17] Imagem elaborada pelo autor

Como se apresenta na figura anterior, a segurança da informação possui os seguintes princípios basilares:

- **Confidencialidade** – Disponibilização da informação apenas a indivíduos que têm autorização para ver a mesma;
- **Autenticidade** – Garantia que a informação é proveniente da fonte anunciada e que não foi alvo de modificações;
- **Integridade** – Garantir que a informação é verdadeira e livre de modificações não autorizadas;
- **Disponibilidade** – Manter a informação acessível sempre que esta é necessária;
- **Não repúdio** – Garantir que não existe a negação da autoria da transação de informação.

Os pilares que podem ser observados na imagem anterior, visam promover de segurança os sistemas de informação e seus utilizadores prevenindo algumas ameaças como as seguintes:

- **Revelação da informação** – Em casos de espionagem coletiva (*NSA Prism*);
- **Fraude** – Não reconhecimento da origem da informação, alteração da informação;
- **Interrupção** – Constrangimento na informação e modificações da informação;
- **Usurpação** – Modificação da informação e negação de serviço;
- **Modificação** – Alteração da mensagem em trânsito;
- **Repetição** – Repetição de operações já realizadas, sem autorização, de modo a obter o mesmo resultado;
- **Disfarce** – Apresentação de identidades falsas perante um determinado interlocutor;
- **Negação de serviço** – Ações que visam dificultar o normal funcionamento de um sistema;
- **Interceção** – Acesso não autorizado a uma mensagem, que, contudo, não é passível de ser alterada;
- **Repúdio** – Negação de participação numa determinada comunicação ou operação, quando efetivamente o fez.

Os tipos de ataques podem ser agrupados em duas classes distintas, de acordo com a metodologia utilizada: ativos e passivos, como se apresenta na figura seguinte.

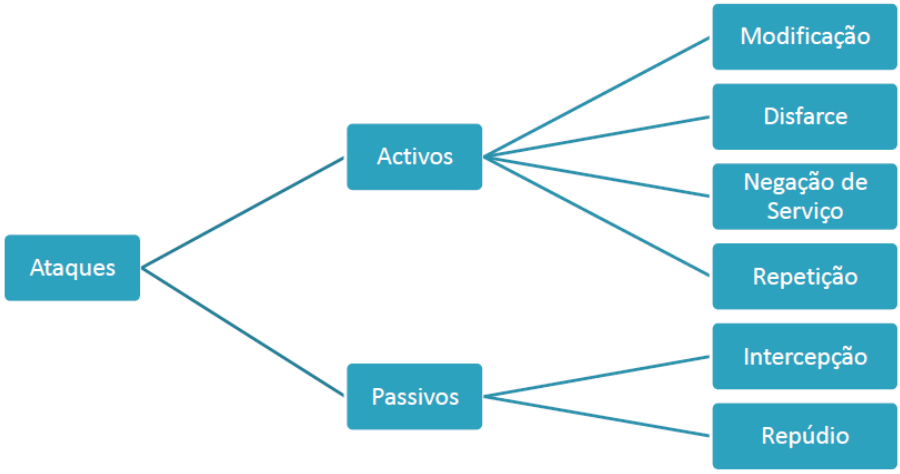

Figura 3 - Tipos de ataques, passivo e ativo[18]

Segundo André Zúquete [André Zúquete, 2014] a segurança de sistemas computacionais centra-se em três grandes eixos de acção: defesa contra falhas ou faltas previsíveis, defesa contra catástrofes (queda das torres do *World Trade Center* em Nova Iorque, em 2001) e defesa contra atividades não autorizadas. Embora fora do núcleo de âmbito da dissertação, mas *in extemis* dentro do mesmo, abordaremos sinteticamente a defesa contra falhas e a defesa contra catástrofes. O maior destaque é dado à defesa contra atividades não autorizadas.

A proteção contra catástrofes, como o nome o indica, consiste em criar sistemas e mecanismos que consigam garantir que o sistema ou os serviços desse sistema, continuam a servir em caso de uma inesperada falha física. Problemas ambientais como tremores de terra, incêndios, inundações, problemas políticos como greves e tumultos ou ataques de terrorismo, problemas materiais como a perda irrecuperável de informação, avarias em discos e erros de *backups*, embora pareçam ser improváveis, o mais certo é que aconteçam diariamente por todo o planeta.

Ao mais baixo nível, mantendo sistemas com partições em *RAID*[19], manter a redundância da informação, descentralização de sistemas, sistemas distribuídos com replicação através de *software,* como por exemplo o *Golden Gate*[20] da *Oracle* ao mais alto nível, a melhor forma de proteção contra catástrofes parte de um bom plano diretor informático e de um sistema

[18] Imagem elaborada pelo autor
[19] RAID – Redundat Array of Independent Disks
[20] Golden Gate – Software de replicação de dados. https://www.oracle.pt

computacional assente em regras de distribuição da informação e redundância triplicada (servidores físicos, servidores da *Cloud* privada e servidores em *Clouds* públicas não gratuitas [Nuno Coelho, 2012]).

A proteção contra falhas previsíveis consiste em reduzir ao máximo o dano que podem causar problemas de frequência constante ou maior. Embora não tão objetivas como no ponto anterior, as falhas previsíveis, consistem em coisas mais mundanas como falhas no fornecimento de energia elétrica, erros e bloqueios na execução de aplicativos ou sistemas operativos, falta de rede ou de ligação à *Web*, sistema em baixo ou simplesmente fontes de alimentação que avariam. Uma lista imensa de prováveis erros que diariamente podem interromper a disponibilidade de um sistema pode ser minimizada através de algumas medidas a conhecer:

- Sistemas *UPS* locais ou de grande escala para garantir a continuidade de energias aos sistemas;
- Sistemas de apoio computacional para garantir a resposta à carga dos S.O.;
- Acessos à rede *Web* por múltiplos operadores ou meios;
- Sistemas de rede com *firewall* centralizada, com rotas definidas para sistemas diferentes dentro de uma rede;
- Servidores com dupla fonte de alimentação.

As proteções contra atividades não autorizadas não são idênticas às analisadas anteriormente. Não ocorrem por fruto do acaso ou catástrofe, mas sim por meio de alguém, algures, que propositadamente testa um sistema computacional ou rede, com a intenção de obter ou interromper o fluxo normal de informação a quem esta informação pertence.

Contrariamente ao anterior, que assenta na estatística dos eventos ou erros, as atividades não autorizadas são perpetradas por entidades (*NSA, CIA, Anonymous),* indivíduos (*Hackers*).

É de salientar que nas organizações, muitos dos ataques ou furtos de informação são efetuados por elementos internos com privilégios acrescidos sem necessidade de se infiltrarem na rede. Embora as grandes organizações trabalhem com sistemas integrados da *Microsoft* e *Linux* que permitem criar grupos de utilizadores e de computadores, nas organizações mais pequenas e sem recursos, a tarefa de manter a segurança assenta muito na experiência do administrador de sistemas e na capacidade económica da organização para

investir em sistemas de permissão de acesso a recursos como a *Active Directory* [21] da *Microsoft*.

As atividades ilícitas encaixam-se em cinco princípios [André Zúquete, 2014]:

- Acesso à informação;
- Alteração da informação;
- Uso exagerado dos recursos informáticos;
- *DoS*[22] *Denial of Service*;
- Vandalismo.

Apresentam-se abaixo estes princípios com algum detalhe:

Acesso à informação: toda a informação que é restrita, confidencial, privada, sensível, intransmissível, guardada em sistemas privados, redes privadas, bases de dados privadas e outros sistemas análogos. Todos os dados privados que circulam assentes em rede públicas, *clouds* de propriedade de terceiros, *email* e chamadas telefónicas *VOIP*, são diariamente em todo o mundo objetivo de intrusão e desvio e por conseguinte devem ser alvo de proteção proativa e consente por parte dos legítimos donos da informação.

Alteração da informação: todas as ações que, de forma simulada ou não, alteram ou modificam, apagam ou escondem a informação de terceiros, em trânsito ou armazenadas.

Ações que alteram a informação são mais visíveis que o exemplo anterior, e como tal podem ser minimizadas as consequências.

Denial of Service: muito comum em servidores que prestam serviços *Web*, esta atividade consiste num ataque que visa a que, por exemplo, um *website* não esteja disponível para um utilizador. Contrariamente a uma invasão, este ataque prevê a sobrecarga de um determinado sistema para que este não responda a pedidos.

Segundo André Zuquete [André Zúquete, 2014], geralmente consistem em 2 métodos:

- Forçar o sistema alvo a fazer *reboot* (reiniciar) ou consumir recursos como memória ou processador impedindo que o sistema responda a pedidos;
- Obstruir o meio de acesso ou de comunicação entre clientes e servidores (*browser* e, por exemplo, servidores do Portal das Finanças).

Os ataques aparecem essencialmente sob três formas:

[21] Active Directory MS – Serviço de Directório no protocolo LDAP
[22] DoS – Denial Of Service – Negação de Serviço: https://www.us-cert.gov/ncas/tips/ST04-015

- Inundação – Envio de volume elevado de tráfego ao sistema alvo através de pacotes *UDP*[23] ou *ICMP*[24];
- Amplificação – Requisições forjadas para um grande número de máquinas ou endereço de IP de *broadcast*;
- Exploração de protocolos – Exploração de um protocolo a uso pelo sistema alvo. Os métodos mais frequentes são uso indevido de pacotes *TCP SYN* e *PUSH+ACK.*

Vandalismo: consiste na invasão de um sistema apenas com o motivo de destruir. *DoS* sem necessidade ou benefício objetivo. Este tipo de ameaça é muito comum numa classe de *hackers* (*crackers*) sem qualquer pudor informático. Mais à frente neste trabalho são analisados os ataques, as consequências e o método mais comum para os evitar.

Lamentavelmente, as organizações olham para a segurança como se de uma despesa *CAPEX* (*capital expenditure* ou despesas de capital ou investimento em bens de capital) ou *OPEX* (*operational expenditure* ou despesas, custos operacionais) se tratassem.

Na realidade, a aquisição de sistemas e peças para estes, licenciamento e melhorias são despesas *CAPEX* e todas as despesas inerentes à manutenção, segurança, formação de ativos especialistas são *OPEX*, mas e os custos que são inerentes à perda de informação ou recuperação da mesma? Porque é que nas organizações nunca é analisado objetivamente o custo da recuperação? Porque é que os utilizadores que perdem informação para entidades adversas não conseguem quantificar esse custo? No Médio Oriente, não conseguir ocultar eficientemente a localização ou o conteúdo informático, pode custar a vida a um ser humano. Onde seria correto colocar esta despesa? A resposta a estas questões é simples e complexa ao mesmo tempo. De uma forma simplista, pode-se dizer que optar por sistemas operativos muito comerciais e soluções de segurança chave na mão é deixar ao acaso elementos chave sobre o indivíduo. Ora, uma pessoa que não pense nestas questões está exposta ao alheio, algo que objetivamente várias organizações e o resultado prático deste trabalho tenciona evitar. A resposta complexa a estas questões entra no meio psicossocial da sociedade e das sociedades informatizadas e consequentemente extenso e complexo de expor.

[23] UDP – User Datagam Protocol
[24] ICMP – Internet Control Message Protocol

2.2.1 Normas e Padrões

Existem no mercado algumas ferramentas de metodologia que permitem balizar os comportamentos adequados e as normas de segurança informática. Estas podem ser adotadas por utilizadores ou entidades, a conhecer:

- *ITIL*
- *COBIT*
- *ISO* – 17799 (*ISO* 27001)
- *ISO* – 20000

ITIL (*Information technology Infrastructure Library)* são um conjunto de guias e boas práticas aplicadas à gestão de infraestruturas e sistemas de informação. Foi desenvolvido nos anos 80 pela *CCTA* (*Central Computer and Telecomunications Agency*). Atualmente esta entidade passou a designar-se de *Office for Government Commerce* (*OGC*) e sita no Reino Unido. O modelo *ITIL* promove a qualidade dos serviços das tecnologias de informação, orientados ao cliente. Lida com processos para a gestão das organizações das tecnologias de informação, e contempla um conjunto abrangente de processos e mecanismos de gestão, organizados por disciplinas com as quais uma organização pode fazer uma gestão tática e operacional com vista a alcançar um alinhamento com a estratégia de negócios dessa instituição. A evolução para o *ITIL* v2 (segunda versão) é a base da norma *BS*15000, que é um anexo da norma *ISO/IEC* 20000, que tem por objetivo a gestão da qualidade dos serviços de tecnologias de informação sobre as regras de *Plan, Do, Check* e *Act*.

COBIT, *Control Objectives for Information and related Technology*, é um guia de boas práticas para a gestão das tecnologias de informação. Sob gestão da *ISACA* (*Information Systems Audit and Control Association*), contempla um leque de recursos que servem de modelo de referência na gestão das Tecnologias de Informação. Inclui um sumário executivo, uma *framework*, objetivos de controlo, mapas de auditoria, ferramentas de implementação e principalmente um guia de métodos de gestão. O *COBIT* é independente das plataformas adotadas nas organizações, do tipo de negócio, valor, participação tecnológica e cadeia produtiva.

Atualmente está na versão 5 e é usado nas principais empresas de renome em Portugal, por exemplo, Sonae, Jerónimo Martins, ANA (Aeroportos de Portugal), entre outras.
Tem como modelos interrelacionados:

- **Eficácia** - Alcance de metas e resultados;
- **Efetividade** - Trabalha com a informação relevante para os processos de negócio, tempo, de forma correta, consistente e utilizável;
- **Eficiência** - Entrega de informação pelos melhores recursos;
- **Confidencialidade** - Proteção da informação;
- **Integridade** - Fidedignidade e totalidade da informação;
- **Disponibilidade** - Disponibilidade da informação de forma útil para ser usada;
- **Conformidade** - Coerência legal;
- **Confiabilidade** - Relaciona-se com a entrega da informação apropriada para posições de decisão.

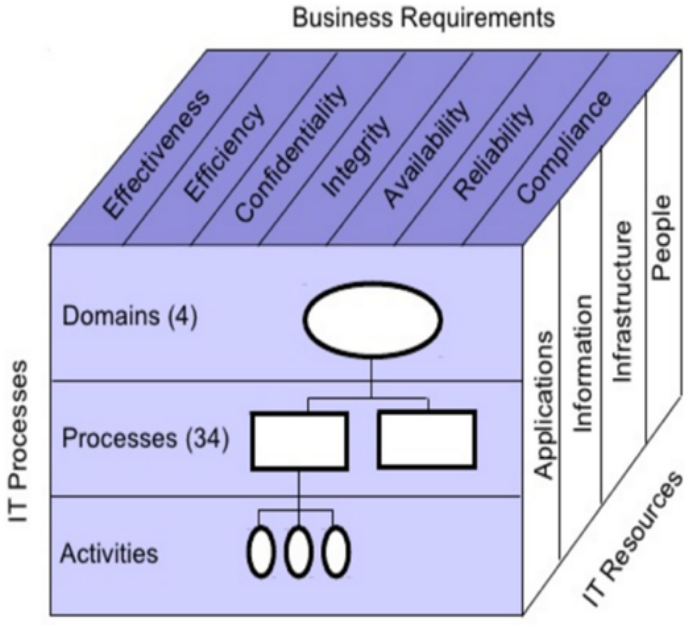

Figura 4 - Cubo de Cobit, dimensões e níveis [25]

*ISO*17799 é uma norma de segurança da informação revista em 2005 pela *ISO* e pela *IEC*. A versão original foi publicada em 2000, que por sua vez era uma cópia fiel do padrão britânico *BS* 7799-1:1999.

[25] Imagem obtida em - https://www.dropbox.com/s/2ay8i1eo053pmh3/Captura%20de%20tela%202015-10-24%2001.40.30.png?dl=0

Este documento fornece um conjunto de guias e boas práticas para a gestão de segurança de informação em sistemas informáticos.

A norma aborda dez grandes áreas relativas à segurança informática:

- Planeamento da prestação do serviço sem interrupções (*Business Continuity Planning);*
- Controlo de acesso a sistemas (*System Access Control*);
- Desenvolvimento de sistemas de manutenção (*System Development and Maintenance*);
- Segurança física e ambiental (*Physical and Environmental Security*);
- Conformidade (*Compliance*);
- Segurança de colaboradores (*Personnel Security*);
- Organização da segurança (*Secutity Organisation*);
- Gestão de computadores em rede (*Computer rand Network Managment*);
- Classificação e controlo de bens (*Asset Classification and Control*);
- Políticas de Segurança (Security Policy).

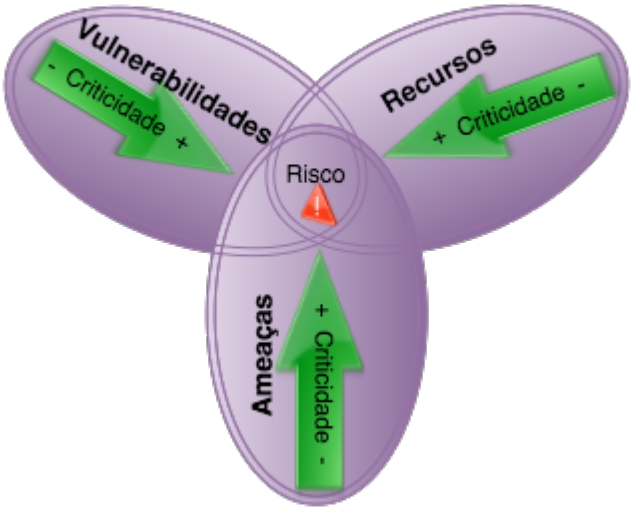

Figura 5 - *ISO* 17799 Grupo de Forças[26]

ISO – ISO/IEC 20000 é a primeira norma editada pela *ISO* (*International Organization for Standardization*) relativa à gestão da qualidade de serviços de tecnologia da informação. É a primeira norma mundial especificamente focada na gestão de serviços. Esta não concretiza o abrangimento das práticas da *ITIL*, embora esteja descrito na norma um conjunto de processos de gestão que estão alinhados com os processos definidos no *ITIL*. A *ISO*20000

[26] Imagem elaborada pelo autor

define as melhores práticas de gestão de serviços sustentadas pela *BS* 15000 (*British Standard)* e visa a compatibilidade com o *ITIL* (*Information Technology Infrastructure Library*).
A norma *ISO/IEC 20000* adota a metodologia *PDCA* (*Plan-Do-Check-Act*) para os processos de planeamento e implementação de serviços, que consistem de quatro fases distintas:

- ***Plan*** – Planeamento: estabelece os objetivos e processos necessários para a realização dos serviços com qualidade;
- ***Do*** – Fazer: implementa os processos estabelecidos no planeamento;
- ***Check*** – Avaliação: monitoriza e estabelece métricas para os processos que visam confirmar se estes estão a ser executados com qualidade;
- ***Act*** – Acão: inicia ações que visam a melhoria contínua dos processos e do resultado destes.

2.2.2 Políticas de segurança

As políticas de segurança providenciam um conjunto de regras e normas que devem ser adotadas e seguidas pelos utilizadores de recursos informáticos numa organização e espelham os objetivos de segurança que essa organização delineou como regra basilar de segurança. Estas políticas estabelecem detalhadamente as utilizações permitidas para os recursos e sistemas de informação e comunicação e as punições em caso de violação ou desrespeito das mesmas. Ao fornecer um enquadramento para a implementação dos mecanismos de segurança, definem determinados procedimentos que são necessários para uma segurança proativa e adequada, definindo métodos de auditoria à segurança e estabelecem um princípio para procedimentos legais na eventualidade de materializar uma ameaça ou ocorrência de um ataque.
Uma política de segurança informática deve ser técnica e plenamente exequível, definindo cabalmente as áreas de responsabilidade dos utilizadores, do suporte técnico e da gestão da organização. Deverá ainda ser suficientemente flexível, adaptando-se as alterações que venham a ser colocadas em prática pela organização.
As principais regras para a definição de políticas de segurança eficazes deverão:

- Ser facilmente acessíveis a todos os membros da organização;
- Estabelecer e definir os objetivos de segurança;
- Determinar concretamente todos os aspetos da sua abrangência;

- Definir a posição da organização em cada questão;
- Justificar as opções tomadas;
- Definir as circunstâncias de aplicação individual das regras;
- Definir o âmbito de ação dos diversos agentes da organização;
- Delinear as consequências de não cumprimentos das regras estabelecidas;
- Definir o nível de privacidade garantido aos utilizadores;
- Identificar os contactos para esclarecimentos de questões dúbias;
- Definir o tratamento das situações omissas.

O documento que define a política de segurança deverá excluir todos os aspetos técnicos de implementação dos mecanismos de segurança, pois cada implementação pode variar ao longo do tempo. Adicionalmente, este tem obrigatoriamente de ser um documento sucinto e de fácil leitura e compreensão.

É essencial que seja prestada especial atenção aos aspetos e procedimentos para que todas e quaisquer ações relevantes sejam mantidas em histórico, de modo a possibilitar a realização de auditorias de segurança. Outros fatores como o registo e certificação de todo o parque informático e respetivo *software* em utilização na rede e a realização de backups, são também de grande importância.

Algumas normas definem aspetos que devem ser levados em consideração ao elaborar as políticas de segurança. Entre essas normas estão a *ISO*17799 e a *ISO*27001 já analisadas anteriormente.

Um dos maiores problemas de segurança nas organizações é a falta de consciência por parte dos agentes dos agentes ativos dessa organização, das ameaças a que os sistemas e redes estão sujeitos. A política de segurança deverá alertar de forma plausível e objetiva todos os utilizadores para as questões de se segurança. Essa atitude deverá ser complementada com ações adequadas no terreno ao nível da segurança. É fundamental ter em mente que a melhor atitude em termos de segurança é sempre um compromisso entre o razoável e a paranóia.

2.2.3 Ferramentas de segurança informática e de acesso a sistemas

Todos os sistemas informáticos e todos os sistemas de gestão de sistemas de informação, manual ou não, necessitam de componentes ou interfaces de acesso para utilizadores (clientes) e para administradores. Sejam estes via *browser* em sistemas de alto nível, ou como

a consola de gestão de servidores *Webmin*[27], sejam estes por consola direta *SSH*[28], ou através de outras aplicações, todos possuem um acesso específico tendo como a porta de entrada de maior importância e possível dano, o acesso de administrador. Como boa prática, os acessos de administrador devem possuir um protocolo de segurança, como por exemplo o *Kerberos*[29]. Este protocolo é muito usual em sistemas *Apache* (com módulo de *mod_auth_kerb*), *Mac OS* (sistema operativo da Apple), *OpenSSH*[30], *SAMBA* (protocolo de partilha de ficheiros em *Linux*) e sistemas *Java* a partir da versão 1.4.2.

Manter seguros e encriptados estes acessos e a informação que através deste tipo de meio circula é essencial.

2.2.3.1 SSH

O *SSH* é um protocolo de ligação remota segura e de serviços de rede seguros sobre redes inseguras. Este consiste em três componentes de relevo:

- **A Transport Layer Protocol** providencia autenticação de servidor, confidencialidade e integridade e opcionalmente compressão. A camada de transporte tipicamente corre sobre ligações *TCP/IP* mas pode ser usada sobre qualquer fluxo (*stream*) de dados seguros;
- **O User Authentication Protocol***,* que autentica o cliente com o servidor (*client-side to server*). Corre sobre o *Transport Layer Protocol*;
- **O Connection Protocol** multiplica (multiplexes) o túnel encriptado em vários canais lógicos. Corre sobre o *User Authentication protocol*.

Para que um utilizador use convenientemente o protocolo *SSH*, necessita de uma aplicação cliente, como por exemplo o *Putty*. Esta aplicação congrega todo o potencial do protocolo *SSH*.

[27] Webmin – Sistema de gestão de servidores por browser, https://pt.wikipedia.org/wiki/Webmin
[28] SSH – Secure Shell, https://pt.wikipedia.org/wiki/SSH
[29] Kerberos – Protocolo de Autenticação de tripla confiança, https://pt.wikipedia.org/wiki/Kerberos
[30] OpenSSH - Conjunto de programas que facultam criptografia em sessões de comunicações numa rede de computadores usando o protocolo SSH

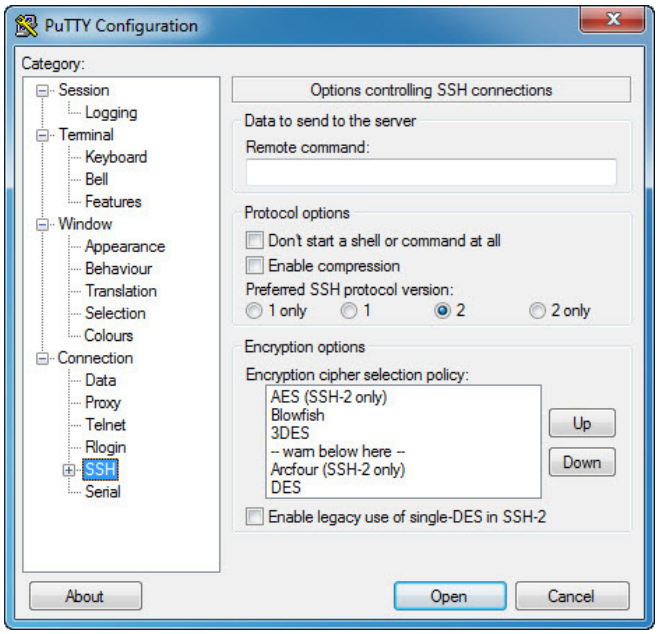

Figura 6 - Aspeto da aplicação cliente SSH Putty[31]

Na imagem anterior, pode-se observar o aspeto da janela de comunicação entre o *Putty* e o seu utilizador. O cliente (aplicação) envia um pedido de serviço quando uma ligação segura estiver estabelecida. Um segundo pedido de serviço é enviado após o utilizador ter completado o processo de autenticação, permitindo que este consiga coabitar com os protocolos descritos anteriormente.

2.2.3.2 VPN

O conceito de rede virtual privada (*VPN*) é hoje em dia usado para identificar diversas soluções de comunicação segura. A *VPN* é uma extensão segura de uma rede privada sobre uma rede insegura ou pública como a *Web*. Regulamentadas pelo consórcio de fabricantes *VPNC* (*VPN Consortium*), as *VPN* seguras garantem que a segurança dos dados entre o emissor e o recetor é independente da honestidade das entidades de acesso e encaminhamento de informação, sendo uma tecnologia amplamente usada, quer em meios empresariais quer domésticos. Uma das maiores redes seguras do mundo, a rede *Tor*, é uma rede *VPN*. Existem também *VPN* que são configuradas localmente através de *software* ou *hardware* e existem redes *VPN* globais que são comercializadas como serviços para que os seus utentes naveguem na *Web*, alegadamente, de forma segura a troco de uma renda.

De certa forma, uma *VPN* atua como um cabo de rede virtual, ou seja, não existe uma ligação física. Contudo, como este cabo virtual estende-se pela rede pública que é insegura, as *VPN*

[31] Imagem elaborada pelo autor

são dotadas de mecanismos de segurança que as permite ser efetivamente seguras. As normas mais comuns são *IPSEC* e *SSL*. O *IPSec* é uma extensão de segurança do protocolo *IP* concebida para o *IPv6* e aplicada ao *IPv4*. O *SSL* é um protocolo criado pela *Netscape*[32] para introduzir segurança no em comunicações *HTTP*.

Os seguintes requisitos fazem parte das VPN:

- Todo o tráfego que circula dentro de uma *VPN* tem de estar devidamente encriptado (cifrado) de forma a garantir eficientemente a confidencialidade perante terceiros, autenticado para impedir a sua alteração. A manipulação criptográfica deve ser efetuada com recurso a uma ou mais chaves de sessão, estas chaves deverão ser simétricas, aleatórias e plenamente confidenciais;
- As propriedades de segurança de uma *VPN*, sobretudo os identificadores de sessão, os algoritmos e chaves de sessão que vão ser usados, têm de estar obrigatoriamente combinados entre os extremos que a vão explorar, por outras palavras, as chaves de segurança têm de ser do cabal conhecimento do servidor e do cliente, os quais devem ser autenticados;
- Quaisquer elementos externos à conceção *VPN* não conseguirão afetar os atributos de segurança. Os possíveis atacantes não conseguirão alterar quaisquer atributos, interferir com parâmetros criptográficos, nomeadamente as chaves de cifra que são usadas na conceção *VPN*.

O *IP-tunneling* (encaminhamento de dados por túnel *VPN*) é uma técnica de encaminhamento que se utiliza para encapsular dados em pacotes dentro de outros pacotes. Por exemplo, duas Escolas Superiores do IPP[33], o Instituto Superior de Contabilidade e o Instituto Superior de Engenharia Informática, partilham recursos para a pós-graduação em Sistemas Informáticos Empresariais e é necessário que os seus alunos acedam a recursos que estão em servidores do ISEP (Instituto superior de engenharia do Porto). O ISCAP (Instituto Superior de Contabilidade e Administração do Porto) tem a rede configurada na gama de endereços 192.168.1.*, enquanto o *ISEP* usa a gama de endereço 192.168.0.*. Em cada uma das escolas existe um *SI Linux* que funciona como *router* ligado à *Web* (meio público). Quando um dos *routers* recebe um pacote destinado à sub-rede de uma das escolas, este será encriptado e encapsulado dentro de outro pacote que será enviado para o *router* da escola destino.

[32] Netscape foi uma empresa de serviços de computadores nos EUA, mais conhecido pelo seu navegador web, dando lugar à Mozilla e à AOL.
[33] Instituto Politécnico do Porto

Por sua vez, a escola destino recebe o pacote e desencripta o seu conteúdo, obtendo assim o pacote interior com a mensagem normal, enviando-a para o endereço destino dentro da rede local.

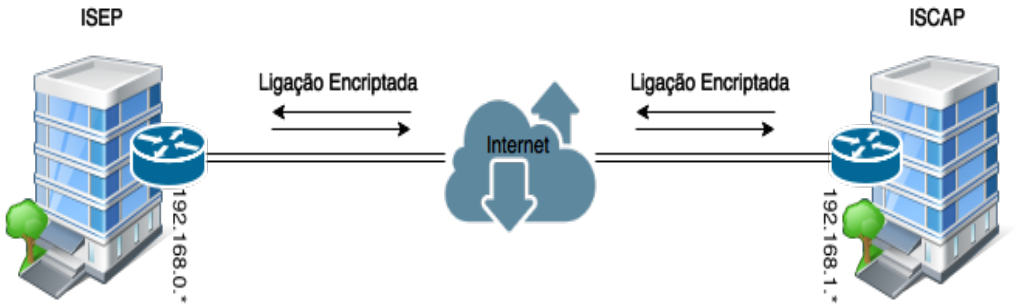

Figura 7 - Ligação entre a VPN ISCAP – VPN ISEP[34]

Do ponto de vista dos restantes computadores das duas redes locais, tudo se passa como se fosse uma rede só. Na verdade, nem é necessário aplicar configurações adicionais bastando definir o endereço no *router*. As *VPN* permitem ainda passar outros protocolos para além do *IP*, como por exemplo voz sobre *IP* (*VOIP* ou *Voice Over IP*).

Do ponto de vista da segurança, as *VPN* são extremamente seguras podendo evitar ataques comuns de *Men-In-The-Middle* desde que um *EndPoint* (ponto de extermidade) tenha conhecimento do outro através de sistemas *public-key-infrastructure*[35]. Em exemplo *SSH*, o conhecimento da existência do *EndPoint* vem de contactos prévios em que o cliente se recorda da chave pública do servidor e recusa-se a prosseguir caso a chave não seja a mesma. Caso exista tentativa de alteração ou escuta do conteúdo desse túnel de dados, a *VPN* desfaz-se e forma-se logo a seguir por outra rota.

Cuidados VPN:

Existem serviços de *VPN* vendidos por empresas e com particular incidência em *VPN* de *Cloud*. Ao confiar o seu tráfego a serviços de *VPN* de terceiros, está-se a confiar plenamente nesse terceiro, o que não impede de forma alguma que este analise o seu conteúdo. *VPN* de terceiros são muito úteis para ultrapassar questões de censura, como por exemplo a Grande *Firewall* da China.

[34] Imagem elaborada pelo autor

[35] Public Key Infrastructure – Infraestrutura de chaves publicas, https://pt.wikipedia.org/wiki/Infraestrutura_de_Chaves_P%C3%BAblicas

2.2.3.3 Firewall

Quando se conectam sistemas com o mundo exterior, deve-se ser zeloso com todas as questões relacionadas com segurança. Um sistema *firewall* controla com grande precisão e exatidão todo o tráfego e quem tem acesso a cada porto *IP* de um determinado sistema.

A *firewall* é um dispositivo, um serviço de *software* presente nos sistemas operativos ou um *software* que determina a política de controlo de acesso a, ou, entre redes, contendo as seguintes características:

- Todo o tráfego de entrada e saída deve passar pela *firewall*;
- Unicamente tráfego de dados permitido através de políticas de segurança local, pode passar a *firewall* sem ser descartado (*droped*);
- A *firewall* tem de ser imune a penetrações.

No *Linux,* por exemplo, existem três tipos de implementação de *firewalls*: *Ipfwadm, Ipchains* e *Iptables.*

O primeiro exemplo foi usado e implementado para *Linux Kernel* 2.0. O segundo, o *ipchains,* foi disponibilizado no *Kernel* 2.2 e tinha já características únicas que o anterior não possuía, nomeadamente *QoS* (*quality of service* ou qualidade de serviço), um sistema em árvore, ao contrário do linear disponível no primeiro exemplo. Flexibilidade na configuração, negação de regras, por exemplo, descartar qualquer pacote que saia e que não venha de um *IP* registado para garantir que não foi origem ou fonte de um ataque *spoofing* são outras das suas características. Para além do anterior, consegue filtrar qualquer protocolo de *IP* e não só *TCP, UDP* e *ICMP*.

O terceiro exemplo é completo e poderoso, foi disponibilizado no *Kernel* 2.4 e tem sido mantido até às versões mais atuais. Ao contrário do exemplo anterior, o *iptables* suporta os protocolos I*Pv4, IPv6, True 1:1 e 1:Many NAT*, a funcionalidade *PORTFW* (encaminhamento de portas) nativamente, e todas as que os anteriores exemplos suportam.

Tabela 2 - Funcionalidade de iptables

Suporte aos protocolos *TCP, UDP, ICMP*
Especificar portas de origem e de destino
Suporte a módulos externos como o *FTP* e o *IRC*
Suporte de um número ilimitado de regras por *chains* (cadeias)
É possível criar regras de proteção contra ataques diversos
Suporte de roteamento de pacotes e redireccionamento de portas
Suporte a vários tipos de *NAT*, como o *SNAT* e *DNAT* e mascaramento
Priorização de tráfego para determinados tipos de pacotes
Suporte a *IPv6*, através do programa *ip6tables*

Na tabela anterior pode-se observar as características do *iptables*. Estas podem ser ajustadas através da consola, que se pode ver na figura 6, ou por linha de comando com recurso a *scripts*.

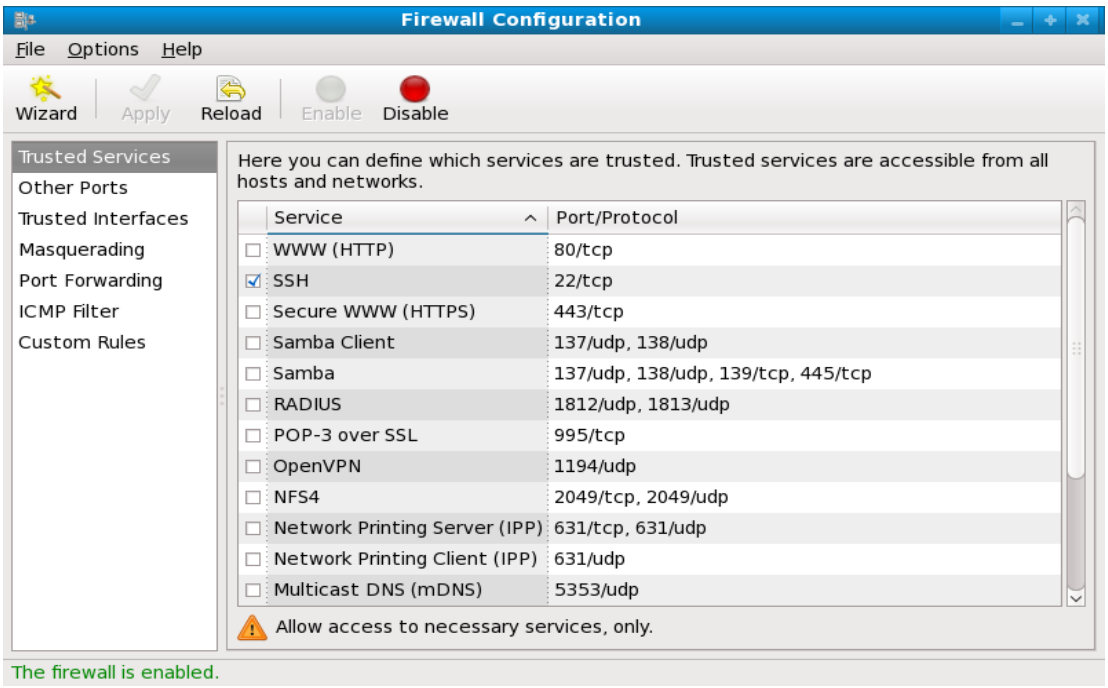

Figura 8 - Painel de controlo da *Firewall* em *Linux Fedora*[36]

A *firewall* opera como um filtro para rejeitar pacotes de dados, de acordo com o endereço de origem, endereço de destino e o tipo de serviços usados. Os pacotes podem ser filtrados em três situações específicas:

- ***Input*** – quando entram no sistema;
- ***Output*** – quando saem do sistema;
- ***Foreward*** – quando são reenviados de uma *interface* de rede para outra.

Em cada caso de entrada de pacotes, pode-se definir uma cadeia de regras que serão aplicadas sequencialmente a cada pacote. Os pacotes podem ser aceites, rejeitados com aviso do emissor ou rejeitados sem qualquer aviso.

[36] Imagem recolhida em https://www.fedora.com

As regras do *iptables* são definidas pelas operações que se podem observar na tabela que se segue:

Tabela 3 - Operações do iptables

-A	Acrescenta uma nova regra existentes.
-D	Para apagar uma regra
-L	Listar as regras existentes
-F	Apagar uma cadeia de regras
-I	Inserir uma nova regra, numa posição definida
-R	Substituir uma regra existente
-C	Para verificar regras existentes
-Z	Limpar contadores de pacotes
-N	Criar uma nova cadeia de regras
-X	Eliminar uma cadeia de regras

As *firewalls* devem ser encaradas como um dos mecanismos de segurança de uma rede e não como *o* mecanismo de segurança da rede. Para além da utilização de *firewall*, outros mecanismos de segurança devem ser usados mesmo dentro de uma rede protegida. Como se pôde analisar anteriormente, uma parte considerável dos ataques têm origem dentro do sistema, pelo que uma *firewall* torna-se ineficaz contra esse tipo de ataques, que têm de ser evitados com recurso a mecanismos de autenticação, controlo de acessos e confidencialidade atuando dentro da rede.

2.2.3.4 Criptologia e Criptografia

Da criptologia, a criptografia que origina do grego *kryptós* cujo significado é escondido, e *gráphein* que significa escrever, é uma ciência informática que estuda os métodos, mecanismos e algoritmos pelos quais uma mensagem é transformada da sua forma original para uma irreconhecível a não ser que se conheça a chave que ajudará a tornar percetível a mensagem. A criptoanálise é o método de estudo que visa obter a mensagem ou a informação da mensagem criptografada sem que se possua a chave que a descodifica.
Os métodos clássicos da criptoanálise são os seguintes e distribuído de acordo com a figura 9:

- **Força bruta** – Método que consiste em testar todas as combinações possíveis de carateres até encontrar a chave que permitirá a descodificação da mensagem;

- **Análise de frequências** – Método que se baseia no facto de em algumas linguagens, certos caracteres ou combinações ocorrerem mais frequentemente.

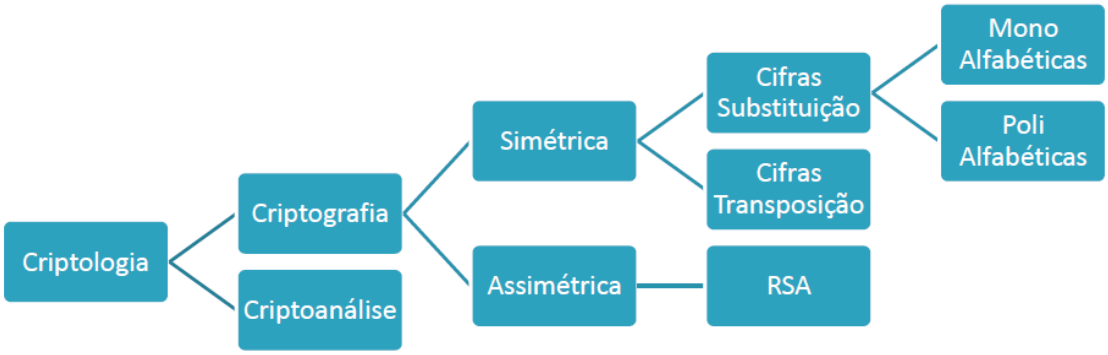

Figura 9 - Árvore de Criptologia[37]

O objetivo principal da criptografia é garantir que a troca de dados entre intervenientes, emissores e recetores, satisfazem os princípios basilares de segurança. Para que tal seja possível, o uso de cifras é a chave (passando a redundância). A cifra é o algoritmo criptográfico, função matemática injetiva que efetua transformações entre o texto original e o texto codificado (cifrado) e vice-versa.

O algoritmo de cifra é essencialmente um conjunto de procedimentos em que se fundamentam as técnicas criptográficas. As chaves destes algoritmos fornecem informação para aplicar esses procedimentos de uma forma singular, sendo conhecidas três tipos de chaves: a secreta, a pública e a privada. A chave secreta é também conhecida por ser a chave simétrica; por outro lado, a chave pública também é designada de assimétrica.

Na utilização de uma chave simétrica para codificar ou decodificar uma mensagem, o emissor e o recetor necessitam de escolher uma cifra e uma chave, sendo que o emissor cifra a mensagem e o recetor decifra a mesma. O algoritmo define o modelo genérico de transformação dos dados e a chave é um parâmetro do algoritmo que permite variar o seu comportamento de forma complexa.

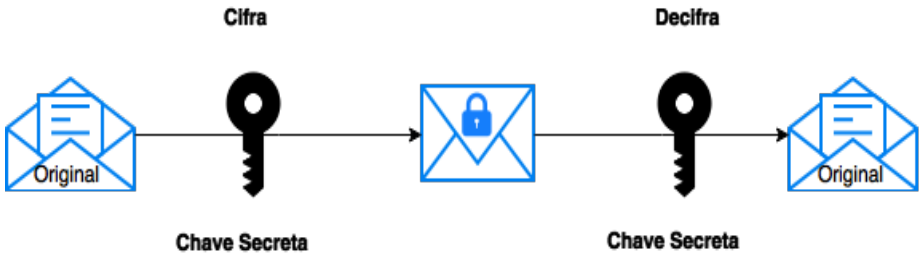

Figura 10 - Método de cifrar Mensagem[38]

[37] Imagem elaborada pelo autor

Na criptografia clássica, as cifras de substituição e transposição eram muito usadas no meio militar. As cifras de substituição consistem em substituir cada letra de uma palavra por uma letra diferente de acordo com o esquema predefinido; a Cifra de Cesar é dos exemplos mais conhecidos. A de transposição consiste numa chave acordada entre emissor e recetor.
A encriptação é sustentada em ciência criptográfica e a maior parte dos sistemas de encriptação são baseados em cinco categorias possíveis:

- **Encriptação por chaves simétricas** – Cada computador possui uma chave secreta que pode ser utilizada para encriptar informação antes de esta ser enviada para outro computador. O computador recetor utiliza a mesma chave para desencriptar a informação. As chaves simétricas implicam que se saiba quais são os computadores que vão efetuar a comunicação para que possa instalar uma chave em cada um;
- **Encriptação por chaves públicas –** Utiliza-se uma combinação de uma chave privada e uma chave pública. O emissor utiliza a chave pública do destinatário (recetor) para encriptar a mensagem. A mensagem encriptada é enviada para o destinatário para que este com recurso à sua chave privada correspondente para desencriptar a mensagem recebida. Este processo garante a confidencialidade da mensagem enviada, pois apenas o destinatário possui a chave privada correspondente. Desta forma, o remetente não consegue desencriptar a mensagem desde que tenha recorrido ao uso da chave pública do destinatário;
- **Chaves públicas *SSL* –** Consistem num popular método de encriptação por chaves públicas através de protocolo *Secure Sockets Layer*;
- **Chaves públicas e simétricas –** A encriptação por chaves públicas obriga a elevados recursos computacionais pois a maior parte dos sistemas usam uma combinação de chaves públicas e de chaves simétricas. Ao iniciar uma sessão segura, um computador cria uma chave simétrica e envia-a para o outro computador utilizando encriptação por chaves públicas. Depois os dois computadores podem comunicar utilizando encriptação por chaves simétricas que é menos exigente. Quando a sessão de comunicação terminar, cada computador "elimina" a chave simétrica utilizada nessa sessão. Quaisquer sessões adicionais requerem a criação de uma nova chave simétrica;
- **Infraestrutura de Chave Publica (*PKI*) –** A infraestrutura de chave pública possibilita aos utilizadores de uma rede pública "insegura", como a *Web*, trocar informação e

[38] Imagem elaborada pelo autor

dados de uma forma privada e segura. Consiste no uso de um par de chaves (uma privada e a outra pública) de encriptação que são obtidas e partilhadas através de uma autoridade de confiança, também denominada de entidade certificadora (*certificate authority*). A infraestrutura de chaves públicas disponibiliza um certificado digital que pode identificar um indivíduo ou uma organização, contendo no mínimo a seguinte informação:

- Chave pública do dono do certificado;
- Nome do dono do certificado;
- Data de expiração do certificado;
- Número de série do certificado;
- Nome da organização que emitiu o certificado;
- Assinatura digital da organização que emitiu o certificado.

2.3 Ameaças

Segundo Paul O'Day no *Journal of Education* da Pacific University [Paul O'Day, 2013], o Governo Norte-americano monitoriza a *Web* desde o seu aparecimento. A sua génese militar coloca as instituições governamentais num lugar privilegiado em relação às demais. O que não era espectável inicialmente, é agora difícil de controlar. Os cérebros académicos e científicos diariamente movimentam o xadrez técnico numa constante fuga-perseguição. Mentes brilhantes como Steve Wozniak, Bill Gates, Tim Berners Lee, James Gosling, Linus Torvalds, Richard Stallman, Artur C Clarke, Ted Shirley, Martha Lane Fox e muito muitos outros, pesquisam e influenciam constantemente o mundo e as novas gerações numa contenda diária entre a liberdade e *software* de qualidade, e o controlo de massas. Isto cria efetivamente grandes dificuldades a quem preconiza a violação da privacidade.

O modo mais eficaz para comprometer a segurança é a escuta e a penetração aos *ISP* antes que os dados cheguem ao computador de destino. Se as comunicações não forem encriptadas, ou mesmo que as conexões o sejam, conseguem descobrir o local, o conteúdo, informações únicas sobre o computador e acima de tudo, com a ligação e cruzamentos de dados, saber quem é especificamente o utilizador [Fabio Locati, 2015]. Não pode ser esquecido nem negado que muitos dados circulam encriptados, mas também é conhecida a promiscuidade entre as grandes empresas de tecnologia como o *Facebook* e a *Google*, e desta forma contornar as questões mais técnicas como encriptação.

Até há pouco tempo não se sabia que a *NSA* espionava os internautas a nível nacional e internacional. Através da imprensa publicitavam que as plataformas que disponham não violavam a privacidade de ninguém, algo que Edward Snowden desmentiu categoricamente e com suporte documental (58.000 documentos classificados e secretos), alertando o mundo para esta sombria realidade. Usou jornais diários e o *Website Wikileaks*, tornando-se uma pessoa procurada em todo o mundo estando radicado na Rússia para evitar a justiça dos Estados Unidos, onde com certeza seria preso perpetuamente ou condenado à morte por traição.

Acima dos programas e das entidades, existe o sempre atento "amigo do alheio". Indivíduos que se dedicam a explorarem sistemas de informação com vários tipos de intuitos, uns inócuos, outros nem tanto. Existe uma extensa classe de profissionais desse campo, como se poderá verificar mais adiante.

2.3.1 O PRISM

Confirmando as suspeitas iniciais Mark Klein (antigo engenheiro de telecomunicações da operadora telefónica AT&T), [David Kravets, 2013], [Nancy Lind, 2015], [James Bamford, 2013], sobre a existência de um programa que vigiava e analisava as comunicações telefónicas diretamente nas empresas de telecomunicações, foi reconhecido que a *NSA* o faz através do *Prism* [Charlie Savage, 2013]. Este nasceu em 2007 sob a lei *Protect America Act* sob égide do Presidente dos Estados Unidos da America à altura. A existência do *Prism* é reconhecida pelo governo norte-americano desde que iniciaram as inquirições por parte do gabinete *Freedom of Information Office* [NSA, 2013].

Segundo Elliot Cohen [Elliot Cohen, 2014] e Bruce Schneider [Bruce Schneider, 2015], o *Prism* é uma ferramenta que permite contornar uma das maiores dificuldades de quem se dedica a estudar e analisar o tráfego que circula em pacotes. Como cada vez mais a encriptação é usada, a técnica *Deep Packet Inspection* (*DPI*) torna-se obsoleta. O *DPI* consiste na filtragem do conteúdo e *header* de um pacote de dados sobre em trânsito n*a Web*. Por outras palavras, permite saber quem enviou, quem recebeu e o que contém num determinado pacote de dados. Se estes dados vierem encriptados, isso não significa que o *DPI* seja inútil, apenas quer dizer que serão necessárias ferramentas adicionais.

Figura 11 - O logotipo do PRISM[39]

Como sistema clandestino de vigilância, o Prism tem a sua utilidade. Segundo Byron Acohido [Byron Acohido, 2013], o presidente Obama aludiu que esta tecnologia ajudou a capturar inúmeros terroristas.

Segundo Andrew Clements [Andrew Clements, 2014], o *Prism* é o nome de código para a iniciativa de recolha de dados *SIGAD US-984XN*, foi revelada mundialmente em abril de 2014 pelo Jornal *Guardian*, suportada documentalmente com dados recolhidos pelo analista de sistemas Eduard Snowden. A prova documental era composta por 41 diapositivos entre 58.000 documentos, que espelhavam como funciona o sistema e como recolhia dados, criando grande confusão a nível mundial, sendo reconhecido pelo governo americano e mundialmente, com algumas exceções, como factos e uma ferramenta verdadeira.

Este sistema recolhe dados dos servidores das oito principais empresas de serviços *Web* americanas, concomitantemente também de relevo mundial. Estas organizações não admitiram em comunicados que facultavam os dados para análise, contrariando as revelações e os documentos apresentados por Snowden. As empresas são a *Microsoft*, *Google*, *Facebook*, *Yhaoo*, *Apple*, *Youtube*, *AOL*, *Paltalk* e Skype. Segundo Frederic Lardinois [Frederic Lardinois, 2013] estas organizações, apesar de nas suas declarações não negaram categoricamente o envolvimento, alegando que fornecem dados avulsos a pedido rogatório legal, independentemente destas declarações, apressaram-se a aplicar medidas de encriptação de todos os dados que circulam nas suas redes.

[39] Imagem recolhida em - https://en.wikipedia.org/wiki/PRISM_(surveillance_program)#/media/File:PRISM_logo_(PNG).png

O *Prism* está focado maioritariamente no território americano, enquanto a versão *Muscular* faz o mesmo globalmente.

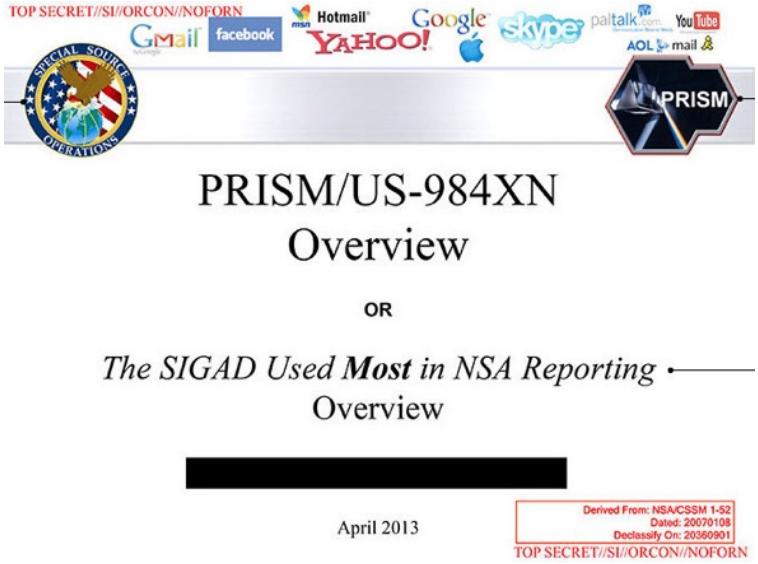

Figura 12 - Diapositivo sobre PRISM disponibilizado por Eduard Snowden [40]

2.3.1.1 Modus Operandi

Imagine-se um cenário em que um analista de sistemas efetua uma pesquisa a partir de uma determinada consola, a partir de qualquer ponto geográfico. Segundo [Julien Assange, 2013], o sistema que coleta dados das principais empresas mundiais do ramo tecnológico guarda esta informação num repositório de fácil acesso e onde pode proceder a análises de complexa estatística preditiva, fazendo combinações de perfis e informação, criando relatórios de conteúdo provado, de acordo com o que consta nas bases de dados. Segundo as empresas envolvidas, os dados são facultados via judicial, mas de acordo com informações providenciadas à *Wikileaks* por Edward Snowden [Julien Assange, 2013], o sistema tem ligações diretas sem que estas organizações os controlem, nada conseguindo fazer para impedir a fuga de elementos. Ainda não existem estudos que mostrem o método de recolha destes elementos, se são livremente ou facultados ou recolhidos via intrusão. Snowden indicou à imprensa que são fornecidos automática e conscientemente, através de um método específico e unilateral.

[40] Imagem recolhida em - https://nsa.gov1.info/surveillance/

Segundo Gianluca Mezzofiore, do *Internacional Business Times* [Gianluca Mezzofiori, 2013], o *Prism* tem acesso a bases de dados diretas das entidades anteriormente mencionadas, daí obtendo o que quiser.

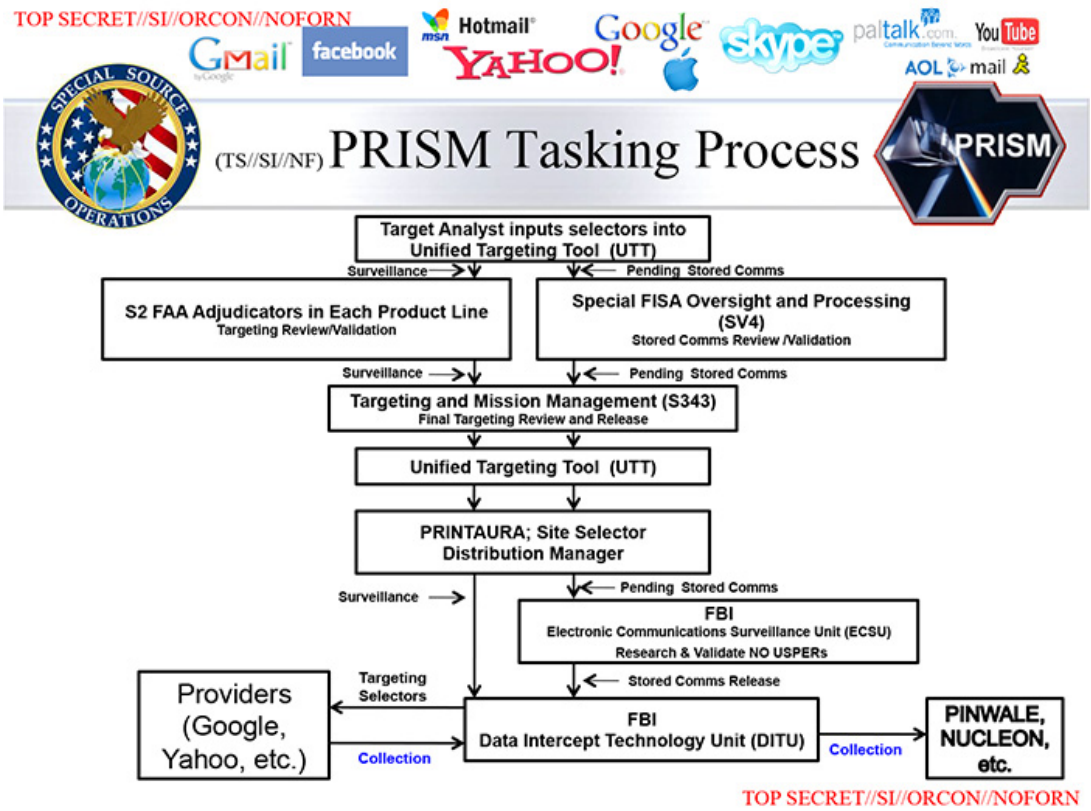

Figura 13 - Workflow de análise aos dados [41]

De acordo com Andrew Clements [Andrew Clements, 2014], professor na *Faculty of Information* da Universidade de Toronto, o Prism permite analisar o comportamento de pessoas através do que falam, escrevem, participam e observam na *Web*. Segundo um trabalho académico deste *PHD* em Ciências da Computação [University of Toronto, 2015], as grandes cidades têm concentradores de tráfego gerido por *ISPs* e empresas a quem estes arrendam infraestruturas e serviços, que não são regularmente mantidos e estando expostos a "escutas" em qualquer ponto geográfico da rede, revelando mais de 95% do tráfego doméstico (local). A *NSA* é perita em intrusão de redes e estruturas de dados, usando este método legal de escutas sem mandato judicial, entrando nos SI e redes sem que, por exemplo, e neste caso meramente especulativo, Meo consiga "notar" essa ligação não autorizada.

[41] Imagem recolhida em - https://nsa.gov1.info/surveillance/

Usando a ferramenta *IXMaps*[42] é simples perceber por onde andam os pacotes de tráfego que emitimos via *router* e onde estes provavelmente são capturados.

O *Prism* recolhe diretamente onze tipos de dados electrónicos, a conhecer:

- *Chat*;
- Correio electrónico;
- Transferência de ficheiros;
- Comunicações *VOIP;*
- Dados de *login* e respetivos *ID's*;
- Metadados;
- Fotos;
- *Social networking*;
- Dados armazenados;
- Vídeo;
- Videoconferências.

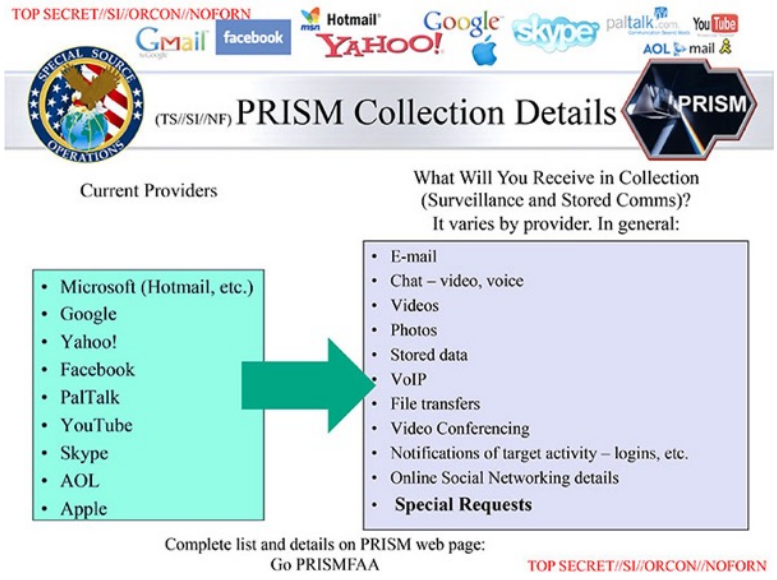

Figura 14 - Informação revelada ao PRISM [43]

Tendo em consideração os grandes volumes de dados, pressupõe-se que se usem técnicas de *BIG DATA* para trabalhar esta quantidade de informação, com recursos a sistemas de *Machine Learning*[44], *Data Mining*[45] e tratados com algoritmos preditivos (*Predictive Analytics*). Estas

[42] http://ixmaps.ca

[43] Imagem recolhida em - https://nsa.gov1.info/surveillance/

[44] Machine Learning é um subcampo da inteligência artificial e consiste no desenvolvimento de algoritmos que permitem a computadores aprender a lidar e a tratar melhor com grandes volumes de de dados e informação

tecnologias e ferramentas permitem classificar e caracterizar informação, permitindo criar rapidamente perfis de indivíduos, e expondo todo o seu uso habitual da *Web*, com quem falam, que dados enviam entre si, a sua localização e a localização dos interlocutores. Segundo Barton Gellman [Barton Gellman and Laura Poitras, 2013] jornalistas do *Washington Post*, estes perfis são, em mais de 50% dos casos, cidadãos de origem estrangeira e residente nos Estados Unidos e com relações fora do país, maioritariamente mediterrânicos e asiáticos.

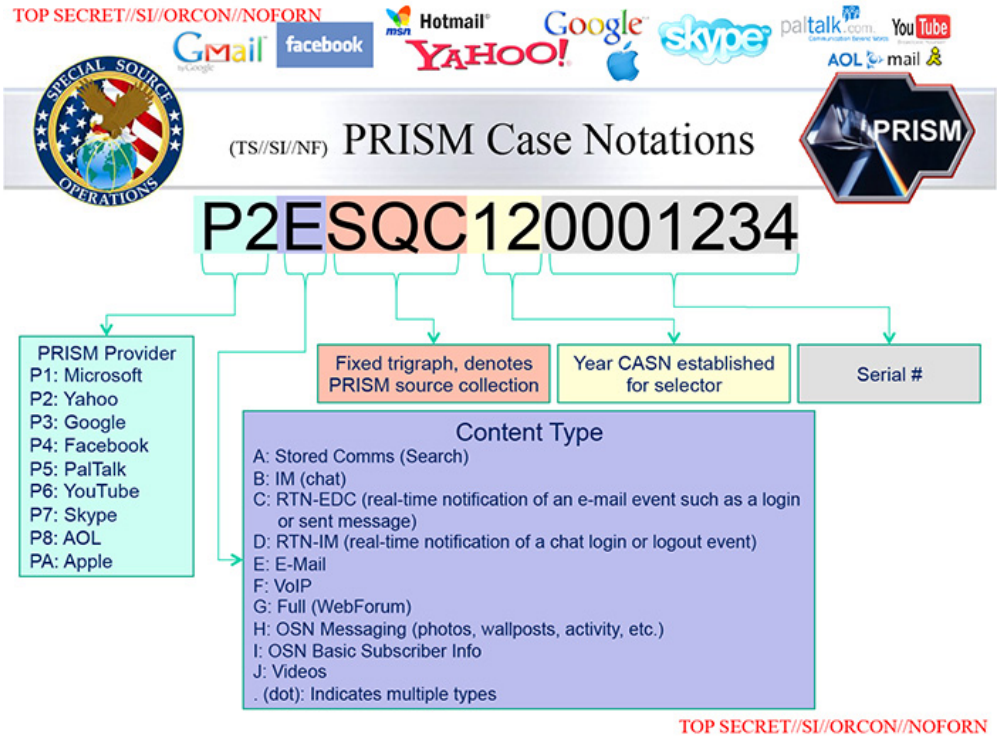

Figura 15 - Dados de origem fornecedores do PRISM [46]

O âmbito desta análise não é escrutinar todas as capacidades e ligações desta ferramenta pois é demasiado complexa e facilmente se entra no campo da especulação científica, descredibilizando todo um trabalho a ser constantemente desenvolvido por investigadores. Por não haver ainda profundos estudos desta disciplina em Portugal, deu-se alguma relevância sobre o tema. Não obstante, consideram-se identificados os elementos capturados e o tratamento que lhes é dado, bem como uma visão ainda de alto nível do método de captura. Mais à frente neste trabalho, precisamente onde estão descritos o tipo comum de atacantes e os métodos de invasão de sistemas que usam, faz-se a ponte de ligação com este ponto e percebe-se como é possível aos sistemas descritos anteriormente, capturar, analisar

[45] Data Mining é uma técnica de tratamento grandes quantidades de dados e informação, com o sentido de a explorar estatisticamente

[46] Imagem recolhida - https://nsa.gov1.info/surveillance/

dados para investigação. Seguidamente podemos ver uma imagem que demostra os meandros desta aplicação. Reitera-se mais uma vez que é meramente informativa.

Designation	Legal Authority *See Note*	Key Targets	Type of Information collected	Associated Databases	Associated Software

US-984XN	Section 702 of the FISA Amendments Act (FAA)	Known Targets include[45]
		• Venezuela
		  • Military procurement
		  • Oil
		• Mexico
		  • Narcotics
		  • Energy
		  • Internal Security
		  • Political Affairs
		• Colombia
		  • Trafficking
		  • FARC
			The exact type of data varies by provider:
			• Email
			• Chat - video, voice
			• Videos
			• Stored data
			• VoIP
			• File transfers
			• Video Conferencing
			• Notifications of target activity, logins, etc.
			• Online Social Networking details
			• **Special Requests**
				Known:
				• TRAFFICTHIEF
				• MARINA
				• MAINWAY
				• FALLOUT
				• PINWALE
				• CONVEYANCE
				• NUCLEON
					Known:
					Unified Targeting Tool

Figura 16 - Visão de alto nível do PRISM [47]

2.3.2 O Muscular

Decorria o ano de 2013 e ainda não se tinha estudado ou percebido bem os meandros e o largo espectro da aplicação *Prism*, quando o *MUSCULAR* foi também exposto. Este consiste num esforço de vigilância conjunta entre os Estados Unidos e o Reino Unido através das agências *NSA* e a sua congénere inglesa, a *GCHQ* (*Government Communications Headquarters* no Reino Unido). Também conhecido pelo seu nome de código *DS-200B*, este visa invadir com sucesso os centros de processamento de informação da *Google* e da *Yahoo*, conseguindo dados que estão armazenados nos seus nós computacionais e na *Cloud* empresarial do *Google* (*Google Cloud)*. De génese idêntica à do *Prism*, este recolhe imensamente mais dados informáticos, pois não está limitado pelas mesmas regras judiciais que imperam nos Estados Unidos.

A sua localização concreta sita no Reino Unido e veio a público através do analista de sistemas da *NSA*, Edward Snowden em abril de 2013, e mais tarde, segundo Barton Gellman [Barton Gellman, 2013] do Jornal *Washington Post*, confirmado por oficiais que servem no *Naval War College*.

[47] Imagem recolhida em - https://nsa.gov1.info/surveillance/

Segundo Elliot Cohen [Elliot Cohen, 2014], o *Muscular* faz a coleta direta de dados que vão alimentar as bases de dados do *Prism* (entre outras) e permitir descortinar a localização de um determinado utilizador, bem como os hábitos *online*.

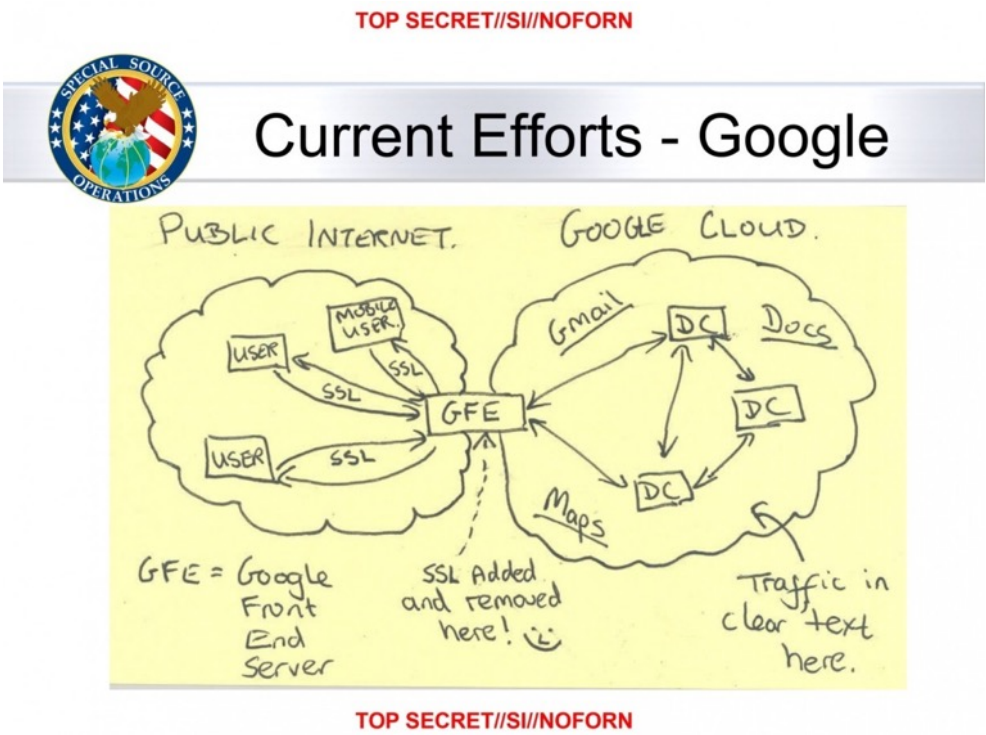

Figura 17 - Imagem sobre o método de captura do Muscular [48]

2.3.2.1 Modus Operandi

O *Muscular* também tem as mesmas características técnicas de atuação que tem o *Prism*, porém o seu principal objetivo é a captura e análise de voz, em particular sistemas de telefonia *VoIP* (*Voice Over IP*). Segundo a Matriz de Vigilância de Christian Gross [Christian Gross, S/D], e outras fontes presentes na possível descrição de atuação do *Muscular* na *Wikipédia*, alegadamente este sistema tem a capacidade de recolher o dobro dos dados ou *selectors*[49] em que o *Prism*. Este sistema, cumulativamente com outros, alimenta uma série de outros sistemas, entre os quais a base de dados primária para a análise de conteúdos e tráfego *Web Pinwale*, que por sua vez é minerada pelo *Prism* devido à sua capacidade de análise e tratamento de dados. Durante o período de dezembro de 2012 e janeiro de 2013, foi responsável pela recolha de 181 milhões de registos, tendo sido quase de imediato

[48] Imagem recolhida em - https://nsa.gov1.info/surveillance/

[49] Selectors, dados recolhidos pela NSA através do programa Muscular, Prism e Incester - https://en.wikipedia.org/wiki/XKeyscore

suplantado por outro sistema idêntico de nome *incenser,* que segundo Barton Gellman [Barton Gellman, 2013] recolheu 14 mil milhões de registo no mesmo período.

Não se sabe concretamente como é feita a maioria da escuta informática, mas segundo Christian Gross [Christian Gross, S/D], depreende-se que os possíveis métodos sejam os descritos no ponto Modus Operandi. Após análise, consegue-se perceber que se devem a ataques similares à invasão *Man-In-The-Middle* (ataque de homem no meio) e clonagem de sistemas de certificação de autoridade e certificados digitais.

Uma breve descrição de como são capturados dados pelo *Muscular* segundo Stuart Sumner [Stuart Sumner, 2015]:

1 O típico utilizador cria documentos, perfis do *Google+* usa o *Google Docs* (*software online* de gestão de documentos da *Google*) para criar ou editar documentos, carregar fotos. Isto é feito através de ligações encriptadas que permitem manter a integridade, disponibilidade e autenticidade da informação e acima de tudo a confidencialidade, o sigilo da mesma;

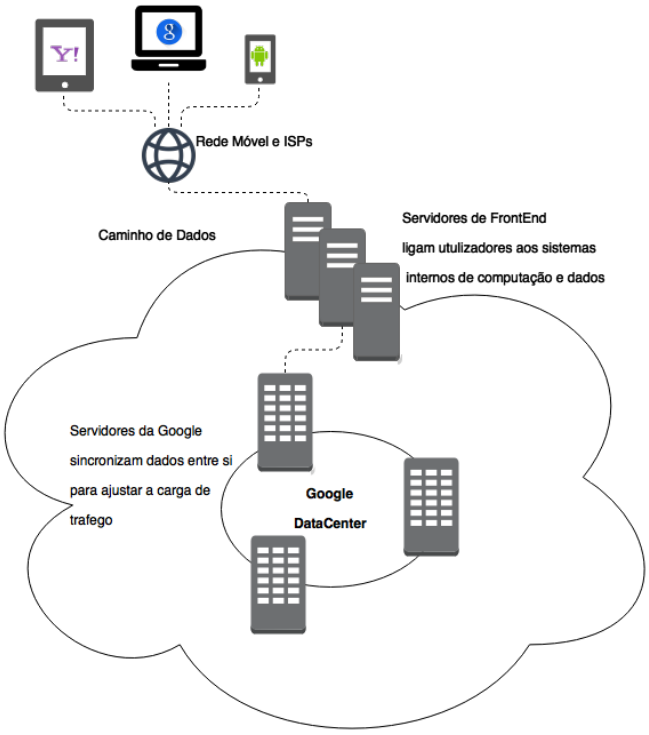

Figura 18 - Diagrama de Acesso ao Meio[50]

2 Todos os pedidos ao *Google, Gmail, Google +, Youtube* e *Drive* são rececionados de forma encriptada (*SSL*) pelos servidores *Front End* do Sistema *Google*;

[50] Imagem elaborada pelo autor

3 Os *datacenters* da Google estão espalhados por todo o mundo, por exemplo na Irlanda, e estão ligados entre si por linhas de fibra ótica;

4 A *Google* e a *Yahoo* guardam múltiplas cópias de todos os ficheiros nos seus sistemas de forma redundante e com recurso a *load balancers* para dividir o volume de informação pela sua rede. Este encaminhamento, divisão e armazenamento é feito por linhas de fibra ótica dedicadas ou alugadas, não partilhando tráfego com outras congéneres de forma a ter segurança acrescida, velocidade na transmissão de dados mantendo uma largura de banda sempre disponível. Por questões ainda agora desconhecidas, até 2014 estas ligações não eram encriptadas e as ligações dos *datacenters* da Yahoo em dezembro de 2014 ainda não o eram também. Importa ainda saber que a 5 de agosto de 2015, a *CNET* informou os internautas que é muito provável que a rede de fibra ótica arrendada, ou seja, que não é de propriedade da *Google* e da *Yahoo*, tenha sido e seja alvo fácil para ligações diretas, sendo o cabo subterrâneo de propriedade da empresa *Level* 3[51] vulnerável a ligações diretas. A empresa em questão recusou-se a comentar estas investigações feitas pelo *Washington Post* e pelo *New York Times*, alegando que apenas transmite às autoridades informação a pedido legal. Não obstante, junta-se ao tema também a interferência direta por meio físico à já conhecida com recurso a *software*. Ainda nesta notícia, o projeto *Muscular* é citado por obter informação através destes métodos e que, para além da *Level* 3, ainda as redes da *Vodafone*, *Verizon* e a *British Telecom* são igualmente alvos fáceis. A *Yahoo* está agora (em meados de 2015) a encriptar a sua *cloud* interna [Richard Nieva, 2015];

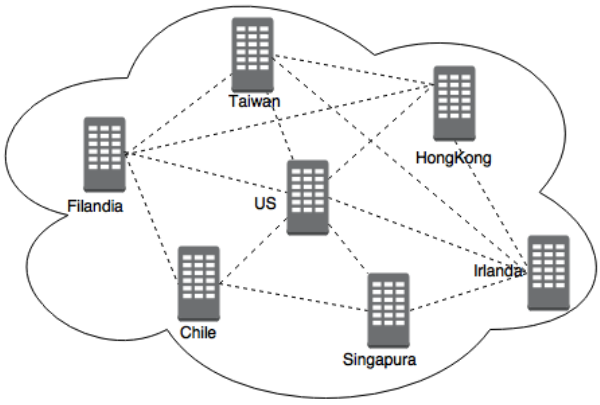

Figura 19 - Fluxo de dados entre datacenters da Google[52]

[51] Level 3 - http://www.level3.com/en/
[52] Imagem elaborada pelo autor

5 São intercetados dados pessoais e de *login* dos utilizadores conforme estes circulam nas redes privadas da Google e Yahoo através de pontos atualmente desconhecidos. Estudos apontam para os seguintes quatro cenários possíveis:

5.1 Cenário 1) Dados entre dois ou mais *datacenters* próprios e geridos por si (Google *Staff* e Yahoo *Staff*), ligados por fibra também proprietária ou rede e sistemas de roteamento geridos ou de propriedade de terceiros. A *NSA*, sem que se saiba exatamente[53] como, penetra nestas redes e desvia tráfego para armazenamento e análise;

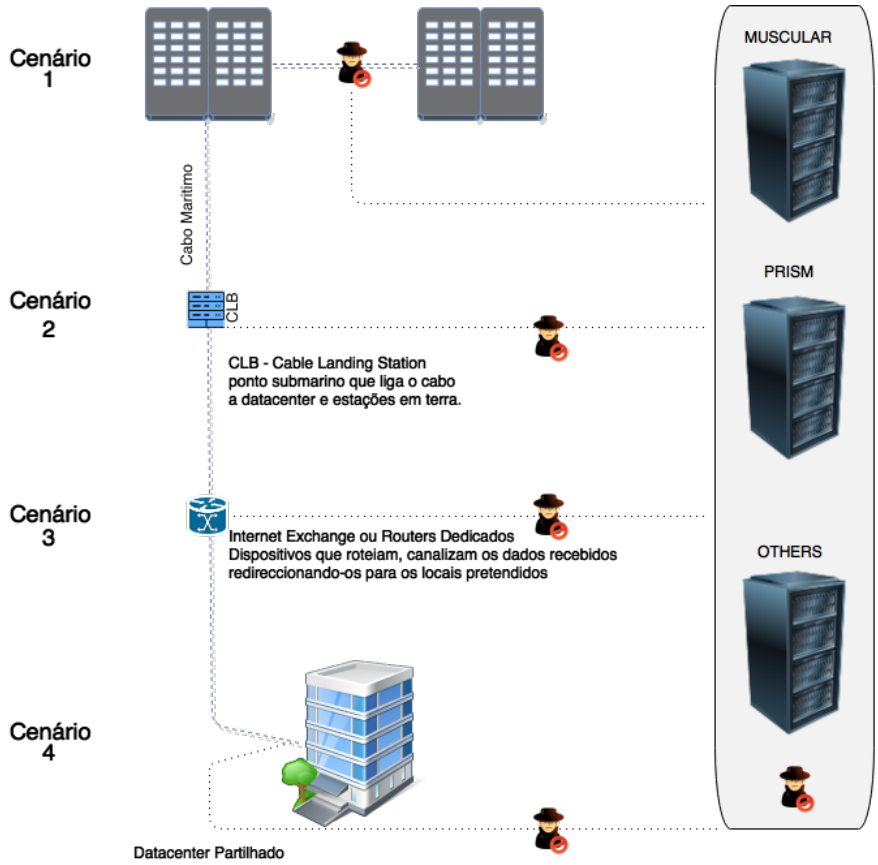

Figura 20 - Cenários possíveis para desvio de informação[54]

5.2 Cenário 2) A Google é proprietária de uma extensa rede de cabos submarinos, fazendo desta a principal empresa de Internet do mundo. A NSA e a Britânica GCHQ podem ter coagido ou intimado operadores de prestação de serviços de manutenção ou arrendamento destas redes, a facultar acesso ao meio. Podem ter solicitado o mesmo a operadores de datacenters usados pela Google e Yahoo;

[53] Notícias de agosto de 2015, referindo estudos, indicam que estes acessos podem ser físicos
[54] Imagem elaborada pelo autor

5.3 Cenário 3) A Google também arrenda redes privadas e links a ISP locais para poder passar os seus dados, deixando assim vulnerável a informação a cargo destes;

5.4 Cenário 4) A Google também partilha servidores com a Amazon e outras grandes empresas como a Microsoft, de forma a poder usar as infraestruturas destes. Isto deixa acessos não monitorizados fisicamente por funcionários da Google, expostos à colocação de dispositivos de controlo de rede.

2.3.3 O Golden Shield Project

Segundo Neil Huges [Neil Huges, 2002], o crescimento tecnológico e a evolução dos mercados financeiros assentes nas tecnologias são antagónicos às sociedades que controlam a liberdade de expressão dos seus cidadãos. Segundo o mesmo autor, a China tem um regime ditatorial comunista, enraizado há mais de 50 anos. Este regime, que preconiza o sistema de tigela de ferro (nada faltará ao povo e todos os bens necessários à sobrevivência estão garantidos, incluindo trabalho vitalício), controla sagazmente todo o tipo de informação externa que chega ao seu povo. Estes tipos de regimes, historicamente estão condenados ao insucesso ou miséria, como se pode ver agora na Coreia do Norte e na antiga União Soviética.

Ainda segundo o mesmo autor, com o crescimento dos mercados financeiros, a China decidiu entrar no jogo e iniciou a produção em massa de quase tudo o que o mundo consome. Ao querer maximizar os lucros (gestão capitalista inversa ao comunismo), a China decidiu que abriria as portas do mundo dos negócios à sua população, ora isso implica poder comunicar com o mundo para não se perderem oportunidades. Esta abertura levou a que a *Web* estivesse ao alcance de todos e especialmente à oposição que fazia questão de passar informação da evolução ocidental, e o conforto da maioria das suas poluções. Para contornar esta questão, o Ministério da Segurança Pública lançou o projeto Escudo Dourado (*Golden Shield Project*). Este projeto consiste na mais sofisticada *firewall* de verificação de pacotes de dados à entrada e à saída da *Web* na China.

Segundo Sarosh Kuruvilla [Sarosh Kuruvilla et al., 2011], após a chegada da *Internet* em 1994, o governo chinês em 1997 colocou em ação as primeiras medidas de controlo, emitindo regulamentação sobre o uso e as devidas penalizações. Em 1998, o partido comunista, com receio de perder o controlo do país, deu instruções para que se produzisse uma rede capaz de controlar todo o tráfego *Web*. Apelidada de Grande *Firewall* da China em 97, emprega mais de 45.000 polícias e é uma complexa rede servidores *proxy* que impedem os *IP* de origem chinesa sair por um dos seis *gateways* chineses.

2.3.3.1 Modus Operandi

- **Boqueio de *IP*** – Impede o acesso a *IP* específicos. Se o *site* destino estiver hospedado em sistemas de hospedagem partilhado, todos os *sites* desse servidor serão bloqueados. Todos os protocolos de *IP*, sobretudo *TCP* tais como o *HTTP*, *FTP* ou *POP* serão bloqueados;
- **Filtragem e redireccionamento de *DNS*** – Este método não resolve o nome de domínio. Afeta todos os protocolos de *IP* tal como *HTTP*, *FTP* ou *POP*. Uma forma típica de evasão a esta técnica é encontrar servidores de *DNS* que resolvam os nomes dos *IP* sujeitos a bloqueios. Para tal altera-se o ficheiro de *host* (anfitrião) ou adicionar na barra de endereço no *browser*, o número de *IP* do *site*;
- **Filtragem de *URL*** – Este método analisa a *string* (sequência de texto) *URL* solicitada pelo utilizador e procura palavras-chave que constem numa lista de *sites* não permitidos. Este método afeta o protocolo *HTTP*. Evasão típica a este mecanismo é o uso de *VPN* e ligações *SSL*;
- **Filtragem de pacotes** – Termina as comunicações entre servidor cliente quando uma determinada palavra-chave é encontrada. Isto afeta todos os protocolos *TCP* como o *HTTP*, *FTP* ou *POP*. As páginas de retorno com resultados de uma pesquisa são mais comuns de serem bloqueadas e censuradas. A forma de iludir este sistema é através do uso de protocolos encriptados, como por exemplo o uso de *VPN* e *SSL*;
- **Reinicialização de contexto** – Se determinada conexão de *TCP* foi bloqueada pelo filtro, futuras tentativas de conexão serão também bloqueadas. Estas estendem-se aos dois lados, servidor e cliente por um período nunca inferior a 30 minutos. Dependendo da localização do sistema bloqueado, outros utilizadores ou *websites* poderão ser bloqueados também, caso haja um encaminhamento de pacotes de comunicação por esse meio, por exemplo, um *hotspot* (ponto de acesso *wifi*) num *shopping*. A forma de evitar este contratempo é ignorar o pacote de dados de reinicialização enviado pela *firewall*;
- **Ataque man-in-the-middle** – Este método cria conexões independentes com a vítima e faz a retransmissão das mensagens, simulando que um sistema está a falar diretamente com o sistema de destino pretendido, quando na realidade a conversa é controla por terceiros;
- **Reconhecimento de tráfego VPN/SSH** – Este método reconhece o tráfego *VPN/SSH* assinalando na rede controlada uma comunicação por esse meio, logo, os *IP*

intervenientes estarão mais propícios a seguimento por parte das autoridades chinesas. Em 2011 foram comunicadas as primeiras ligações *VPN* a serem desligadas em massa. O sistema aprenderia a identificar autonomamente os traços digitais das redes *VPN* e passaria a quebrar as ligações desses *IP* ou dos *IP* das entidades que fornecem *VPN* como serviço;

- **Recolha de nomes de serviços** – Este método é um dos mais recentes adicionado pela Grande *Firewall* da China, permite coletar informação dos *IP* e dos *usernames* de utilizadores de serviços específicos como a rede *Tor*. Embora ainda não plenamente confirmado, esta possibilidade poderá criar elevada vítimas, uma vez que a rede *Tor* tem um elevado número de utilizadores na China.

Segundo Jonathan Zittrain [Jonathan Zittrain, 2003] e Benjamin Edelman [Bejamin Edelman, 2003], professores na Universidade de Harvard nos Estados Unidos, escrito no trabalho "*Empirical Analysis of Internet Filtering in China*", alguns *sites* famosos bloqueados pela censura Chinesa são *websites* ligados a temas proibidos como o confronto na Praça de *Tiananmen* ou *sites* ligados à causa do *Dalai Lama*. Grandes empresas de prestação de serviços *Web* globais como a *Google*, tentaram em ingloriamente combater a Grande *Firewall* da China, mas os interesses económicos fazem com que a gigante tecnológica desistisse da ideia e se rendesse às exigências de Pequim.

Segundo Greg Walton [Greg Walton, 2010], um investigador *freelance* citado no Torfox[55] da Universidade de Stanford, estudos apontam para que a *firewall* tenda a assemelhar-se com iniciativas americanas, onde se coletam grande informação de dados. O intuito é capturar e guardar dados massivos dos utilizadores, tais como registos faciais, dados de crédito bancário, reconhecimento de voz, entre outros dados dos internautas. O resultado de 800 mil milhões de dólares gastos nesta tecnologia desde que surgiu em meados dos anos 90, foi uma complexa plataforma protegida e aumentada com recursos a meios legais. A título conclusivo, uma portaria da lei da China obrigava a que todas as máquinas fabricadas e vendidas na China devessem ter instalado o *Gree Dam Youth Escort*, um *software* de controlo de conteúdo orientado para a reeducação cultural do uso da *Web,* bem como uma forma de controlo contra pornografia e outros *websites* indesejáveis. Embora obrigatório ao início, o seu uso é agora facultativo.

[55] Torfox – Grupo de investigação da Universidade de Stanford que estuda a grande firewall da China http://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/FreedomOfInformationChina/technology/index.html

Um caso notório de repercussões levadas a cabo pelas entidades chinesas foi a prisão do ativista Wang Xiaoning, sentenciado a dez anos de cadeia e reeducação por trabalhos forçados por usar o sistema de *email* da *Yahoo* para colocar comentários anónimos sobre o sistema escolar chinês e publicar fotografias *online* de escolas a cair de velhice e completamente inadequadas para o serviço que se propunham [Rebecca Makinnon, 2012].

2.3.4 Piratas Informáticos

As ameaças não são apenas de origem governamental ou de sociedades mais ou menos secretas. É também uma atividade criminosa danosa e lucrativa, uma chamada de atenção para os problemas informáticos existentes em plataformas ou sistemas, uma fonte de informação que permite que terceiros obtenham uma posição revelante no uso dessa informação e muitas outras atividades. Segundo Eric Raymond [Eric Raymond, 1997], e de acordo com Robert Moore [Robert Moore, 2010], existe um grupo de pessoas que, com recurso às elevadas capacidades informáticas que possuem, com objetivos muito específicos, se dedicam a desenvolver as suas capacidades de explorar, modificar ou aceder a sistemas, a conhecer:

- ***Hacker*** - Pessoa que procura quebrar a segurança de sistemas ou redes, através de vulnerabilidades, com fins destrutivos ou para posse de informação privilegiada;
- ***White Hat Hacker*** - *Hacker* interessado por segurança informática, procura explorar e testar os sistemas através dos seus conhecimentos, sem violar leis, procurando advertir as entidades proprietárias desses sistemas para as falhas que descobre;
- ***Black Hat Hacker* ou *cracker*** - É um individuo que procura quebrar, penetrar e destruir efetivamente código, e modificando o mesmo acede a um determinado sistema. São especialistas em invasões maliciosas e silenciosas que visam simplesmente a destruição com benefício económico ou aparato mediático para se auto promover, em tudo semelhante ao que se pode encontrar em organizações de crime organizado. Posteriormente utilizam a informação recolhida para proveito próprio;
- ***Gray Hat Hacker*** - Possui características semelhantes ao *White Hat Hacker*. A sua atuação é compreendia algures no meio do *White e o Black hacker*. Entra em sistemas de forma ilícita e prontifica-se a demonstrar como o fez, através de um valor

pecuniário. Por questões de ego, também alteram e publicam os seus feitos informáticos junto da sua comunidade;

- ***Elite hacker*** - Um *Elite Hacker* é o mais "graduado" e talentosos dos *hackers*. Quando descobrem novas formas de violação de sistemas, partilham entre si essa informação e estão agregados em clãs. A permanência num grupo de elite, como por exemplo os *Annonymous*[56];
- ***Neophyte*** - É um iniciado ao *hacking* (ato de violar sistemas) e apesar de não possuir grandes conhecimentos técnicos, tem imensa vontade aprender. Não atua sozinho e está por norma em fase de formação, sendo, no geral, inofensivo;
- ***Blue Hat*** - Alguém que não trabalha diretamente nas empresa de consultoria informática mas que por ser um *hacker* talentoso, é chamado a testar sistemas, seja por contrato ou por evento, por exemplo o *Hackathon*[57].

2.3.4.1 Modus Operandi

Existe um elevado número de ataques possíveis concentrados em quatro categorias gerais: ataques por monitorização, ataques de validação, ataques de negação de serviços e ataques por modificação. Estes exploram as vulnerabilidades dos sistemas de informação, o seu mau uso, medidas de contenção existentes e igualmente inexistentes e as políticas de segurança. Adicionalmente, o uso de *software* pirata e o desconhecimento dos ataques e dos impactos possíveis destes levam ao crescente aumentos dos tipos de ataques e do modo como estes são efetuados.

Os ataques de monitorização executam-se com o intuito de observar as vítimas e os seus comportamentos *online*, bem como o uso empregue aos seus sistemas de informação com o objetivo de obter informação valiosa e privilegiada. O seu principal objetivo é enumerar as vulnerabilidades para encontrar formas alternativas de acesso e monitorização.

- ***Shoulder Sniffing*** - Como o nome indica, consiste no ato de espiar fisicamente a vítima (espreitar sobre o ombro). Por exemplo, estar atento ao que determinada pessoa está a introduzir quando está a aceder a um sistema, tentar guardar os dados de *login*, ou mais simplesmente, tentar ver qual o *pin* de acesso de um telefone. Mais complexamente, foi usado no passado por *phrackers* (*hackers* que se especializam em

[56] Anonymous é um grupo anónimo de piratas informáticos (hackers) que se dedicam a causas alegadamente nobres do mundo informático e social. Conhecidos pela guerra informática constante com a Igreja da Cientologia

[57] Hackathon, também conhecido por hackday, hackfest ou codfest é um evento anual em que as grandes empresas como a Apple, Google e Microsoft convidam pessoas especialistas em informática, entre os quais hackers, para encontrar vulnerabilidades num espaço de 24 horas, a troco de um prémio monetário

sistemas de telefonia), que recorriam a métodos menos tecnológicos, como vasculhar o lixo da vítima à procura de dados que possam levar a informação sensível;

- ***Decoy*** - Programas que se instalam no computador das vítimas para que se interponham entre o utilizador e os serviços de destino. Este consiste no uso ou desenvolvimento de numa interface com o utilizador, igual ao que realmente corresponde ao serviço. Esta interface tem o intuito de apanhar os dados de *login* da vítima, no momento que esta os fornece conscientemente, pois considera a interface legítima. Este tipo de programa permite que o serviço legítimo funcione em plenitude. O seu único intuito é captar dados de *login*. Alguns exemplos deste tipo de *softwares* são os *keyloggers* (*softwares* que captam o registo de teclas pressionadas no teclado). Este tipo de incursão é muito conhecido pelos ataques aos sistemas de *home banking* (acesso ao banco por meios digitais), registando os dados inseridos pelo utilizador e remetendo estes para terceiros de forma anónima;
- ***Scanning*** - Este método é usado para descobrir canais de comunicação suscetíveis de serem utlizados por intrusos, sendo que através deles enviam-se pacotes de diversos protocolos diretamente aos portos de uma máquina virtual, deduzindo, segundo a receção ou extravio de pacotes resposta, que serviços dessa máquina estão disponíveis;
- ***Scanning TCP Connect*** - Pertencente à categoria anterior, este é o mais simples dos ataques a portos *TCP*. Se determinado porto do alvo está à escuta, este devolverá ao pedido de ligação uma resposta de sucesso, estabelecendo com o atacante uma conexão. Este método é também conhecido como acordo de conectividade em três vias, ou em inglês "*three-way handshake*". Esta técnica levanta suspeitas pois a degradação da performance do computador vítima é notória para o administrador de sistemas (no caso de existir) que iniciará o encerramento de portos de comunicação;
- ***Scanning TCP Syn*** - Quando se efetua um pedido de ligação entre máquinas, como por exemplo a máquina atacante e a máquina vítima, é lançado um pedido de *Syn*[58] da máquina atacante para a vítima. Isto significa solicitar uma ligação para a transmissão de dados ou informação para um determinado porto destino. A máquina vítima responde com uma *Ack*[59] confirmando a receção do pedido. Caso o porto esteja fechado ou indisponível, o interveniente destino responderá com um recibo

[58] SYN – Synchronization ou pedido de sincronização
[59] ACK – Acknowledge ou confirmação da recepção do pedido

Rst[60]. Na eventualidade do recetor responder com um *Ack*, o atacante responde com um *Ack* também para se registar na máquina vítima, ficando desta forma concretizada a ligação para a troca de dados entre os dois sistemas. O intuito não é estabelecer ligações com este ataque, mas sim fazer uma leitura de todos os portos disponíveis, enviando um ou mais *Ack*, aguardando pelas respostas e caso estas sejam positivas, enviando um ou mais *Rst*, no sentido de transmitir o desinteresse na ligação. Assim, com este ataque, consegue-se descobrir quantos portos estão abertos a comunicações para intentar a mais variada panóplia de intrusões;

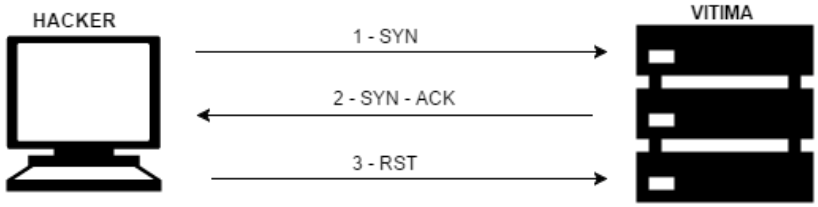

Figura 21 - Workflow Syn, Ack, Rst[61]

- ***Scanning TCP Fin*** - Este é um ataque que pretende não ser detetado pelas medidas de segurança colocadas em prática, por exemplo, por administradores de sistemas de informações numa determinada organização. A grande maioria das *firewalls* deteta o ataque anterior e adiciona o *IP* do agressor à lista negra, evitando que este continue a fazer tentativas de leitura de portos abertos. Normalmente portos fechados respondem com um *Fin*[62]ou com um pacote *Rst*. Estando os portos abertos, estes não irão transmitir o *Fin* sendo automaticamente registados como portos abertos. Esta técnica é exclusiva dos sistemas não *Windows* pois envia sempre o *Rst* independentemente do estado do porto;
- ***Scanning Fragmentado*** - Também para contornar as *firewalls* que estão à escuta das tentativas de leitura de portos, o *scanning* fragmentado consiste no envio para a máquina vítima de pacotes divididos em pequenas tramas (frações), forçando a máquina vítima a perceber estas como comunicações corrompidas e não como um possível ataque. Neste caso, o atacante quando receber o *Ack* nada responderá e procede ao registo do porto como estando aberto;
- ***Eavesdropping / Sniffering*** - Este ataque é muito comum e foi bastante recorrente em cibercafés no início da década passada. Consiste na colocação não autorizada de

[60] RST – Refuse State ou porto fechado ou indiponivel
[61] Imagem elaborada pelo autor
[62] FIN – Final ou finalização de transmissão

um programa na máquina vítima. Este programa, ou *sniffer*, tem como objetivo registar toda a informação do tráfego de rede num ficheiro disponível ao atacante. O seu alvo preferencial consiste em dados de *login*, contas de correio, dados bancários, cartões, dados de rede como informação de máquinas disponíveis e respetivos serviços, processos de conectividade e dados de *VPN*. O mecanismo desta técnica baseia-se no facto de quando uma máquina da rede envia informação, todas as outras escutam, mas só apenas a máquina destino responde reclamando os pacotes de dados que lhe é dirigido. O *sniffer* dá instruções de cópia de todos dos pacotes que passem pela placa, quer sejam eles para a máquina destino ou não.

Nos ataques de validação o objetivo é usurpar a identidade de um utilizador ou máquina, passando a usar estes como origem de qualquer ataque. É considerado um processo de ataque por suplantação.

- ***Spoofing-Looping*** - Este ataque consiste no uso dos dados de *login* para entrar numa rede e recolher dados sobre os equipamentos e serviços da rede. A informação vital que é recolhida será usada para atacar outros alvos na rede ou noutras redes. Visualize-se a seguinte analogia: imagine-se uma espécie de rede de *proxys* em que o atacante cria uma ponte de máquina em máquina para chegar a um alvo, impossibilitando a deteção do computador de origem;
- ***IP Spoofing*** - Neste ataque o intuito é a criação de um endereço de *IP* que é credível para a rede alvo ou o uso de um já existente nessa rede. Gera-se depois um pacote de informação cujo emissor possui de *IP* diferente daquele que o intruso usa e por norma, o de uma máquina já existente na rede. Esta técnica pode ser usada em conjunto com outras para descobrir processos de segurança implementados de forma a conseguir aprender a evitar os mesmos.

A imagem seguinte representa o raciocínio anterior;

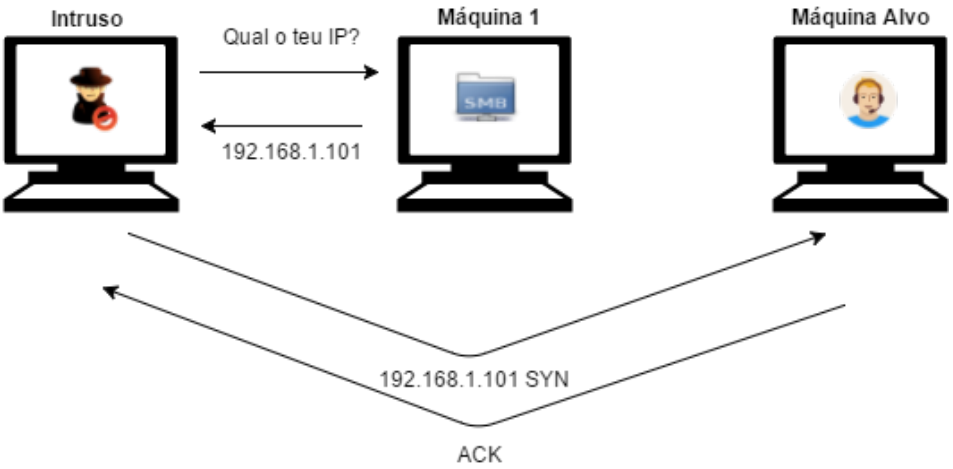

Figura 22 - Técnica de IP Spoofing[63]

- ***DNS Spoofing*** - Este ataque consiste na manipulação de pacotes *UDP* para enganar um servidor de *DNS* no intuito que este disponibilize as suas tabelas de registo para que se possam alterar as mesmas enquanto correm na cache (memória intermédia entre operação e processo). Este permite dois ataques, o *DNS ID Spoofing* e o *DNS Cache Poisoning;*
- ***DNS ID Spoofing*** - O atacante obtém o *ID* do pedido ao *DNS* para a resolução de um determinado nome, respondendo à vítima com um destino correspondente a uma máquina de sua conveniência, como por exemplo, uma máquina que simula um *Website* de um banco;
- ***DNS Cache Poisoning*** - Esta técnica visa envenenar a memória do servidor de *DNS* com a colocação de registos onde a correspondência é a que mais convém ao atacante. Esta técnica usa funcionalidades de pedido de resolução que é feita por um *DNS* a outro *DNS* na tarefa de atualização das suas tabelas de registo. O cenário baseia-se num pedido feito pelo atacante a um servidor *DNS* de um nome que este não tem na sua tabela de registos, forçando assim este a consultar outro *DNS* para se atualizar. A variante é que o *DNS* que faculta a informação de atualização está adulterado com endereços de conveniência do atacante;
- ***IP Splicing / Hijacking*** - O objetivo consiste num novo tipo de usurpação de identidade, mas desta vez com o desígnio de intromissão numa conversação em curso,

[63] Imagem elaborada pelo autor

tendo em vista obter informação significativa. Através da análise de uma comunicação entre dois elementos, em que um deles é eleito como potencial vítima, e em que num determinado momento é capturada uma resposta destinada à vítima, alterando ligeiramente a mesma, mas tentando que esta alteração não seja percetível. O elemento que originou a mensagem deturpada aguarda a resposta, estando o atacante a intercetar todos os novos pedidos para a vítima e respondendo-lhe como se esta estivesse ocupada ou indisponível, garantindo assim que nem o emissor ou recetor desconfiem que existe uma terceira pessoa entre os dois.

- ***Backdoors*** - É uma técnica de usurpação de identidade. Um programador desenvolve uma aplicação, mas deixa um processo oculto para testar a sua aplicação, esquecendo-se de eliminar. Esta *backdoor* propositadamente existente pode ser encontrada e explorada;
- ***Uso de Exploits*** - Esta técnica consiste em ferramentas que compreendem um conjunto de instruções que exploram as vulnerabilidades de um *software* ou sistema de informação, resultante de erros de programação ou *bugs,* permitindo a alteração de privilégios dos utilizadores, criação de novos utilizadores, conexões ou mesmo *backdoors*.

Ataques de negação de serviços visam negar bloquear ou esgotar os recursos disponíveis de uma máquina, impedido que outros lhe acedam. Uma vez que a máquina está alcançável do ponto de vista comunicacional, o ataque consiste em reduzir ou mesmo interromper os recursos que permitem à máquina alvo prestar um serviço baseado em rede, seja ele por excesso de processamento ou por entupimento devido a excesso de pedidos.

- ***Flooding*** - Este ataque consiste numa inundação de pedidos para estabelecer conexão com a máquina alvo, forçando esta a reservar recursos e a saturar o seu *buffer* com conexões abertas à espera de respostas que propositadamente não irão chegar. Este processo obriga a uma elevada alocação de recursos, que devido à sua extensão conduzem a máquina a recusar novos pedidos de ligação. Um ataque conhecido é o "*Ping of Death*", ou envio de *email* um-a-um de uma lista subtraída de um servidor, levando à saturação da máquina que labora como servidor de correio;
- ***Syn Flood*** - Este ataque consiste no envio de um pacote *Syn* mas não responder à resposta *Ack* que a máquina vítima irá enviar. Esta medida obriga a que a vítima aguarde pela resposta por um período indeterminado de tempo. O impacto será

maior se o *IP* do atacante for de uma rede externa ou desconhecido. A massificação destes pedidos leva a que a vítima perca a capacidade de resposta;

- ***Connection Flood*** - Similar ao ataque anterior, mas desta vez a conexão é feita sem qualquer envio de dados por parte do atacante. O atacante implementa ciclos que voltam a proceder à conexão quando a anterior faz *timeout*. Este ataque impede que novos clientes se conectem a um determinado *Website* que possuem alojado, pois os recursos estão a ser massivamente usados;
- ***Broadcast Storm*** - Esta técnica consiste no envio massivo para a rede de pedidos *ICMP*[64] para o endereço de *broadcast* (255.255.255.255) com indicação do *IP* de origem a máquina alvo. Desta forma colapsa-se a vítima com respostas *ICMP* às quais não conseguirá dar seguimento;
- ***Network Overflow*** - Este ataque consiste no lançamento para uma determinada rede, de um sem número de pacotes de dados desconexos ou sem sentido, forçando estes a transitar de máquina em máquina, esgotando assim os recursos da rede, impossibilitando a sua normal actividade;
- ***Email Bomber*** - Consiste este ataque na saturação de uma caixa de correio com o envio massivo da mesma mensagem com o único intuito de entupir a caixa de receção de correio. Este ataque é comum, mas visa normalmente uma lista de contas de correio furtadas e recorre a um automatismo ou programa para enviar milhares de *emails* por segundo.

Ataques por modificação possuem o objetivo de modificar dados, ficheiros e por consequência informação contida nos sistemas de informação atingidos por este tipo de iniciativa.

- ***Tampering*** - Este tipo de situação está relacionado com a modificação sem autorização de dados ou programas instalados num determinado sistema de operativo, incluindo o comando para apagar comandos ou outros comandos. São ataques muito perigos, pois, se o intruso conseguir obter privilégios de administrador da máquina, irá conseguir alterar o que pretender a seu bel-prazer sem muitas barreiras;

[64] Internet Control Message Protocol ou Protocolo de Controlo de Mensagens por Internet

- ***Tracks Erasers*** - Estes tipos de ataques são mais direcionados a sistemas do que indivíduos. Consistem na alteração dos registos de *log* (ficheiros que registam operações e o seu histórico) onde estão contidas as atividades sobre esses sistemas;
- **Ataques com *Java Scripts*** - Este ataque consiste no uso do *browser* para proceder a operações na máquina vítima sem o conhecimento dos seus utilizadores. Alguns exemplos comuns é a instalação de *keyloggers* e capturas de dados do *browser*;
- **Ataques *Java Applets*** - Os *applets* são programas executáveis em linguagem *java* que por norma permitem a intrusão num sistema ou computador de um utilizador. Muitos destes *applets* estão escondidos noutros programas aparentemente inofensivos. Para que o *applet* corra, necessita que a máquina vítima tenha a plataforma *Java Virtual Machine* que, por norma, está instalada de origem em muitos sistemas operativos;
- **Ataques *ActiveX*** - Muitas páginas *Web* solicitam ao utilizador que aceite a execução de alguns controlos de estilo *ActiveX* para executar tarefas perfeitamente normais, mas que ocultamente abrem *backdoors* que permitem acesso aos sistemas. Mais recentemente, algumas publicações na rede social *Facebook*, solicitam uma aprovação por *Like* (botão que informa outros utilizadores da concordância ou gosto afirmativo de um conteúdo) que seguidamente abrem uma nova *Webpage* com conteúdos especificamente ajustados para correrem, ou publicidade ou extensões *ActiveX*, sobre o pretexto de ser necessário atualizar o computador para visualizar a página. Isto leva a que o utilizador incauto aceite e instale *software* malicioso.

Criptoanálise:

Anteriormente foi possível analisar de forma sintética a criptografia e em que métodos consistem. Para um *hacker*, existem inúmeras técnicas de criptoanálise sendo que as seguintes são as mais utilizadas:

- **Ataques usando apenas o criptograma -** Visam descobrir o texto ou cifra (algoritmo ou chave) que originaram um dado criptograma, partindo apenas do conhecimento deste último;
- **Ataque com conhecimento do texto original -** Visam descobrir o texto ou cifra (algoritmo ou chave) que originaram um dado criptograma, partindo da análise do texto por encriptar e da versão encriptada;

- **Ataque com texto original escolhido -** Visam descobrir uma cifra (algoritmo ou chave) usada num sistema criptográfico, introduzindo nesse sistema texto escolhido, e analisando o criptograma resultante. O objetivo é coletar informação que reduza a segurança do método de encriptação;
- **Ataques com texto original escolhido de forma adaptativa -** São uma variante dos que usam texto escolhido. A diferença está no facto de parte do texto introduzido ser escolhido em função dos criptogramas obtidos previamente;
- **Ataques com criptogramas escolhidos (*ACE*) -** Consistem numa variante dos que usam texto escolhido. A diferença consiste em introduzir criptogramas no sistema criptográfico e analisar o mesmo a partir de textos originais produzidos;
- **Ataques de aniversário -** Consistem numa variante dos que usam a pesquisa exaustiva. Exploram a matemática do paradoxo do aniversário na teoria da probabilidade e conseguem chegar a uma solução num número inferior de tentativas, próximas da raiz quadrada do que seria expectável à partida.

Ataques comuns sem criptografia:

Sem o recurso a métodos de criptoanálise, os métodos mais comuns de ataque, potencialmente métodos não invasivos da camada física dos sistemas analisados anteriormente (*Prism*, *Muscular*) não teriam ocorrido.

- ***Man-in-the-middle attack*** - Indivíduo que se coloca à "escuta" normalmente usando uma porta bem conhecida para capturar informação entre um emissor e um recetor;
- ***Denial of service (DoS, DDoS)*** - Este ataque consiste em sobrecarregar um sistema através de ligações simultâneas. Estas ligações têm o intuito de desencadear falhas que coloquem o sistema numa posição fragilizada, abrindo brechas de acesso, ou simplesmente para conseguir torná-lo indisponível. O ataque distribuído (*DDoS*) tem a particularidade de ser executado por vários sistemas tendo cada um deles o mesmo sistema-alvo;
- ***Ping of death*** - Ataque que consiste em enviar sucessivamente mensagens com tamanho maior que os 65.536 *bytes* permitidos pelo protocolo *IP*. Uma ferramenta deste género é o *sPing*;
- ***Buffer Overflow*** - Este ataque é tipicamente um erro comum entre programadores, acontecendo quando uma aplicação recebe dados com um tipo ou tamanho

inesperado quando estão a correr na memória RAM, não havendo tratamento da exceção. Provocado na rede, este ataque permite a que as máquinas lhe estão conectadas não respondam, sendo um exemplo clássico de um meio para atingir o objetivo que é o ataque *DDoS*;

- ***Spoofing & Poisoning*** - Estes conceitos podem ser aplicados a protocolos como o *IP*, *DNS*, o *ARP* e o *DHCP*, e são por vezes usados em conjunto para permitir um ataque mais bem-sucedido. O *spoofing* consiste em falsificar uma identidade recetora, levando o emissor e comunicar normalmente com o atacante. O *poisoning* consiste em modificar um pacote, adulterando o seu conteúdo em proveito do atacante;
- **Ataque de autenticação** - Este é um tipo de ataque que visa obter acesso a um sistema sem ter credenciais para o fazer;
- **Dedução** – No qual o atacante tenta adivinhar os dados (através de dados pessoais do titular da conta, usando o sistema de recuperação de chaves por pergunta/resposta, entre outros);
- **Força bruta** - Através de aplicações que testam múltiplas combinações de chaves por segundo, usando dicionários de palavras ou conjuntos de caracteres. Um exemplo é o programa *John the Ripper*[65];
- ***Sniffers*** - Estas aplicações executadas em rede permitem capturar pacotes transmitidos entre um emissor e um recetor, em busca de palavras que possam tratar-se de palavras-chave. Estes aplicativos podem mesmo desencriptar os dados caso não circulem em *plain text* (texto simples).

Segundo a Agencia Reuters [Reuters, 2015] recentemente foi notícia grandes ataques diretos a plataformas que servem grandes expressões de utilizadores, como é o caso da plataforma *Ashley Madison*. Estes ataques são efetuados por *hackers* experientes que, sob o lema de informar, expõem as vulnerabilidades que encontram. Se alegadas vulnerabilidades não forem corrigidas, espalham por toda a *Web* o método do ataque e o resultado deste. Por norma são divulgados grandes conjuntos de informação que em análise podem prejudicar gravemente os utilizadores destas plataformas e dos seus serviços.

Aqui levanta-se a questão da seriedade intelectual destes supostos piratas que pretensamente apenas querem fazer o bem. As suas ações podem ser de tal gravidade que levam, e neste caso em particular levaram, a que algumas pessoas se tenham suicidado [Rob Waugh, 2015]. Ainda segundo o mesmo autor, os atacantes comuns, em vez de aceitarem a

[65] John the Ripper Password Cracker – Download em http://www.openwall.com/john/

responsabilidade dos seus atos, imputam estes gestos de desespero aos prestadores de serviços inseguros, sendo moralmente desonesto e até nefasto.

2.4 Soluções

A segurança efetiva é dispendiosa e avaliar o retorno da mesma é uma tarefa árdua e fora do alcance de quem tem por norma a capacidade de desbloquear verbas para quem decide a implementação das medidas de segurança. Na informática existem duas áreas em que não existem soluções que respondam a cem por cento dos problemas: segurança informática e testes e qualidade de sistemas e *software* [Fernando Boavida et al., 2013].

Embora não o pareça, as duas áreas tocam-se quando se trata de segurança informática. Como observado anteriormente, na segurança informática existem normas *ISO* (*ISO/IEC 17799*) e quando se efetuam testes de qualidade, normalmente a matriz de rastreabilidade consiste em verificar que os pontos pertencentes à norma são efetivamente objeto de teste e consequente sucesso.

O nível de complexidade aumenta quando no panorama surgem vários fatores que contribuem para a degeneração da segurança e anonimato *online*. Segundo Bruno Garracho [Bruno Garracho, 2009], a maioria dos sistemas operativos são *COTS* (*Commercial Off-the-Shelf*), privilegiando o uso e a estética à segurança. Este fenómeno verifica-se, pois, um sistema seguro ou mesmo a segurança informática são desconfortáveis. Aplicações que efetivamente protegem os utilizadores são ruidosas e complexas de configurar, e quando estes as configuram, privilegiam sempre os modelos *Wizard, next*, *next, next, end*. Preferem sempre sistemas operativos que façam atualizações automáticas e, na grande maioria dos casos, não querem pagar pelo conteúdo, recorrendo a *software* que permite ultrapassar as barreiras de licenciamento impostas pelos fabricantes. Ora, aqui se cria o primeiro precedente de segurança. A instalação de *software* que permitirá violar o sistema de ativação de aplicativos. Aqui, de forma obscura e transparente para o utilizador, abrem-se portas e recursos que por norma estão vedados ao exterior. A troco de *software*, expõem-se identidades, documentos, senhas, dados bancários e toda a panóplia que permite que o cibercrime floresça no meio informático com graves impactos na vida das pessoas, organizações e sociedades.

É através deste tipo de mecanismo que entidades como as analisadas anteriormente na secção Ameaças, acedem aos registos e a outro tipo de informação que permite seguir

utilizadores, vigiar os seus comportamentos, seguir as suas atividades e saber em última instância onde estes estão sediados.

Nos pontos seguintes são analisados sistemas operativos e aplicações informáticas que permitem ser uma solução à grande parte do problema acima descrito, pelo menos para as pessoas que privilegiam a segurança ou necessitam de se manter anónimas e seguras *online*, quer seja de pessoas próximas que são uma ameaça à sua integridade, quer seja de entidades que pretendem censurar e controlar a informação ou o acesso a esta.

2.4.1 Sistemas operativos seguros

Existem múltiplos sistemas operativos que conferem mais ou menos segurança ao utilizador. Existem os sistemas mais comercias, comummente vistos em arquiteturas x86 e x64, que primam pela beleza e deixam a segurança informática a cargo de terceiros que vendem aplicações para esses sistemas. Embora esta seja a realidade, quando se trata do prestígio de um *software*, as marcas fabricantes apressam-se a lançar pacotes corretivos e pacotes preventivos, como se pode observar em sistemas operativos de génese *UNIX*. Também no *Windows* estes tipos de correções existem, mas são mais espaçadas.

Atualmente, a maioria dos sistemas operativos seguros são de base *Linux* e são mundialmente conhecidos pela sua qualidade pois estão equipados com o mais recente *software* que diariamente é analisado para que a segurança do utilizador esteja sempre em primeiro lugar.

2.4.1.1 Tails - The Amnesic Incognito Live System

Dentro da classe de sistemas operativos com o propósito de garantir a segurança e o anónimato dos seus utilizadores, destaca-se o *Tails*[66]. Assente no sistema operativo *Linux Debian*, com o lema de privacidade para todos em todos os lugares, este sistema operativo é conhecido pela sua orientação paranóica (designação que se dá a sistemas operativos que prezam muito a segurança e anonimato) e por ser extremamente seguro e versátil.

Com o objetivo de preservar a privacidade e o anónimato, este ajuda no uso da *Web* de forma anónima e consegue evitar a censura imposta por conhecidos sistemas de *firewall*, sem deixar rasto a não ser que o utilizador assim o especifique, encaminhando todo o tráfego *Web* pela rede *Tor*.

Este sistema vem com uma série de aplicações pré-configuradas tendo em vista a segurança. Com recurso à rede *Tor* ou *I2P,* consegue ocultar o *IP* de forma consistente e segura.

[66] TAILS – Download https://tails.boum.org/

O uso deste sistema operativo num computador não altera e nem depende do sistema operativo instalado pois corre a partir de uma unidade de *DVD* e é único pois não permite ser instalado num dico rígido e ser um sistema operativo normal para uso diário. Todas as aplicações instaladas e dados registados e guardados no momento do seu uso perder-se-ão permanentemente após reiniciar o computador. Após a configuração da *BIOS* (*Basic Input/Output System* ou sistema básico de entrada e saída), qualquer computador pode executar o *Tails* a partir de uma *drive CD/DVD* ou dispositivo de armazenamento *USB*. Este será carregado para a memória do computador e funcionará a partir daí como se estivesse efetivamente instalado num disco rígido.

Este sistema vem equipado com sistema de criptografia para o suporte de armazenamento. Através do *LUKS* pode-se encriptar o disco de suporte para uma utilização mais segura e inclui um leque de aplicações incluídas na distribuição, a conhecer:

- **Cliente de *email*** – *Claws*;
- **Ferramenta de *chat*** – *Pidgin*;
- ***Browser*** – *Tor Browser*;

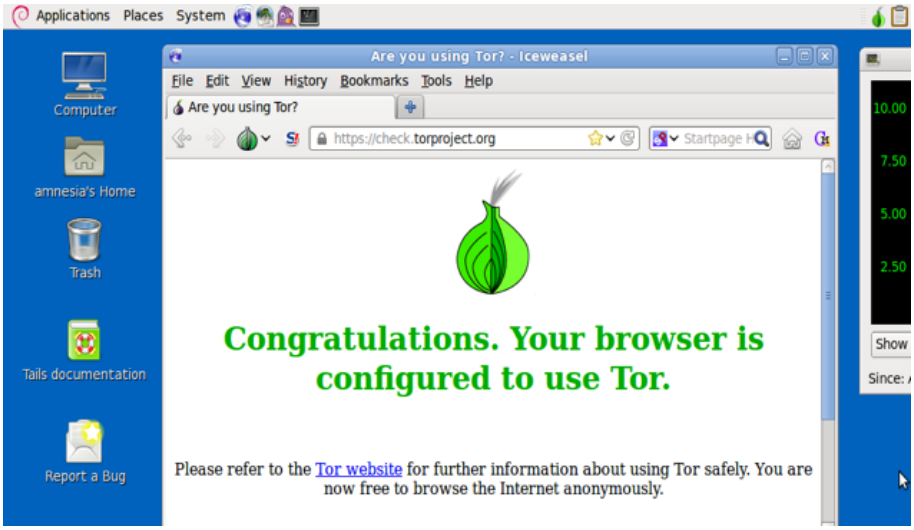

Figura 23 - Imagem do ambiente de trabalho do Tails [67]

Como características positivas tem o facto de ser um sistema baseado no *open source Debian* e bastante fácil de auditar para detetar conteúdo malicioso. Contempla algum *software* de entidades reputadas e que contribuem constantemente no panorama da segurança informática. Como características negativas tem o facto de apresentar um aspeto desatualizado e não permitir guardar de forma permanente os ficheiros em uso.

[67] Imagem recolhida no website do Tails – https://www.tails.com

2.4.1.2 JohnDo Live-DVD

Desenvolvido inicialmente pela Universidade de Dresden na Alemanha sob o nome de *JAP* (*Java Anon Proxy*), o agora *JonDonym* é muito similar ao *Tails* no modo de distribuição do sistema operativo; contudo, este produto destaca-se por ser uma versão comercial de segurança informática. Assente numa rede de servidores *proxy*, funcionam de forma similar ao *Tor* com dois níveis de fornecimento de serviços, gratuito e *premium* (versão melhorada), que encriptam a informação a cada passagem de informação por cada nó. O *JonDonym* assenta num princípio diferente das redes *P2P* (*peer to peer ou* ponto a ponto*)* nos quais se baseiam o *Tor* e o *I2P* ao manter os seus nós anónimos. Ao contrário do *Tor* que estabelece uma rede *VPN* distribuída por todos os servidores de forma anónima, esta versão alega ser mais fiável pois existe a certeza a cem por cento da propriedade do nó. Na rede *Tor,* qualquer cidadão pode programar e disponibilizar um nó de acesso ou de saída para a rede não encriptada, tornando o sistema potencialmente vulnerável se entidades menos confiáveis que decidirem criar os seus nós com intuito de analisar o tráfego.

O *LiveDVD* do *JonDo*[68] vem devidamente configurado para o uso desta rede proprietária assente no ambiente seguro que é a distribuição de *Linux Debian*. Este também disponibiliza uma série de *software* que permite a comunicação de forma segura, tal como o *browser* dedicado *JonDonym* e o *TorBrowser*.

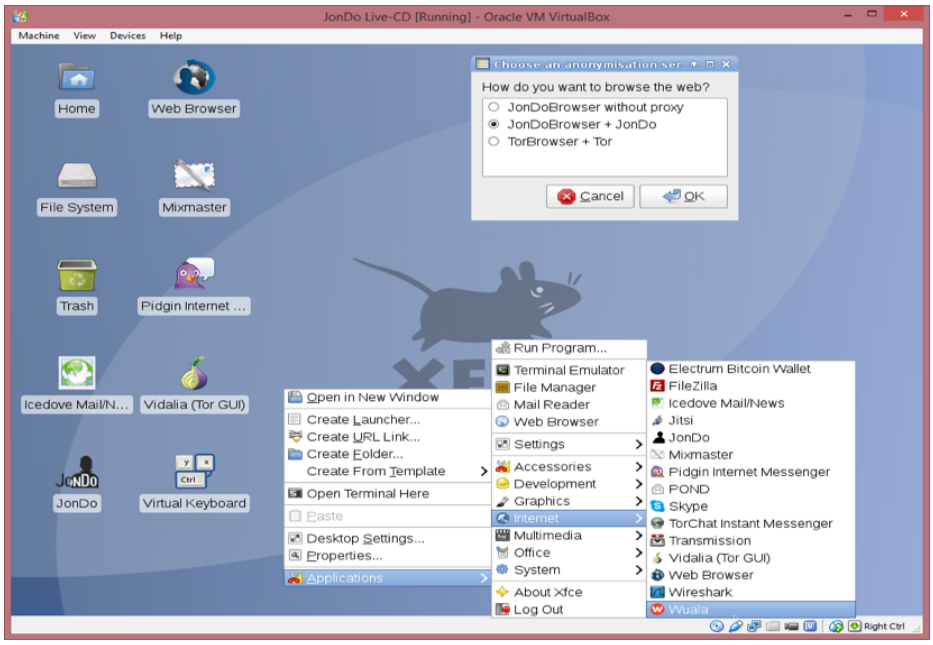

Figura 24 - LiveDVD do JonDo e das opções que dispõe [69]

[68] JonDo Live DVD – Download https://anonymous-proxy-servers.net/en/jondo-live-cd.html
[69] Imagem recolhida em - https://anonymous-*proxy*-servers.net/en/jondo-live-cd.html

Como características positivas tem o ambiente de *Linux Debian* e a rede *JonDonym* pré configurada. Inclui o *Tor* e algumas ferramentas de uso seguro de desenvolvidas por entidades credíveis e de renome. Relativamente ao suporte e documentação de uso, este *software* por ser um serviço comercial está bem estruturado ao nível do apoio pós-venda ao cliente. Como características menos positivas está o facto de não ser uma versão instalável e não servir para guardar de forma permanente dados do utilizador.

Na figura seguinte podemos observar o *workflow* do uso da rede baseado em cliente com conta *premium* e sem a conta *premium.*

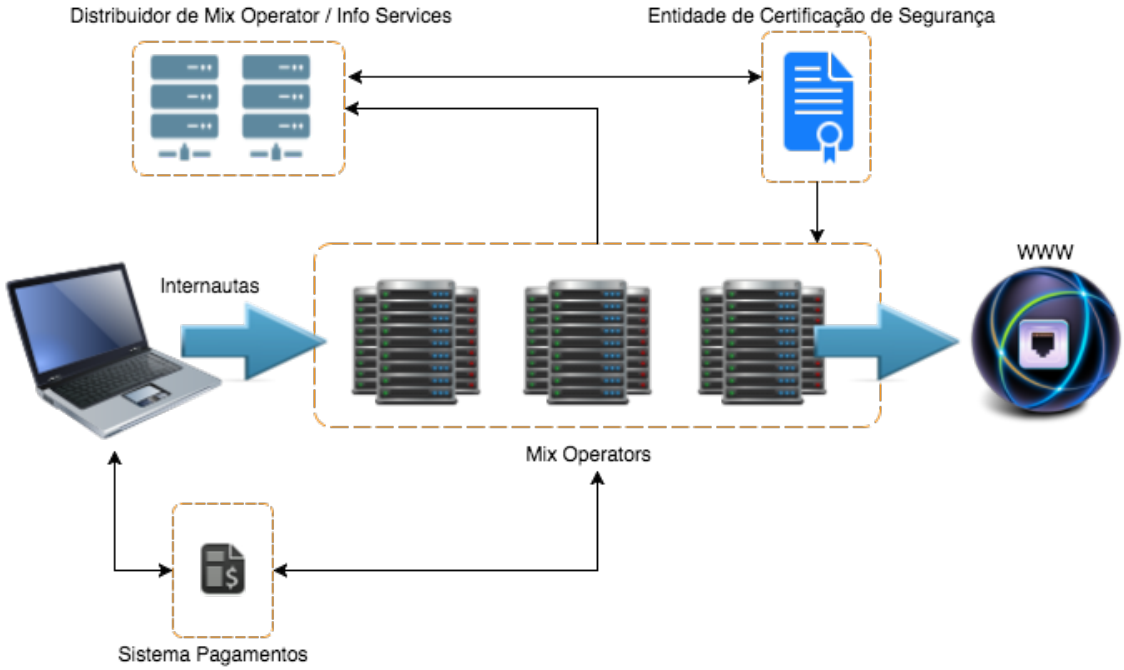

Figura 25 - Wokflow de uso da rede JonDonym[70]

2.4.1.3 UPR – Ubuntu Privacy Remix

Com origem na Alemanha, o *Ubuntu Privacy Remix* [71] é um sistema operativo de base *Ubuntu/Linux* que assenta nos pilares da segurança por isolamento e *Air Gap*. O objetivo é providenciar um sistema operativo completamente isolado de comunicações por rede. Pretende facultar um ambiente controlado para que a informação sensível esteja sempre contida dentro de um circuito específico onde apenas dispositivos encriptados podem ser usados para transferir informação. De génese não instalável, este *LiveDVD* evita qualquer acesso não autorizado ao sistema diminuindo o risco de roubo ou perda de informação pelos meios convencionais de *malware*, *trojans*, vírus e acessos não autorizados. Segundo o *Website*

[70] Imagem elaborada pelo autor

[71] *Ubuntu* Privacy Remix – *Download* https://www.privacy-cd.org/en/

do *UPR*, desde os relatos de Edward Snowden tornou-se claro que entidades governamentais seguem atentamente os internautas pelo que a ferramenta evita isso mesmo, pois para além de ser impossível ajustar ou configurar as definições base de segurança que já estão pré configuradas, todos o suporte de rede *LAN*, *WLAN, Bluetooth*, infravermelhos bem como *PPP* (*point to point* ou ponto a ponto), foram retirados do *kernel* modificado desta distribuição. Este tipo de técnica pode parecer simples de implementar apenas desligando da placa de rede sem fios; contudo, existe *software* capaz de ligar e desligar o suporte sem que o utilizador repare. Este sistema operativo possui um conjunto de aplicações e ferramentas gratuitas para o uso seguro e comum de qualquer possível utilizador, a conhecer algumas:

- **Ferramentas de produção** – *LibreOffice e Latex;*
- **Aplicação de edição de imagem** – *Gimp;*
- **Ferramenta de edição de vídeo** – *Ariste;*
- **Tecnologia de encriptação** – *TrueCript.*

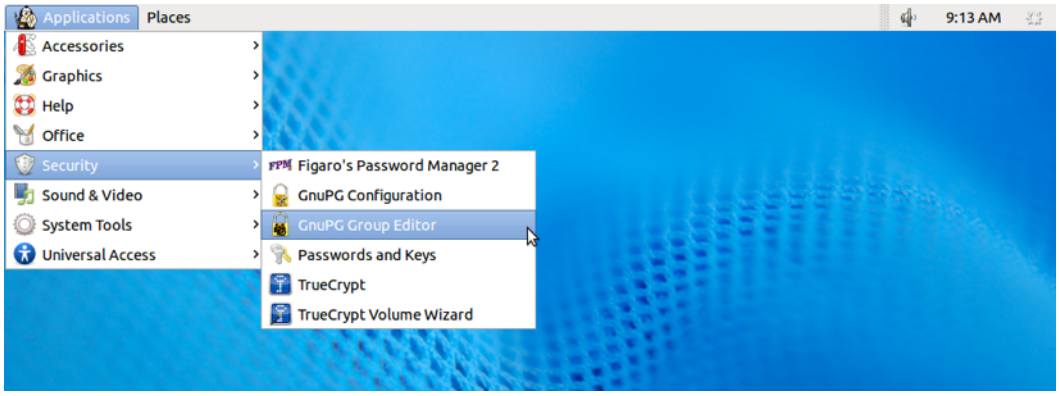

Figura 26 - Ambiente de Trabalho do Ubuntu Privacy Remix[72]

As principais características enaltecidas desta ferramenta multimédia são o facto de ser um sistema de leitura, uma vez que não permite ser instalado e todos os dispositivos de armazenamento são encriptados em contacto com o sistema. Para além de ser bastante *user friendly* (simples de usar), tem por base a distribuição *Ubuntu* e é imune a infeções por *software* malicioso pois é apenas um sistema de leitura e não escrita. Como principais desvantagens está o facto de não permitir a navegação *Web* segura ou outra qualquer.

[72] Imagem recolhida em - https://www.privacy-cd.org/en

2.4.1.4 IprediaOS

O *Ipredia OS* [73] é um sistema operativo extremamente funcional, rápido e estável. Assente numa distribuição *Fedora Linux*, faculta uma solução de navegação anónima incluindo *email*, *chat* e partilha de ficheiros *online*.

Figura 27 - Sistema Operativo IprediaOS[74]

Contrariamente às soluções analisadas anteriormente, esta versão não usa a rede *Tor* para comunicações encriptadas, mas sim o protoloco *I2P* para permitir o anónimato do utilizador através da sua rede *VPN*. Esta solução permite a sua instalação, bem como o uso em *LiveDVD,* sendo apenas desejável escolher o *GUI* de ambiente de trabalho, *Gnome* ou *LXDE*. Na versão mais recente e disponível para *download*, um elevado leque de ferramentas é facultado ao utilizador que vai desde cliente de *Bit Torrent*[75], editor de texto, calendário, visualizador de *PDF*, cliente de *email,* entre outros devidamente seguros. No ambiente de trabalho ainda é disponibilizado um sistema de *chat* (conversação) seguro, *IRC* através da Rede *I2P* e o *browser Firefox* devidamente configurado para navegação anónima. O uso desta ferramenta como *LiveDVD* pode ser utilizado com toda a segurança e pode também ser instalado diretamente no computador de um possível utilizador.

Este sistema operativo possui um conjunto de aplicações e ferramentas gratuitas para o uso seguro e comum, a conhecer:

- **Calendário** – *Osmo*;
- **Aplicação de *chat*** – *XChat*;
- **Protocolo de partilha *P2P*** – *Bit Torrent Robert*;

[73] ImprediaOS – *Download* http://www.ipredia.org/os/*download*
[74] Imagem recolhida em - http://www.ipredia.org/
[75] Bit Torrent – Sistema de partilhas de ficheiros P2P - http://www.bittorrent.com/

- **Cliente de *Email*** – *Sylpheed*;
- **Sistema de análise de rede** – *Wireshark*;
- **Teclado virtual** – *eekboard*;
- ***Browser*** – *SE Linux Alert.*

Uma vantagem saliente é a possibilidade de usar a rede *I2P* para fazer a partilha de ficheiros ou a receção dos mesmos por *bit torrent*.

As principais características positivas são o uso da rede *I2P*, o uso generalizado das ferramentas facultadas de forma confidencial e a possibilidade de dois interfaces específicos, o *Gnome* e o *LXDE*[76]. Como aspetos menos vantajosos está o facto de ser um sistema operativo "ligeiramente" simples e incompleto para substituir plenamente um sistema operativo comum, como por exemplo o *Windows* ou *Mac OS X*.

2.4.1.5 Whonix

O *Whonix*[77] é um sistema operativo assente no isolamento (*AirGap*) mas com a diferença dos sistemas operativos abordados anteriormente, pois este apenas trabalha dentro de uma máquina virtual (*VirtualBox*[78]), de forma a assegurar que as fugas de *DNS* são impossíveis e que é seguro contra *malware* que descobre a localização ou o *IP* do utilizador.

Este sistema consiste em duas máquinas virtuais conhecidas por *Gateway* e *Workstation* que correm num qualquer sistema operativo em cima de uma plataforma de virtualização, sendo a recomendada a *VirtualBox*. Cada sistema possui uma interface distinta e a base do sistema é o *Linux Debian*. Para atualizar basta usar os canais devidamente configurados para correr os códigos no terminal com o comando *apt-get-install* (comando de linguagem *Bash* que chama o repositório de *software*) pela rede *Tor*. Sempre que se inicia o sistema, este corre uma rotina de verificação de atualizações.

O objetivo é que a máquina virtual *Gateway* corra os serviços pela rede *Tor* enquanto a outra máquina virtual, a *Workstation*, recorre à anterior para endereçar os pacotes de dados. A máquina *Gateway* contém dois interfaces de rede, um para comunicar com a rede *Tor* via *NAT* (*Network Adress Translation*) e o outro para comunicar como rede interna, rede isolada (rede no próprio *host*). A máquina virtual *Workstation* corre as aplicações que o utilizador pretender estando conectada diretamente à rede interna da máquina virtual *Gateway*, não conseguindo contactar ou criar outra rede ou interface de rede. É deste modo que as comunicações se

[76] O LXDE é um ambiente gráfico para Linux - http://lxde.org/

[77] Whnix – Download https://www.whonix.org/wiki/Main_Page#Download_Whonix

[78] VirtualBox – Plataforma de virtualização de hardware e sistemas operativos - https://www.virtualbox.org/

tornam seguras pois, para além de se tratar de máquinas virtuais ajustáveis a cada sistema anfitrião, todas as comunicações do utilizador passam por uma rede privada e depois encaminhadas pela rede *Tor*, encriptadas a 100%. Através desta técnica não há forma das aplicações que existem nativamente na distribuição ou instaladas pelo utilizador, consigam conhecer o tipo de *hardware* disponível no sistema base, nem conhecer mais algum *IP* que o da rede interna. É importante salientar que este sistema não é amnésico, ou seja, não esquece informação de uso anterior a não ser que se corra sempre uma instância nova. A figura 28 ilustra a arquitetura de funcionamento das comunicações nesta distribuição *Linux*.

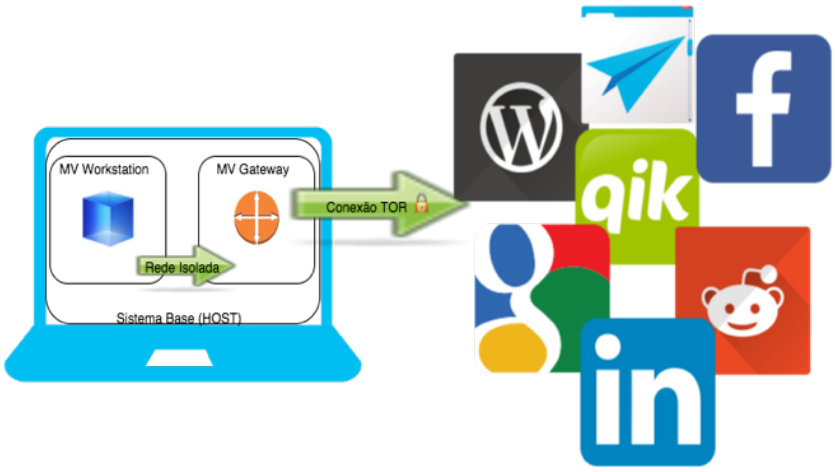

Figura 28 - Diagrama de Arquitetura Whonix[79]

Este sistema operativo possui um conjunto de aplicações e ferramentas *open source* para o uso seguro e comum de qualquer possível utilizador, a conhecer algumas:

- **Cliente de *email*** – *Mozilla Thunderbird*;
- **Aplicação de *chat*** – *Xchat*;
- **Ferramenta de visualização de vídeos** – *VLC Media Player*;
- **Ferramenta de captura de ecrã** – *Shutter*;
- **Calculadora** – *Kcalc*;
- **Ferramenta de produção** – *LibreOffice.*

Este sistema tem como principais características o isolamento da informação em máquinas virtuais e redes próprias, e como maiores desvantagens a complexidade de configuração, algo que é inalcançável pelos utilizadores comuns. Por fim, salienta-se o facto da lentidão normal deste sistema, pois sobrecarrega o sistema anfitrião com duas máquinas virtuais.

[79] Imagem elaborada pelo autor

2.4.1.6 C3Piv, a Iniciativa Portuguesa

Com o objetivo de poder dotar os utilizadores comuns de uma ferramenta que permita responder às suas necessidades de segurança, o Centro de Competências em Cibersegurança e Privacidade da Universidade do Porto (C3P), em consórcio com a Comissão de Proteção de Dados (CNPD), desenvolveu uma *pen USB* que, segundo estes, devolve o controlo da privacidade ao utilizador, sem que este tenha que se preocupar com a configuração das aplicações.

A solução é composta por uma *pen USB* com um conjunto de *software* configurado para forçar o respeito pela privacidade do seu utilizador. Para o desenvolvimento desta ferramenta, foi usado o *site PortableApps*[80], uma plataforma *online* que é usada para distribuição de uma variedade grande de programas *portable* (executáveis sem necessidade de instalar) *open source* e disponíveis para *download*. A aplicação desenvolvida inclui, para além de outros programas relevantes, um *software* de encriptação, assim como uma pasta encriptada na *pen USB* que funciona como uma pasta segura.

Ao usar o sistema de programas *portable* permite-se que as aplicações funcionem da mesma forma que fariam se estivessem instaladas num sistema operativo, mas foram adaptadas para que toda a informação necessária esteja presente em subpastas no diretório do próprio programa, permanecendo toda a informação na *pen USB,* em vez de no computador. Esta solução permite ser usada em qualquer ponto do mundo, como por exemplo num cibercafé, com toda a segurança necessária, reduzindo ao mínimo a informação deixada nesse computador. Ao recorrer a aplicações *open source* permite a análise do código fonte por parte da comunidade, garantindo a possibilidade de pesquisa e procura de vulnerabilidades que permitam a fuga de informação.

Este sistema operativo possui um conjunto de aplicações e ferramentas gratuitas para o uso seguro, a conhecer algumas:

- **Compressor de ficheiros** – *7-Zip*;
- **Antivírus** – *ClamWin*;
- **Aplicação de leitura de PDF** – *Evince*;
- **Cliente SSH** – *Kitty*;
- **Ferramenta de produção** – *Libre Office*;

[80] Portableapps – Website de configuração de aplicações normais em versões que não necessitam de ser instaladas, http://portableapss.com/

- ***Software* de telephone Voip** – *MicroSip*;
- **Browser** – *Tor* e *Mozilla Firefox*;
- **Cliente de *email*** – *Mozilla Thunderbird*;
- **Ferramenta de *VPN*** – *OpenVpn*;
- **Aplicação de *Chat*** – *Pidgin*;
- **Media Player** – *VLC*;
- **Cofre de *passwords* –** *Kee Pass*.

Esta aplicação foi noticiada por alguns canais informativos nacionais [Filipa Sousa, 2014] quando foi disponibilizada ao público. Pode-se fazer o *download* diretamente do *Site* da *CNPD* ou pelo portal do *C3P*.

Na figura seguinte, pode-se observar o conteúdo da *pen USB*.

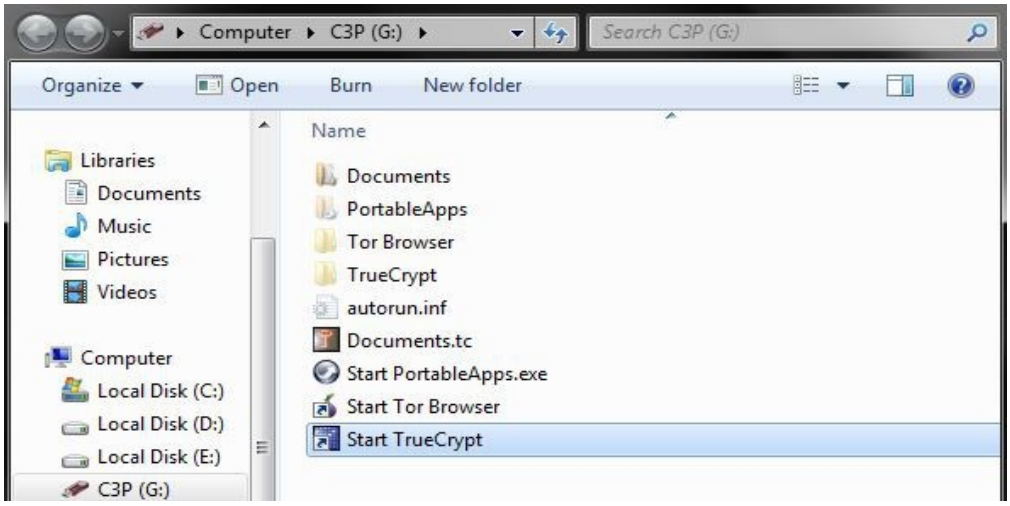

Figura 29 - Conteúdo da pen usb C3P[81]

Como principais características positivas do C3Piv[82] está o facto de possuir um leque enorme de aplicações configuradas para o uso a partir da *pen USB*. Como aspetos menos positivos estão a impossibilidade de uso em qualquer sistema operativo, pois o programa de configuração da *pen* é um executável *Windows*, deixando de fora a configuração no *Apple OS X* e no *Linux.*

[81] Figura 29 recolhida em - http://www.c3p.up.pt/c3priv/

[82] C3Piv – Download em http://www.c3p.up.pt/c3priv/

2.4.2 Ferramentas de navegação *Web* anónima

Com o aumento exponencial do uso da *Web*, também aumenta a possibilidade de se perderem dados para terceiros pois estes atacam primeiramente os servidores onde circula a informação. Com o passar dos anos, desenvolveram-se poderosas ferramentas que servem como contramedida. Existem também na *Web* serviços de *proxy*, uns gratuitos e outros com custos para os utilizadores, que alegam garantir a segurança e ultrapassar mecanismos de censura.

2.4.2.1 TOR

Segundo a página TorProject.org, e Roger Dingledine [Roger Dingledine, 2014] o TOR (The Onion Router) tem origem militar e foi desenvolvido em meados dos anos 90 pela mão do USNRL (*United States Naval Research Laboratory*), pelos investigadores Paul Syverson, Michael Reed e David Goldschlag, tendo como primeiro propósito proteger as comunicações das forças militares Norte Americanas. Mais tarde, em 1997, a *Darpa* desenvolveu o *Onion Router* e a versão de testes desenvolvida por Syverson, Roger Dingledine e Nick Matherson foi lançada há 12 anos. Em 2004 foi disponibilizado à comunidade o código fonte, tendo-se tornado a partir daí *open source,* e em 2006 foi criada uma organização de pesquisa científica sem fins lucrativos para manter e evoluir o *Tor*.

O principal objetivo é fomentar a segurança do internauta, mantendo o anónimato pessoal quando este navega pela *Web* ou conduz atividades *online*, protegendo-o conta mecanismos de censura e, concomitantemente, a sua privacidade. Compatível com a maioria dos sistemas operativos correntes (*Linux, Mac OX, Windows*) o *Tor* é uma rede de túneis *VPN*, sobre a *Web* desprotegida, onde os computadores dos utilizadores comuns são os *routers* desta, desde que operacionalizem nos seus computadores a versão de distribuidor de rede. Os utilizadores que usarem apenas o *Tor browser* ou outro, desde que contenha um *plugin* para permitir o uso da rede, serão apenas clientes desta rede anónima, que tem por base o domínio .*onion*.

O seu funcionamento é bastante simples e em camadas (daí a ligação com a analogia da cebola). Com recurso a um programa cliente (*Tor Bundle*) previamente instalado no computador de um qualquer utilizador, este funcionará como um *proxy socks 5*, que é um conhecido protocolo de *Internet* desenvolvido por David Koblas em 1992 [Elizabeth Zwicky, 2000]. Este encaminha todos os pacotes de dados entre cliente-servidor, por um servidor *proxy socks5*.

Na imagem seguinte podemos observar a representação esquemática de um servidor *proxy*.

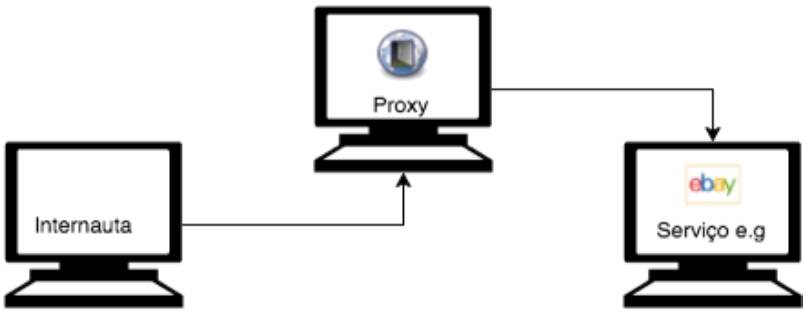

Figura 30 - Representação esquemática de um servidor proxy[83]

A partir desse ponto, todo o tráfego do computador através do túnel *http* da rede *Tor* é encaminhado até ao destino de forma segura e encriptada. Se o internauta pesquisar a sua localização com recurso a *websites* de triangularização de localização por *IP*, como por exemplo, *http://myip.is*, poderá verificar que a sua localização estará agora noutro local que não onde fisicamente se encontra. O local que retornará dessa pesquisa será a localização do servidor de saída da rede *Tor*, em qualquer lugar do mundo. A rede automaticamente gere a localização e o nó de saída de forma automática e em função da carga na rede. Por configuração de base, o utilizador não consegue escolher o ponto de saída da rede pois este é gerido em função do número de computadores a "tunelar" a rede, e o número de alternativas de saída desta que é também conhecida por *DeepWeb* [Nildo Ello, 2015].

Segundo o mesmo autor, uma característica específica desta rede complexa e larga, é que diariamente tornam-se nós de encaminhamento ou saída de tráfego, um grande número de utilizadores e organizações, procedendo à instalação do modelo de servidor num computador e iniciam o roteamento do tráfego *Tor*. Isto, porém, não acontece sem alguns riscos, que serão abordados mais adiante nesta exposição.

A rede *Tor* também é um fornecedor de anonimato para outro tipo de serviços que vão para além da navegação *Web*, nomeadamente alojamento de servidores e *websites*. Servidores plenamente configurados para receber conexões de entrada exclusivamente através da rede *Tor*, são conhecidos como serviços ocultos. Um serviço oculto sobre o domínio *.onion*, recebe pedidos de de acesso mesmo atrás de *firewalls* ou *NAT*, preservando sempre o anonimato de das partes, daí a denominação "serviços ocultos".

[83] Imagem elaborada pelo autor

Na figura 31, pode-se observar o fluxo de dados entre nós da rede *Tor* e a ligação segura entre serviços ocultos na rede.

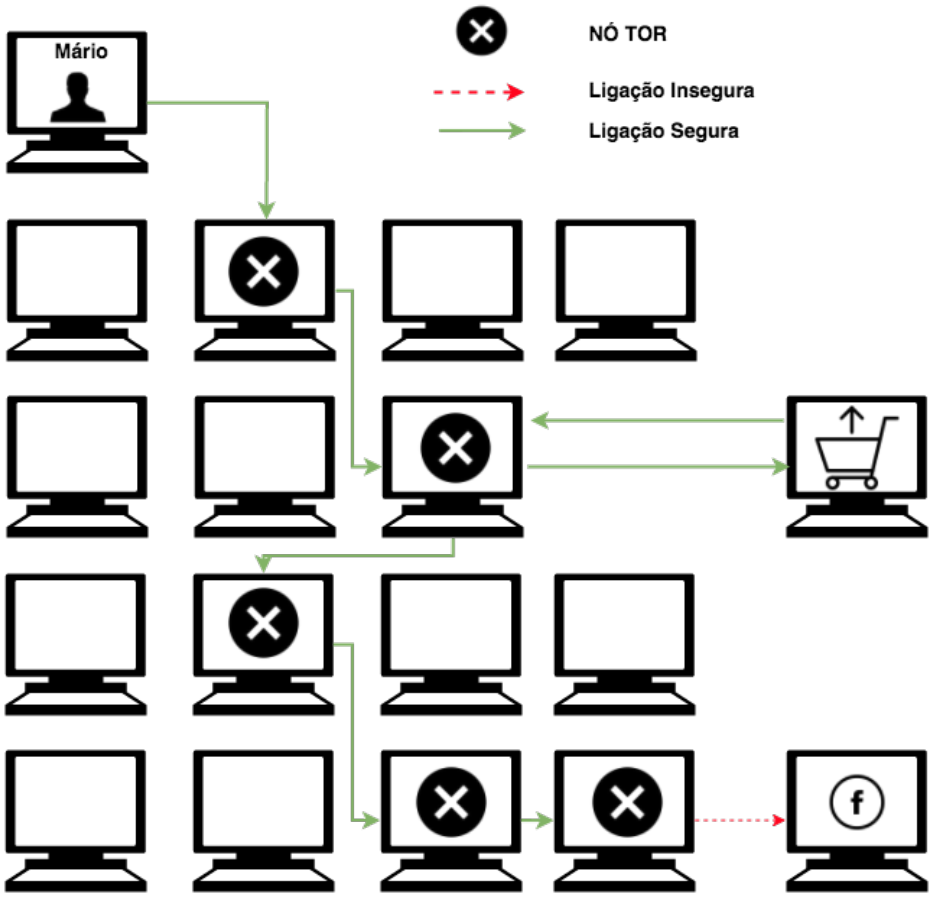

Figura 31 - Fluxo de dados entre nós da rede Tor[84]

É possível ter esta tecnologia nos *smartphones,* desde que estes sejam de tecnologia *Android*. O *software* especificamente criado para este efeito é o *Orbot* e é um *proxy* gratuito que permite utilizar a rede em perfeitas condições de segurança. Para tal, é necessário transferir para o equipamento o *Orbot Proxy* [85] e o *OrWeb*[86].

Embora seja uma aplicação considerada plenamente segura, têm sido desenvolvidos estudos por entidades universitárias e investigadores *freelancers*. A principal suspeita assenta no facto dos principais patrocinadores económicos do projeto serem agências militares americanas. Segundo Mike Power, [Mike Power, 2014], veio a público recentemente, possíveis inseguranças que conduziram ao encerramento do *Web*site de venda de serviços e produtos ilícitos *online "Silk Road",* após uma investigação informática, levada a cabo pelo *FBI* (*Federal Bureau of Investigation*).

[84] Imagem elaborada pelo autor
[85] Orbot Proxy – Download em https://play.google.com/store/apps/details?id=org.torproject.android
[86] OrWeb – Download em https://play.google.com/store/apps/details?id=info.guardianproject.browser

Analisando os documentos entregues por Eduard Snowden ao jornal *The Guardian*, verificou-se que a *NSA* estava a tentar descodificar os conteúdos encriptados e lançava ataques a nós e a utilizadores da rede, de forma a poder conhecer as vulnerabilidades desta, embora sem grande sucesso geral. A *NSA, GCHQ* e a NCA (*National Crime Agency*) recorrem a uma ferramenta chamada *Shadowcat* para desencriptar ligações ponto-a-ponto entre clientes *SSH* e *VPS* sobre a rede *Tor*, tendo como fonte dessa informação documentos[87] da *Wiki* interna dessa organização. Em setembro de 2007, o consultor de segurança Dan Egerstad [David Leigh and Luke Harding, 2013] revelou que conseguiu intercetar *usernames* e *passwords* nos nós de saída da rede *Tor* pois a informação quando sai da rede, caso o utilizador não tenha o cuidado de usar endereços *https*, está exposta.

2.4.2.2 I2P

Nascido em 2003 e conhecido como o *Invisible Internet Project* (*I2P*), é uma aplicação que permite navegar na *Web* de forma anónima e segura, fornecendo uma capa de abstração para a comunicação entre computadores. Similar ao conceito da rede *Tor*, comunicação por camadas, este difere no facto de todos os nós da rede estarem devidamente identificados numa base de dados distribuída pela rede e de o acesso a todas as funcionalidades da mesma terem um custo a suportar pelo utilizador.

O elemento diferenciador da rede *Tor* é, precisamente, o facto de toda a rede poder ser possivelmente associada a alguém ou a alguma entidade.

Cada cliente tem o seu *router I2P*, que permite a criação de túneis para tráfego *inbound* e *outbound*. São criadas sequências de dois túneis de forma eleatória para passar as comunicações entre o cliente-servidor e o servidor-cliente.

Quando o cliente envia uma mensagem (pacotes de dados) são criados dois túneis (similares a uma *VPN*) que permitem o envio de informação pela rede *I2P*. A rede em si é estritamente baseada no protocolo *IP*, mas possui uma biblioteca disponível que permite a comunicação segura sobre o protocolo *TCP*. Todas as comunicações são encriptadas de ponto-a-ponto, recorrendo a um método de quatro camadas de criptografia composto por um par de chaves-públicas. Os pacotes de dados são divididos pelos dois túneis e o recetor, que está à escuta por outra sequência de dois túneis, recebe os pacotes de dados por essas entradas.

[87] Wiki National Crime Agency - https://assets.documentcloud.org/documents/1217406/jtrigall.pdf

Na imagem que se segue, pode-se observar o modelo de comunicação segura por pares de túneis do I2P.

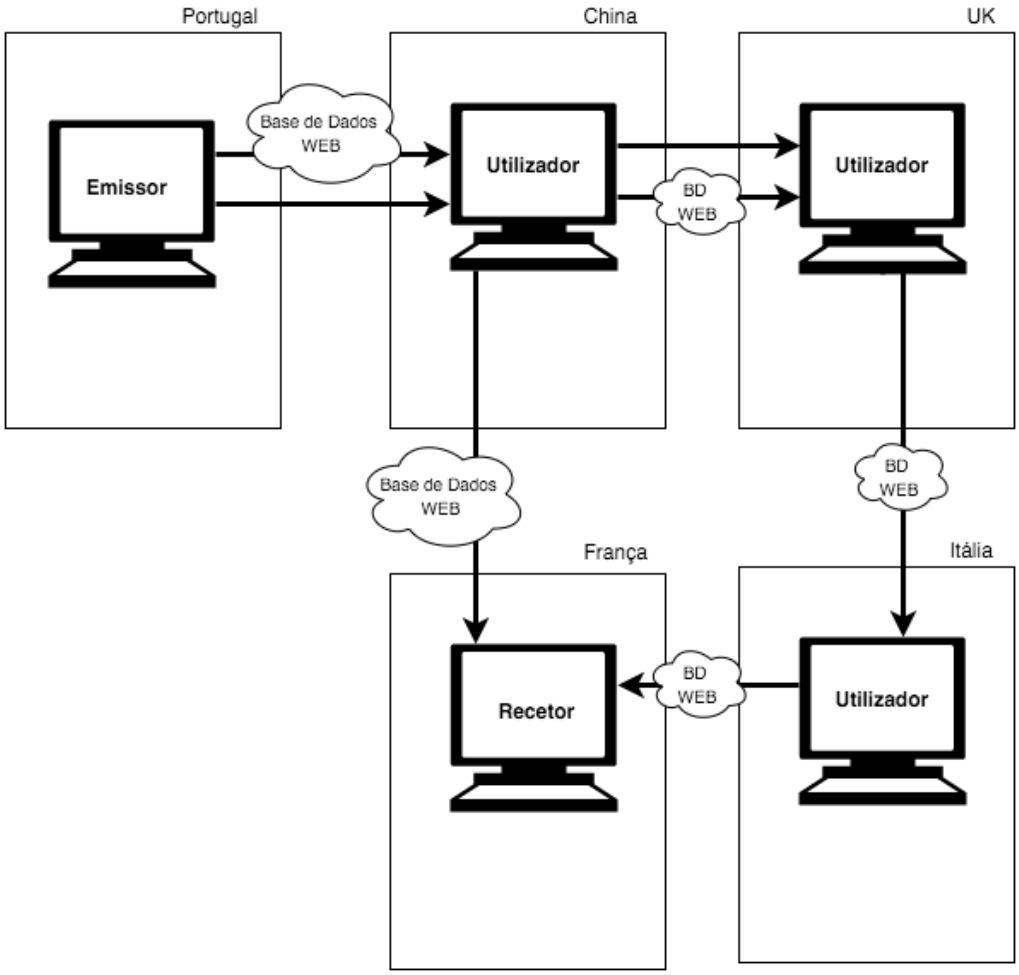

Figura 32 - Método de comunicação do I2P[88]

Cada interlocutor da rede escolhe o comprimento destes túneis e, ao fazê-lo, faz uma troca entre o anonimato, a latência e a taxa de transferência de dados de acordo com as suas próprias necessidades. O resultado desta operação permite que a mensagem passe por um número mínimo de *peers* (*routers* da rede a tunelar tráfego). Na primeira tentativa de comunicação entre cliente servidor e servidor cliente, cada cliente efetua uma consulta à base de dados encriptada e totalmente distribuída pela rede 100% encriptada para identificar seguramente os túneis de comunicação do recetor, sendo este um processo algorítmico randomizado e encriptado também. Este processo repete-se várias vezes ao longo de uma comunicação.

[88] Imagem elaborada pelo autor

3 Implementação do protótipo

"If you spend more on coffee than on IT security,
you will be hacked. What's more, you deserve to be hacked."
White House Cybersecurity Advisor,
Richard Clarke

Neste capítulo, após uma breve reflexão sobre o modelo concetual do protótipo que pretendemos implementar, são analisados os métodos e tecnologias relativos ao desenvolvimento do mesmo, é efetuada a seleção do sistema operativo base e apresenta-se a análise da criação de uma solução de raiz, escolha dos módulos que permitem ser uma resolução à problemática, instalação e análise do do seu comportamento.
Foi realizado o estudo de um sistema operativo com potencial para garantir que os serviços base corram de forma segura, isolada e com atualizações constantes. São ainda analisadas as necessidades técnicas na elaboração e planificação da construção do protótipo, testes de eficácia e de implementação.
Foram abordadas as capacidades técnicas dos principais programas disponibilizados no protótipo e as medidas de disponibilização simples dos mesmos, sem comprometer a sua utilidade.

3.1 Modelo concetual do protótipo

O objetivo, a que se propõe e se pretende apresentar neste capítulo é criar um sistema operativo virtual, diferindo das opções analisadas anteriormente, como por exemplo impedir que seja possível proceder à sua instalação numa unidade física. O principal objetivo deste protótipo é correr a partir da memória *RAM* do computador.
Pretende-se que este pode ser utilizado de forma eficiente, sendo na sua amplitude máxima um sistema operativo igual a muitos outros nas características de produção.
Este protótipo, não pressupõe várias soluções para a mesma necessidade e não contempla algum *software* produtivo, como por exemplo o *LibreOffice*[89].

[89] LibreOffice é um software produtivo open source. https://www.libreoffice.com

Contudo, pretendemos que este e outro software a gosto do utilizador, seja descarregado seguramente a partir do *Software Center*[90] (a disponibilizar). Sempre que se proceder ao encerramento do protótipo, o seu conteúdo será irreversivelmente descartado. O sistema deverá funcionar independentemente de qualquer *hardware* instalado e deve ser plenamente funcional em qualquer computador. Antagonicamente ao *Windows,* que necessita de manter a arquitetura base de *hardware* para funcionar [Tom Carpenter, 2011] o protótipo deve operar sem limites e com performance aceitável independentemente da arquitetura e máquina virtual.

Na imagem seguinte apresentamos o diagrama conceptual do protótipo e dos dois possíveis métodos de uso, *download* pela *Web* para uso direto em máquina virtual, ou uso direto pela unidade de *USB* ou *CD/DVD:*

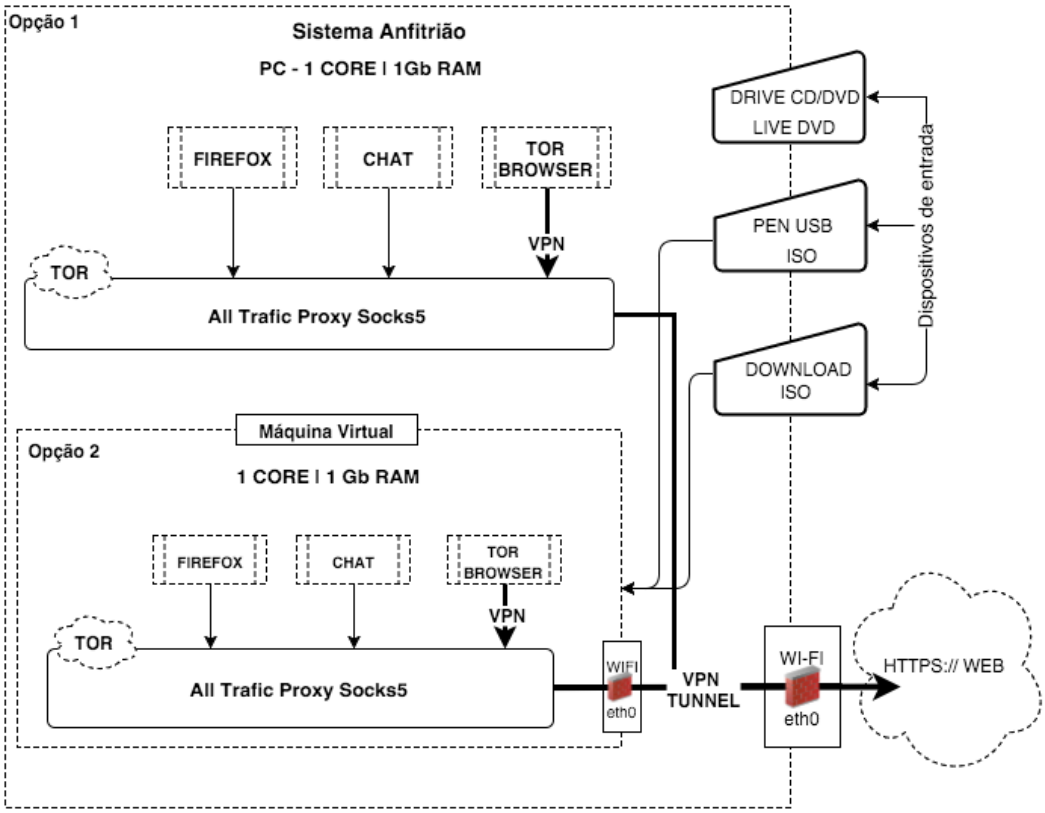

Figura 33 - Diagrama conceptual[91]

Apresentamos uma descrição do *workflow* de uso para cada uma das situações:

Opção 1 – Inicializar a partir do *CD/DVD*: o protótipo inicia, o utilizador escolhe a opção de iniciação em modo *Live*; após o carregamento dos controladores de *hardware*, o protótipo

[90] Software Center é a loja de aplicações do Ubuntu, onde estão disponíveis vários pacotes de dados e programas e, através deste aplicativo procede-se à desinstalação de programas instalados no sistema.

[91] Imagem elaborada pelo autor

comporta-se como se estivesse instalado no disco rígido do computador; para desligar, basta escolher essa opção e aguardar a mensagem a solicitar que remova o *DVD* da unidade de *CD/DVD;*

Opção 2 – Utilização a partir de uma máquina virtual: é necessário proceder ao *download* do ficheiro *.iso* a partir do repositório apropriado (*https://www.dropbox.com/sh/gs2drontef4vdxo/AADIyCzLtV8-0Z4KfX3IM3HHa?dl=0*), para dentro do *host*, ou para uma *pen USB*; inicializar a máquina virtual, selecionando a opção de instalação a partir de uma imagem *.iso*; o sistema reconhece o conteúdo da imagem e automaticamente ajusta as definições técnicas. Na eventualidade de tal não acontecer, é necessário escolher da lista de opções o exemplo *Ubuntu 32Bits*, com 1Gb de *Ram* e 20*Gb* de disco rígido. Estas opções são suficientes e comuns aos *software*s de virtualização comerciais (*VMware, VirtualBox*) para *Windows*, *Mac OSX* e *Linux*. Após os passos anteriores, dentro da máquina virtual estará disponível o protótipo. Para encerrar pode-se desligar e aguardar a mensagem de confirmação da máquina virtual, ou pode-se fazer pausa, que suspenderá o protótipo. Por questões de segurança, aconselha-se a primeira opção e correr numa máquina virtual instalada num sistema operativo (*Windows, MacOS ou Linux*).

3.2 Calendarização do projeto

Após a definição do modelo conceptual para o protótipo que se pretende implementar avança-se para a fase de planeamento.

O planeamento de um projeto é a mais primordial tarefa de gestão. Permite ter uma noção do tempo necessário e despendido para a elaboração do estudo, desenvolvimento da dissertação, elaboração do protótipo, reflexão e conclusão do trabalho.

Apresenta-se em seguida um gráfico que pretende ilustar o número de dias necessários para cada uma das tarefas a realizar para a implementação do protótipo descrito na secção de anterior.

O início deste projeto é marcado pela tarefa de investigação, conhecer as necessidades e analisar que ofertas existem no mercado da segurança informática que consigam responder como solução à problemática identificada neste trabalho.

Prevendo-se que desde a fase de investigação iniciada em 15-10-2014 até à entrega final em Outubro de 2015, todas as atividades planeadas sejam concluídas.

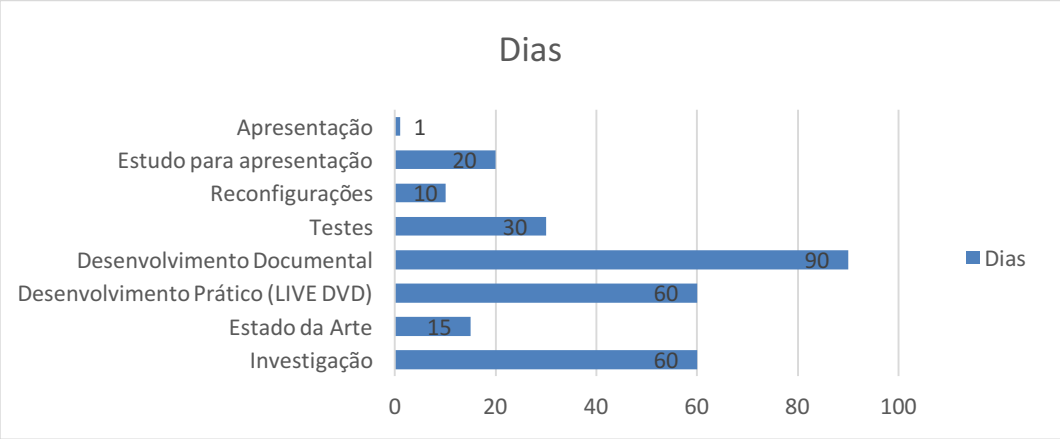

Figura 34 - Previsão do número de dias necessário por tarefa[92]

A *WBS* (*Work Breakdown Structure*) é composta por 8 tarefas principais, e que podem ser observadas na tabela nº. 4:

Tabela 4 - WBS do projeto

Tarefa	Início	Dias	Fim
Investigação	15-10-2014	60	13-12-2014
Estado da Arte	01-01-2015	15	15-01-2015
Desenvolvimento Prático (LIVE DVD)	01-02-2015	60	01-04-2015
Desenvolvimento Documental	01-03-2015	90	29-05-2015
Testes	01-06-2015	30	30-06-2015
Reconfigurações	01-07-2015	10	10-07-2015
Estudo para apresentação	01-08-2015	20	20-08-2015
Apresentação	2015	1	2015

Estas tarefas decorrem intercaladas com as aulas das unidades curriculares do mestrado em curso, compreendidas num espaço temporal aproximado de 250 dias.

Após uma fase de estudo relacionada com o estado da arte iniciou-se o desenvolvimento do produto técnico. Prevendo-se após essa fase a realização de inúmeros testes para validação, seguidos de um período de reconfigurações e ajustes.

Posteriormente, os resultados do presente estudo foram colocados no presente documento.

[92] Imagem elaborada pelo autor

3.3 Metodologia

Este projeto consiste numa análise sintética à segurança informática, ameaças, soluções e respetivo desenvolvimento de uma distribuição *DVDLive Linux,* contendo as mais recentes tecnologicas para permitir que o utilizador consiga navegar na *Web* anonimamente, sem a possibilidade de ser revelada a sua localização geográfica. Posteriormente será submetido a testes funcionais e de qualidade, bem como testes de viabilidade e segurança por um grupo de participantes que deverá responder por questionário, no sentido de nos ajudar a aferir se efetivamente o objetivo foi alcançado.

O protótipo deverá ficar disponível como um *LiveDVD*, podendo ser usado diretamente a partir da unidade de *CD/DVD*, ou procedendo-se ao *download* da imagem do protótipo e correr a partir de uma *pen USB,* ou usar dentro de uma máquina virtual.

Devido ao facto de os computadores mais recentes não possuírem unidade de *CV/DVD* (por exemplo o *Macbook* da *Apple*), o protótipo deverá ser ajustado para ser usado de forma igualmente segura, a partir de um sistema de virtualização de *hardware* e sistemas operativos, vulgarmente conhecido por sistema de máquina virtual.

Nesta fase foi possível verificar que existem várias soluções gratuitas para o utilizador doméstico tais como: *VirtualBox*, *VMware Player* e *Vmware Workstation*.

Com o objetivo máximo de disponibilizar todas as tecnologias para que estas podessem ser úteis, mas mantendo a segurança, não se pretende fazer uma análise minuciosa de todo o processo de criação e configuração, contudo, deverão ser explanados os passos gerais e o seu resultado.

3.4 Problemática

Como foi analisado anteriormente, o problema persistente é a não-privacidade ao usar a *Web*. Desde sistemas operativos a aplicações que partilham informações com terceiros, existem também as entidades que se dedicam a capturar, guardar dados, coletar a localização dos internautas, espionar os seus hábitos e conversas. Também a existência de grandes *firewalls* coordenadas por entidades governamentais com o objetivo de não permitir o acesso livre a *websites* e outros recursos da *Web.*

Existem também regras impostas pelas autoridades reguladoras das comunicações, como é exemplo em Portugal a Anacom, que por diretiva legal impossibilitam o acesso a *websites* de partilha de ficheiros *torrent* como o *Piratebay*[93].

Um dos maiores problemas no uso das tecnologias de informação são os piratas informáticos que procuram obsessivamente vulnerabilidades na *Web* e um meio de ganhar dinheiro à custa de pessoas e empresas incautas. Como analisado já neste trabalho, o número extenso de ataques e mecanismos de invasão coloca os sistemas mais comuns na linha da frente, algo que este protótipo pretende contornar, por ser na sua génese um sistema que esquece todas as ações dos utilizadores após ser reiniciado.

O protótipo a desenvolver permite ainda, com o recurso a tecnologia diversificada, ultrapassar os limites descritos, bem como ser uma solução segura para as vulnerabilidades do uso quotidiano da *Web* e ser também uma solução única pois recorrerá a um circuito duplo para correr uma rede *Tor* dentro de uma rede *Tor*.

3.5 Prototipagem e tecnologias a usar

Existem pela *Web* várias opções de sistemas operativos para o uso diário. Praticamente, se a decisão for usar o *Linux* como sistema operativo, a lista de sistemas criados por pessoas e organizações perde-se de vista. Garantir que essas versões estão e são devidamente seguras e estanques a ataques é uma tarefa potencialmente difícil. Não obstante, existem já produtos similares, como é possível verificar neste documento no estado da arte.

Após a cuidada análise iniciou-se um protótipo de uma versão de *Linux* criada de raiz com o *Linux From Scratch*[94]*,* sendo possível verificar que a mesma não iria ser a curto prazo uma solução verdadeiramente segura. Esta tecnologia permite criar um sistema operativo do zero e com o recurso a esta entidade, garantir a certificação do mesmo, obter um reconhecimento oficial após alguns anos de testes e uso por uma amostra significativa de utilizadores. Independentemente do tempo, foi efetivamente iniciada uma versão que foi encaminhada para testes e verificação, ficando como trabalhos futuros no âmbito desta dissertação.

Considerando o panorama anterior, cientificamente correto seria escolher uma base *open source*, devidamente acreditada e testada pela comunidade e trabalhar sobre a mesma no

[93] Piratebay é um website de partilha de links onde se podem descarregar pelo protocolo de torrente, conteúdos e ficheiros de forma gratuita. http://www.thepiratebay.se

[94] LFS – Linux From Scratch ou Linux a Partir do Zero, é um método de criação de sistemas Linux baseado num algoritmo próprio de um grupo de académicos que se dedica ao Linux. http://www.Linuxfromscratch.com

protótipo. Inicialmente a opção foi utilizar uma versão do *Ubuntu Server*[95] pois esta distribuição está completamente vazia de qualquer *software* e de ambiente gráfico, sendo possível desenvolver o protótipo à medida das necessidades de segurança. A abordagem anterior mostrou ser complexa e de certa forma insegura, pois a escolha *ad-hoc* de aplicações sem ter a noção do comportamento que poderão ter com outras aplicações, poderia ser no futuro um problema de segurança, pois mais uma vez, a aferição de segurança pelo uso iria requerer alguns meses de testes e prática para aferir incompatibilidades.

Considerando o cenário anteriormente descrito, a opção foi usar a versão mais recente do *Ubuntu* para computadores cliente, e a partir daí, ir removendo todas as aplicações não passíveis de configuração e outras inúteis para o uso em forma de *LiveDvd*.

Utilizando o estado da arte, procedeu-se ao estudo individual de cada uma das ferramentas disponíveis no protótipo, quanto à sua capacidade de uso seguro e possibilidade de atualização em versões futuras. De modo geral, pretende-se instalar várias tecnologias e testar as mesmas, para verificar se coabitam em harmonia, a conhecer:

- Sistema operativo *Ubuntu 14.04 LTS* (*Long Term Support*), que tem por base o sistema *Linux Debian*;
- Ferramenta de encriptação *LUKS Cryptosetup*;
- Extensão HTTPS Everywhere para browsers;
- Cryptkeeper;
- Rede *Tor*;
- Motores de pesquisa anónima, como o *DuckDuckGo*;
- Sistema de *chat* anónimo como o *Pidgin* e *Torchat*;
- Bleachbleed;
- Vidalia;
- ClamTK;
- Chaves e senhas;
- Electron Bitcoin Wallet.

Ferramentas produtivas presentes no protótipo como:

- Audacity;

[95] Ubuntu Server – É um sistema operativo da Canonical de base Debian que está na sua origem sem qualquer software adicional instalado e por conseguinte usual no meio empresarial para solução de sistema operativo para servidores. https://www.canonical.com

- ImageMagic.

Ferramentas de desenvolvimento do protótipo:

- Macbook Pro 15";
- Windows 10;
- Mac OS X El Capitan;
- VMWare Fusion 7 Pro;
- VMWare Player;
- Ubuntu 14.04 LTS.

O protótipo desenvolvido corresponde à mesma arquitetura que os demais sistemas que se podem verificar no estado da arte. O âmbito deste trabalho é efetivamente apresentar uma solução específica, não obstante, o estado da arte mostra a coincidência entre plataformas e sistemas similares, adjacentes às Diretrizes para Distribuições de Sistemas Livres [*Free Software Foundation, 2013*]. A figura 35 mostra o diagrama funcional que é tautócrono, com a maioria dos diagramas de distribuições de *Linux* que fornecem anonimato na *Web*.

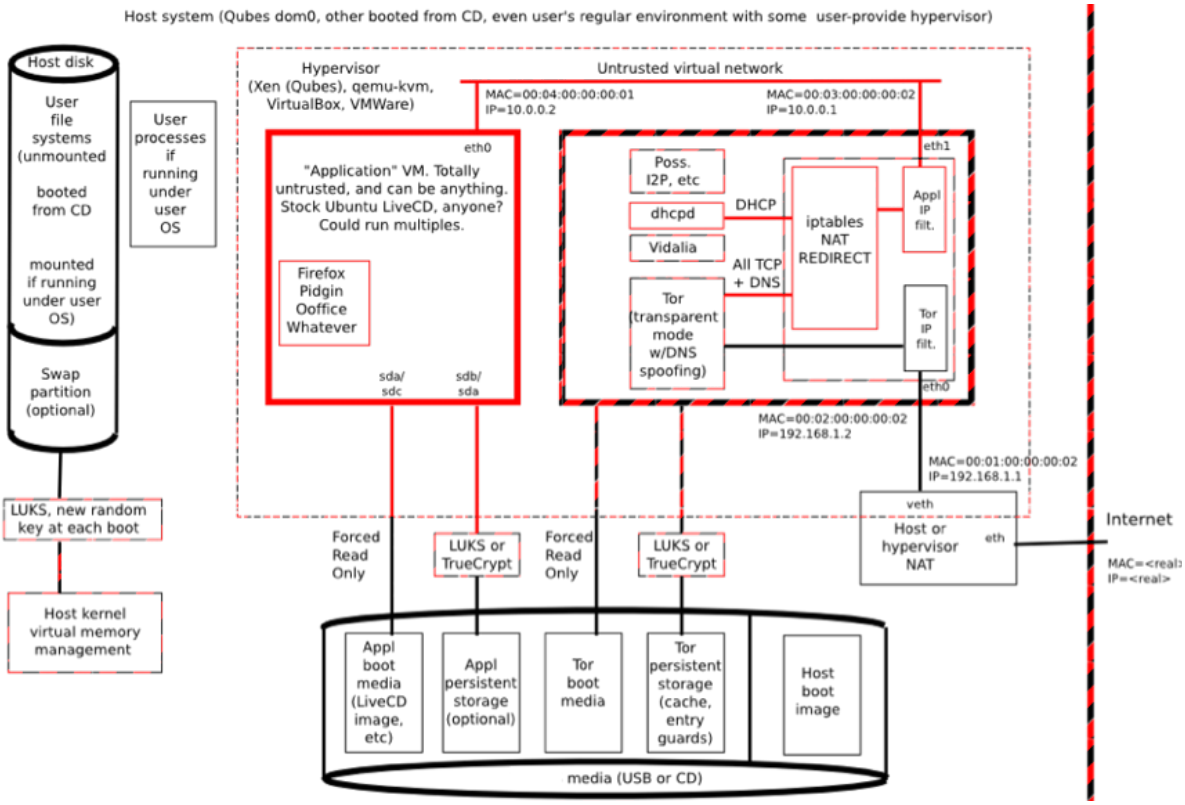

Figura 35 - Arquitetura Funcional de sistemas LiveDVD [96]

[96] Imagem adaptada a partir do original disponível em – http://www.tails.com

3.6 Preparação, desenvolvimento e configuração de ferramentas

A preparação inicial consistiu na escolha da plataforma de desenvolvimento do protótipo, que tipo de máquina de suporte, e que ferramentas seriam próprias e seguras para estarem contempladas no protótipo sem colocar em causa a performance e a segurança.

O desenvolvimento foi efetuado com recurso ao repositório na *cloud* da *DropBox,* onde estiveram armazenados os resultados e os desenvolvimentos por forma a estarem disponíveis a quaisquer máquinas de desenvolvimento.

A necessidade de criar uma ferramenta que fosse capaz de se diferenciar dos restantes produtos analisados no estado da arte levou a que o tempo de desenvolvimento do protótipo fosse abundante, tendo sido gastos sessenta dias com um investimento diário de aproximadamente 4 horas. A fase de desenvolvimento foi dividida em três fases de vinte dias a conhecer:

- Preparação;
- Desenvolvimento;
- Instalação e configuração.

Em seguida apresentam-se cada uma destas fases com mais detalhe.

3.6.1 Preparação

O trabalho de preparação consistiu no desenvolvimento de três possíveis cenários candidatos, já referidos anteriormente neste capítulo.

- O *Linux From Scratch* (*LFS*), desenvolvido no âmbito deste trabalho, foi um processo complexo e longo. Com origem dentro de uma versão de *Linux*, este consiste na criação de um repositório local onde todo o sistema operativo tem de ser assemblado e configurado. O *filsesystem* (sistema de ficheiros) final é depois compilado e preparado para ser complementado com a segunda parte do desenvolvimento desse projeto, que consiste na aplicação de um ambiente gráfico e todas as aplicações de produtividade necessárias para o funcionamento normal de um sistema operativo. O *LFS* é desenvolvido puramente com recurso a código, quer seja para criar as partições ou iniciar qualquer funcionalidade. No exemplo de código seguinte pode-se observar a criação de um ambiente de arranque (*startup*) que é necessário preparar, para que

o projeto possa correr sem problemas, e a preparação para o uso da Shell (terminal) do utilizador padrão com autorização de escrita.

```
cat > ~/.bash_profile << "EOF"
exec env -i HOME=$HOME TERM=$TERM PS1='\u:\w\$ ' /bin/bash
EOF
cat > ~/.bashrc << "EOF"
set +h
umask 022
LFS=/mnt/lfs
LC_ALL=POSIX
LFS_TGT=$(uname -m)-lfs-Linux-gnu
PATH=/tools/bin:/bin:/usr/bin
export LFS LC_ALL LFS_TGT PATH
EOF
source ~/.bash_profile
```

Como se pode observar pelo exemplo anterior, este tipo de abordagem é complexa de implementar e de perceber o estado do desenvolvimento geral, pois assenta unicamente em contexto de consola. Facilmente se ultrapassaria qualquer prazo útil para a elaboração da dissertação de mestrado. Foi efetivamente concluída uma versão inicial desta versão, que será relegada para trabalho futuro.

- O *Ubuntu 14.04 Server* foi um potencial candidato e excelente possibilidade de desenvolvimento em trabalhos futuros. A versão *Server* (servidor) é uma excelente distribuição de *Linux* pois na sua versão mais recente comporta desenvolvimentos e melhorias que, para além do prazo de suporte de cinco anos, dificilmente se encontram noutras versões de uso massivo. É verdade que no mercado existem outros exemplos como o *RedHat 7 Beta*, CentOS mas o *Ubuntu Server* é usado maioritariamente por pessoas ou pequenas empresas sem grande capacidade de investimento, criando assim um ecossistema de respostas a dificuldades espalhado pela *Web*, pois é norma dos seus utilizadores discutirem as dificuldades em fóruns [*Linux* Counter, 2015]. Acima de tudo, o referido anteriormente possui um nível de performance similar ao de alguns concorrentes, como o caso do *RedHat* 7 (versão *beta* e com custos de aquisição), verificado em testes em plataformas iguais[97].

A versão de servidor ocupa pouco espaço, não corre nativamente serviços desnecessários e não tem qualquer processo em curso ao iniciar para além dos nativos da versão, tais como o *kernel*, sessão e controladores de *hardware*.

O facto de ser uma versão já elaborada pela *Canonical* e atualmente usada em todo o mundo por milhares de sistemas de informação, não ter nativamente qualquer aplicação produtiva ou

[97] Bechmark entre Ubuntu Server 14.04 e RedHat 7 Beta - http://www.phoronix.com/scan.php?page=article&item=*Ubuntu*1404_rhel7b_test&num=1

ambiente gráfico, tornou o candidato pouco viável pela incerteza do comportamento de performance e de segurança, ao serem instaladas as ferramentas para o propósito da dissertação.

Na imagem seguinte pode-se observar o aspeto gráfico de uma versão *Ubuntu* Server 14.04:

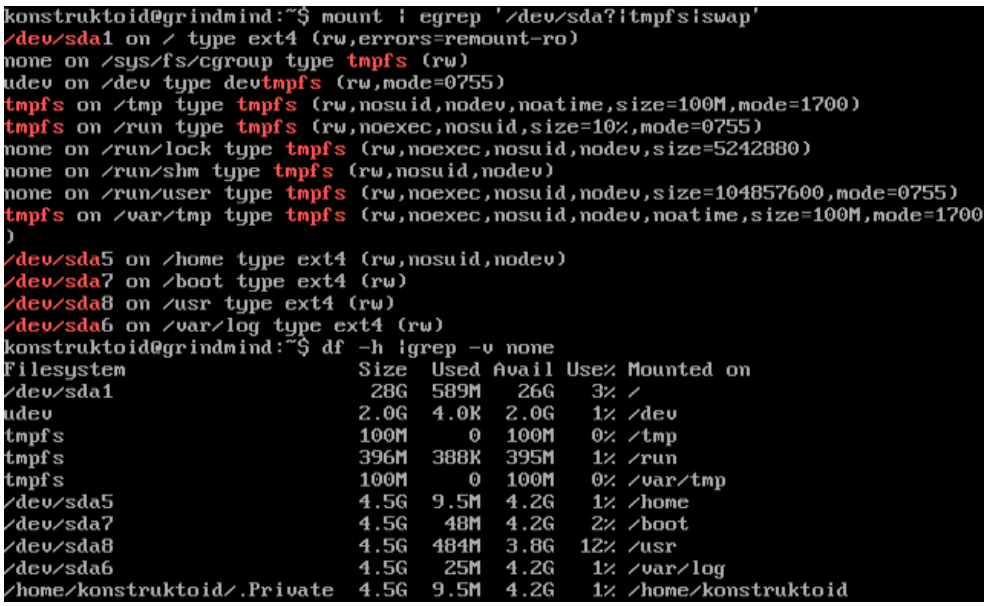

Figura 36 - Ambiente shell do Ubuntu Server 14.04 LTS[98]

- *Ubuntu 14.04.03 LTS* é a versão *Desktop* (para PC) para substituir as versões de *Ubuntu* anteriores. O *Ubuntu* 14.04.3 LTS (nome completo da versão, embora reconhecida como *14.04 LTS*) é um sistema operativo *Linux open source* propriedade da *Canonical*[99], com suporte de cinco anos e completamente gratuita, pois o seu código fonte é aberto.

Esta versão contém já um *kernel* novo (3.19) e, para além de outras novas funcionalidades, as de maior destaque são a *stack* (pilha) gráfica que permite fazer uma melhor gestão dos recursos de *hardware* gráfico e atualizações de segurança.

Nesta fase do trabalho foi selecionada a versão do *Ubuntu 14.04 LTS* a ser alterada e ajustada para que servisse o propósito final desta dissertação.

Na imagem seguinte pode-se observar o aspeto geral do *Ubuntu 14.04 LTS* e do seu ambiente gráfico nativo:

[98] Origem da imagem - http://konstruktoid.net/2014/04/25/creating-a-baseline-Ubuntu-14-04-server/

[99] Canonical é uma empresa de desenvolvimento de software e de sistemas operativos de base Linux. É uma organização de renome internacional e proprietária do Ubuntu. https://www.canonical.com

Figura 37 - Ambiente gráfico nativo do Ubuntu 14.04 LTS[100]

3.6.2 Desenvolvimento

A tarefa de desenvolvimento foi constituída por vários passos, tendo sido o primeiro a instalação da versão do *Ubuntu* escolhida no ponto anterior.

No âmbito do relato do desenvolvimento efetuado, o mesmo não será exaustivamente explanado neste ponto pois a sua extensão foi de dimensão considerável e de grande complexidade. De uma forma sucinta, seguidamente demonstrar-se-á *lato senso* o procedimento geral e passos principais.

Para o desenvolvimento foi necessário trabalhar sobre uma versão do sistema operativo *Ubuntu* para que, seguidamente, fosse possível remover os componentes desnecessários. A plataforma tecnológica escolhida foi um *Macbook Pro* 15*" Retina, Intel* i7 2.2Ghz e 16Gb de memória RAM (*random access memory*) e o sistema de virtualização de *hardware* e *software VMWare Fusion* para poder instalar o sistema operativo ajustado no decorrer do processo.

Figura 38 - Definições da plataforma de desenvolvimento[101]

[100] Imagem elaborada pelo autor
[101] Imagem elaborada pelo autor

O *VMware Fusion* é uma aplicação que permite a instalação e a utilização de um determinado sistema operativo dentro de outro sistema operativo. Comummente usado como *software* de virtualização, permite criar e executar um ou mais sistemas ou computadores (virtuais) a partir do interior de um computador *host* (anfitrião). Do ponto de vista do utilizador, este não consegue notar grande diferença entre a máquina virtual e a máquina física, desde que usadas para procedimentos normais e não de desenvolvimento de *software* ou outros programas que requeiram demasiados recursos do computador físico. Não obstante, caso o *host* o permita, podem-se sempre aumentar os recursos da máquina virtual e então obter uma experiência muito similar entre os dois tipos de máquina. Existem várias versões, dependendo do sistema operativo anfitrião e da arquitetura na máquina física.

Para o *MAC OS X* existe o *VMware Fusion* e para o *Windows* e *Linux* o *VMware Player* e *Workstation*. Na imagem seguinte pode-se observar a criação da máquina virtual utilizada no desenvolvimento do protótipo:

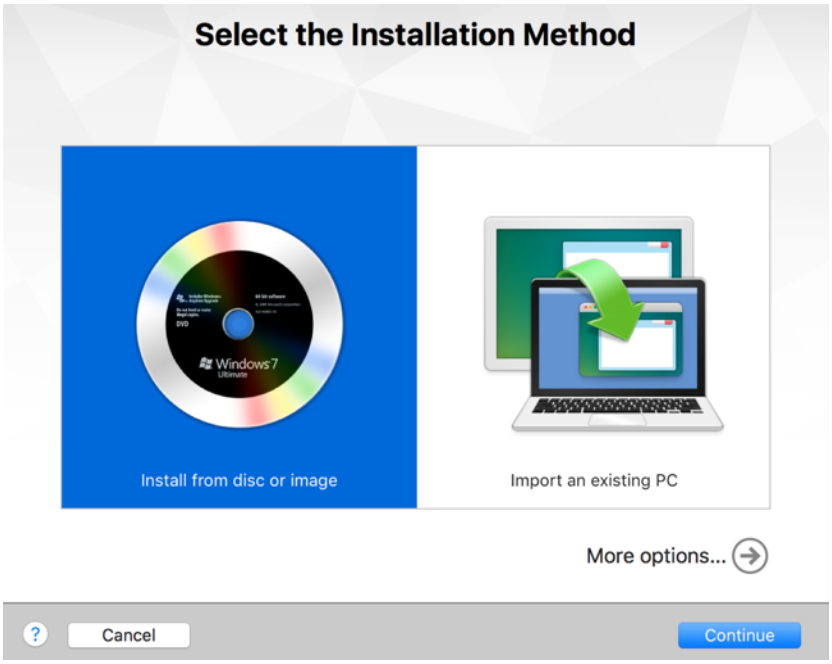

Figura 39 - Assemblagem de máquina virtual[102]

Partindo de uma imagem de um sistema operativo em formato *.iso*, e utilizar a opção de instalar a partir de uma imagem, como se pode analisar na imagem anterior.

De forma automática, o *VMware* deteta o sistema que se pretende instalar e apresenta uma série de *hardware* padrão necessário a virtualizar, como se pode ver na imagem seguinte:

[102] Imagem elaborada pelo autor

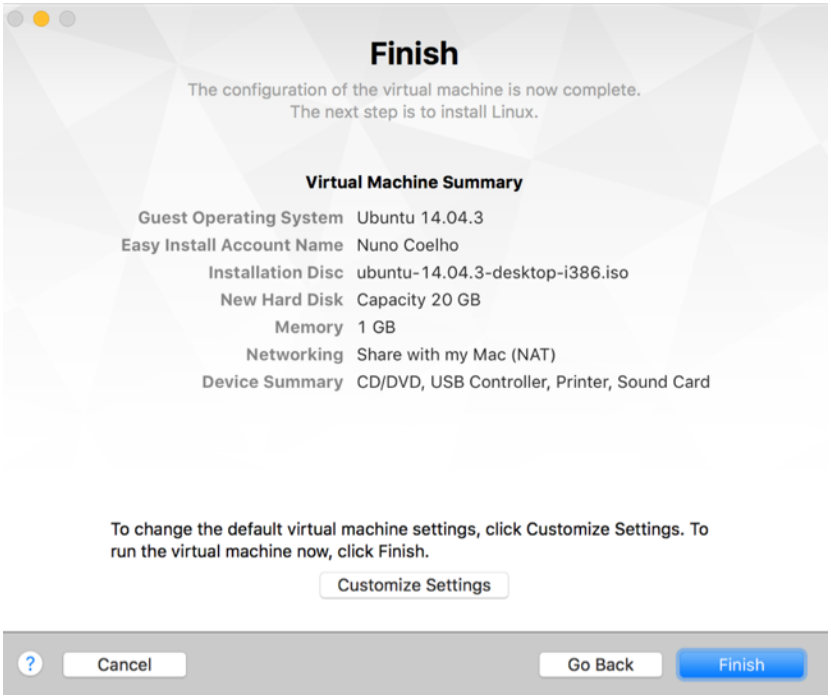

Figura 40 - Finalização da criação de máquina virtual[103]

Na imagem seguinte pode-se verificar o aspeto de uma máquina virtual dentro de uma máquina física:

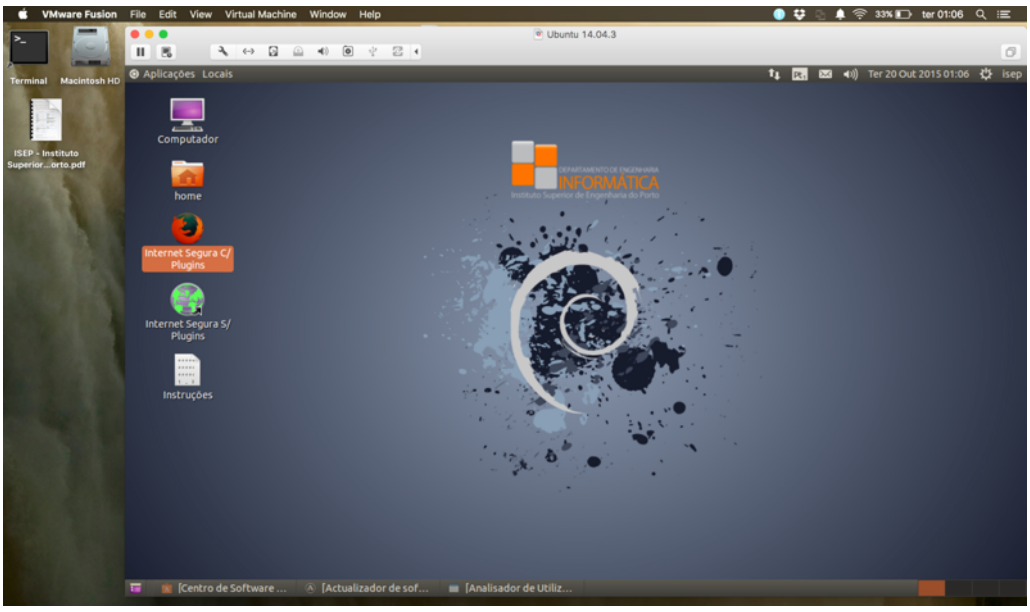

Figura 41 - Máquina virtual dentro de uma máquina física[104]

Doravante, o comportamento é similar ao da instalação de qualquer sistema operativo em que se seguem os passos de deteção de *hardware* e instalação de controladores e outro *software* padrão da distribuição selecionada. O *Ubuntu* tem um aspeto bastante *user friendly*

[103] Imagem elaborada pelo autor
[104] Imagem elaborada pelo autor

(amigável) e no processo de instalação é bastante verboso relativamente ao seu potencial e ferramentas disponíveis.

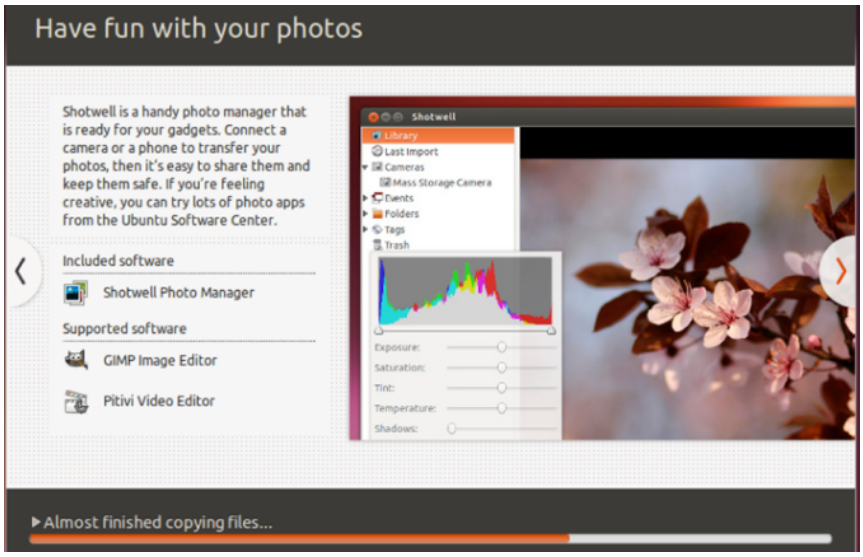

Figura 42 - Processo de instalação do Ubuntu[105]

Após concluída a instalação, foi iniciado o processo de remoção de todo o *software* adicional que necessite de comunicar pela *Web* e não permita ser ajustado nas suas preferências, de forma a utilizar a rede *Tor* para atualizar ou comunicar.

Foram removidos os seguintes itens de uma mais vasta lista de *software* excluído:

- Ambiente gráfico *Unity*;
- Thunderbird Mail Cliente;
- RythmboxPlayer;
- Vídeo Player;
- Jogos;
- Gestor de definições de aparência (temas, ícones, fontes extra, fundos de ecrã);
- Gestor de monitores (ajuste manual de cor e de resolução do ecrã);
- Hotel Photo Manager;
- Gestor de impressoras e serviço que correm nativamente associado à impressão;
- Gestor de *hardware* e de controladores adicionais;
- Sistema de estatística de energia;
- Gestor de *backups* e sistema de replicação de dados para repositório ou outro tipo;

[105] Imagem elaborada pelo autor

- Gestor de ficheiros, nomeadamente a capacidade de gestão e alteração de qualquer ficheiro que necessite de autorização *root* para modificação;
- Gestor de contas de utilizador;
- Suporte de *Webcam* com *software* de animação;
- Sistema de partilha de ecrã;
- LibreOffice;
- Suporte de idiomas para além do português, seja ele gráfico ou de recurso literário;
- Gestor de contas na rede;
- Sistema de antisspam Spam Assassin;
- Remina Remote Desktop Client;
- Sistema de digitalização.

A lista é vasta e extensa e não se limita ao anteriormente descrito pois, para que se possa proceder à instalação dos componentes necessários, primeiramente foi preciso obter um sistema operativo que não comunicasse com o exterior, a não ser que o seu utilizador assim o instruísse.

Uma vez alcançado o objetivo anterior, foi necessário proceder à instalação do serviço de *Proxy* da Rede *Tor* e configurar o *proxy* (*socks5*) para correr nativamente ao iniciar o computador. Ao contrario do *I2P* que tem de ser gerido por uma consola e tem a sua base de dados espalhada pela *Web*, o *Tor* permite a sua configuração como um serviço nativo do sistema. Sempre que qualquer aplicação inicie e necessite de comunicar via *Web*, fá-lo-á pela rede *Tor*, não expondo a localização do utilizador e circundando qualquer mecanismo de censura. Para tal foi necessário adicionar o repositório de *software* do *Tor*:

```
deb http://deb.torproject.org/torproject.org isepsafe main
deb-src http://deb.torproject.org/torproject.org isepsafe main
gpg --keyserver keys.gnupg.net --recv 886DDD89
gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add –
tar xzf tor-0.2.6.10.tar.gz; cd tor-0.2.6.10
./configure && make
$ apt-get update
$ apt-get install tor deb.torproject.org-keyring
```

Após a instalação por procedimento verificado anteriormente, foi necessário garantir que sempre que se recorre ao método *apt-get-install* (comando para instalar *software* a partir de consola) para adicionar *software*, este usa a rede de forma segura e, para tal, foi necessário editar o ficheiro *sources.list*:

```
/etc/apt/sources.list
gedit /etc/apt/sources.list
deb http://deb.torproject.org/torproject.org isepsafe main
deb-src http://deb.torproject.org/torproject.org isepsafe main
gpg --keyserver keys.gnupg.net --recv 886DDD89 gpg --export
A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -
sudo apt-get update
sudo apt-get install tor deb.torproject.org-keyring
sudo apt-get install apt-transport-tor
gedit /etc/apt/sources.list
```

O resultado evidenciado foi o seguinte:

```
# deb cdrom:[Ubuntu 14.04.3 LTS _Trusty Tahr_ - Beta i386 (20150805)]/
trusty main restricted
# See tor://help.Ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.
deb tor://us.archive.Ubuntu.com/Ubuntu/ trusty main restricted
deb-src tor://us.archive.Ubuntu.com/Ubuntu/ trusty main restricted
## Major bug fix updates produced after the final release of the
## distribution.
deb tor://us.archive.Ubuntu.com/Ubuntu/ trusty-updates main restricted
deb-src tor://us.archive.Ubuntu.com/Ubuntu/ trusty-updates main restricted
deb tor://us.archive.Ubuntu.com/Ubuntu/ trusty universe
deb-src tor://us.archive.Ubuntu.com/Ubuntu/ trusty universe
deb tor://us.archive.Ubuntu.com/Ubuntu/ trusty-updates universe
deb-src tor://us.archive.Ubuntu.com/Ubuntu/ trusty-updates universe
deb tor://us.archive.Ubuntu.com/Ubuntu/ trusty multiverse
deb-src tor://us.archive.Ubuntu.com/Ubuntu/ trusty multiverse
deb tor://us.archive.Ubuntu.com/Ubuntu/ trusty-updates multiverse
deb-src tor://us.archive.Ubuntu.com/Ubuntu/ trusty-updates multiverse
deb tor://deb.torproject.org/torproject.org trusty universe main
deb-src tor://deb.torproject.org/torproject.org trusty universe main
deb tor://us.archive.Ubuntu.com/Ubuntu/ trusty-backports main restricted
universe multiverse
deb-src tor://us.archive.Ubuntu.com/Ubuntu/ trusty-backports main
restricted universe multiverse
deb tor://security.Ubuntu.com/Ubuntu trusty-security main restricted
deb-src tor://security.Ubuntu.com/Ubuntu trusty-security main restricted
deb tor://security.Ubuntu.com/Ubuntu trusty-security universe
deb-src tor://security.Ubuntu.com/Ubuntu trusty-security universe
deb tor://security.Ubuntu.com/Ubuntu trusty-security multiverse
deb-src tor://security.Ubuntu.com/Ubuntu trusty-security multiverse
deb tor://extras.Ubuntu.com/Ubuntu trusty main
deb-src tor://extras.Ubuntu.com/Ubuntu trusty main
```

Este é um passo importante no desenvolvimento do protótipo pois, entre outros necessários, o de maior relevo é a instalação e disponibilização do serviço de comunicação por *Web* da Rede *TOR*.

Após garantir o procedimento anterior, foram novamente instaladas as aplicações e as ferramentas de produção e de utilização comum num sistema operativo.

Para ambiente gráfico de interface com o utilizador, optou-se pela utilização do *Gnome Classic* e procederam-se aos ajustes para garantir um ambiente de trabalho eficiente e mais comum à maioria dos utilizadores.

Figura 43 - Aspeto gráfico do Gnome Classic [106]

Todos os procedimentos subsequentes foram sempre executados por consola, após inclusão dos repositórios seguros, providenciando anonimato e segurança no momento de instalação e configuração.

Uma das configurações iniciais mais importantes do protótipo é a configuração nativa da *Firewall*. Aqui foram inseridas as regras que permitem bloquear todo o tráfego que esteja fora das portas definidas na *firewall*. Sem atalhos no ambiente gráfico do protótipo, esta só está acessível através da linha de comando com o seguinte comando:

```
isepsafe@Ubuntu:~$ sudo gufw
[sudo] password for isepsafe: 123
```

[106] Imagem obtida em: http://www.up*Ubuntu*.com

Na imagem que se segue pode-se verificar a configuração em uso:

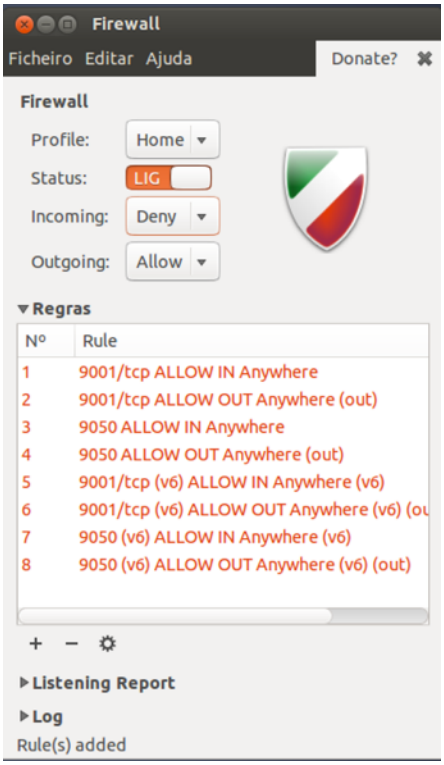

Figura 44 - Configuração da Firewall[107]

3.6.3 Instalação e configuração

A terceira fase de desenvolvimento do protótipo consistiu na instalação e configuração a partir da versão instalada no *host* e preparada anteriormente. Foram instaladas 31 aplicações que variam entre a calculadora e o *Tor Browser*. Nos pontos seguintes será possível verificar de uma forma sintética, um pequeno grupo das 31 instaladas e o seu potencial de segurança e multimédia.

Devido à extensa lista de aplicativos, apenas se demonstra onde se encontram caso se justifique, e as configurações individuais.

A primeira configuração a ser efetuada foi a instalação da ferramenta *Cryptosetup* para proceder à encriptação da partição do disco e disponibilizar ao utilizador final uma ferramenta de encriptação de dispositivos físicos. Seguidamente, pode verificar-se que aplicações estão disponíveis no protótipo bem como foram configuradas e o seu propósito.

[107] Imagem elaborada pelo autor

3.6.3.1 Encriptação do LiveDvd

Uma necessidade de extrema importância é a garantia da encriptação das unidades de armazenamento permanente, de forma a garantir que o seu conteúdo não seja passível de leitura em caso de extravio ou tentativa remota de acesso aos dados. Para garantir que este protótipo seja seguro no conteúdo, a sua preparação implica o uso das técnicas *LUKS*. Esta tecnologia consiste na encriptação de dispositivos na sua capacidade total, tal como discos rígidos, *pen USB*, e outros dispositivos de armazenamento através da implementação de encriptação com recurso a cifras aes-cbc-essiv:sha256.

Consistindo a composição deste protótipo de forma primária na configuração de um sistema operativo *Ubuntu 14.04*, todo o seu conteúdo foi encriptado para garantir a segurança na instalação inicial.

Para fazer a encriptação do conteúdo do protótipo, utilizou-se a ferramenta *Cryptsetup*.

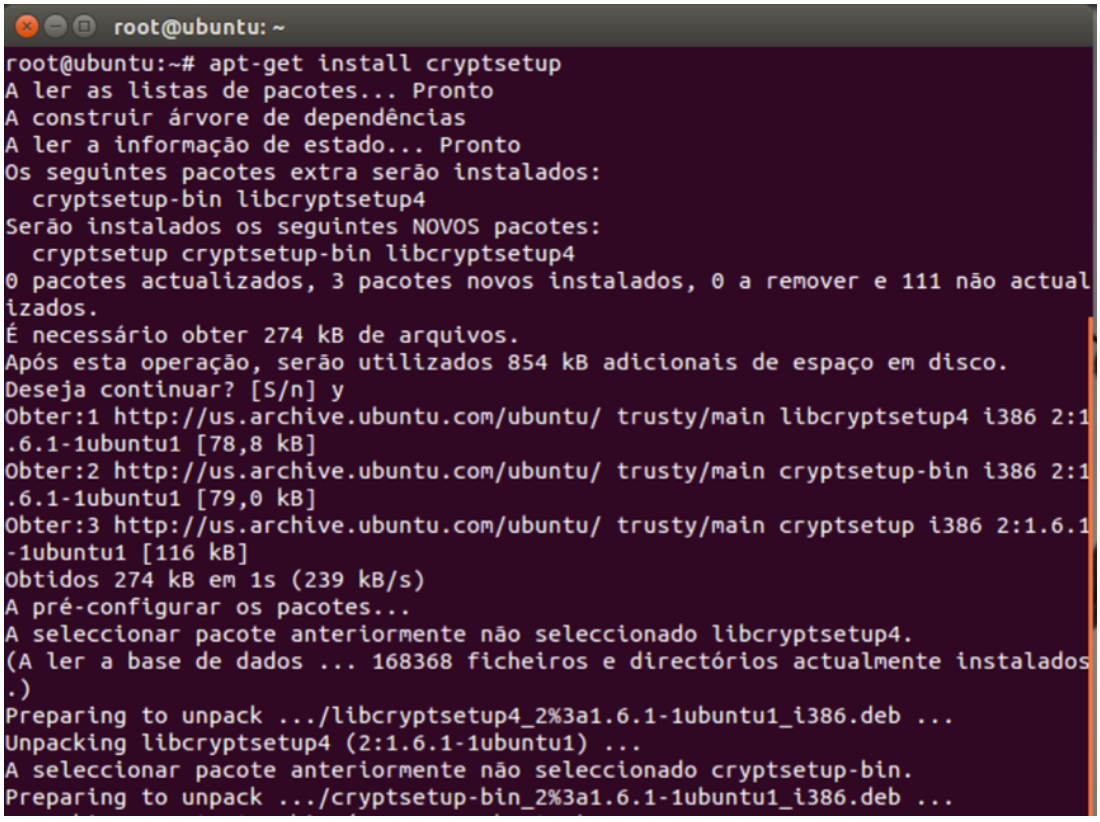

Figura 45 - Encriptação conteúdo Cryptosetup[108]

3.6.3.2 Captura de ecrã

Está disponível uma aplicação de captura de ecrã, comumente conhecida por *printscreen,* contudo a disponível permite algumas configurações. Como se pode observar na figura

[108] Imagem elaborada pelo autor

seguinte, são possíveis para além da captura do ecrã, capturar a janela de uma aplicação ou mesmo selecionar uma área a capturar. Pode ser ainda definido um intervalo em segundos para repetição do processo.

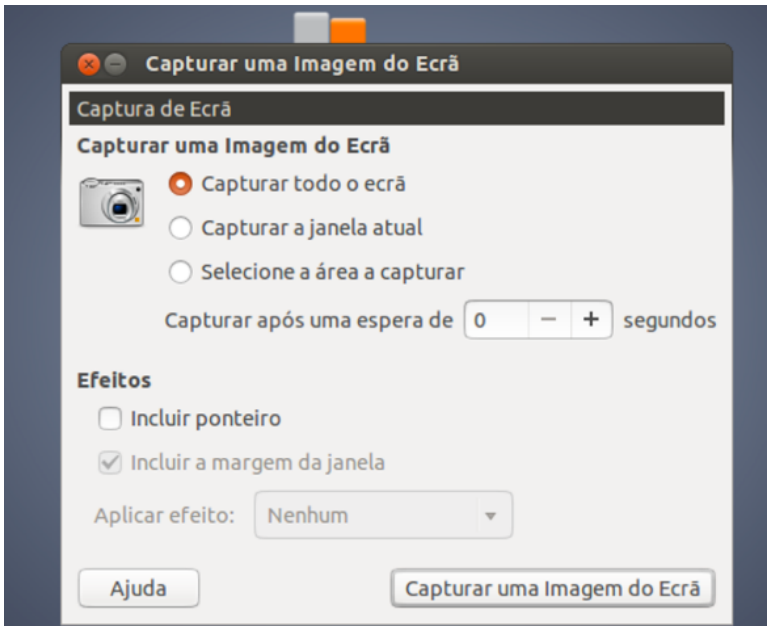

Figura 46 - Aspeto gráfico da aplicação de captura de imagens[109]

3.6.3.3 Antivírus Clam AV

Uma ferramenta de antivírus é útil e necessária, não obstante o sistema operativo ser de maior ou de menor confiança. O protótipo dispõe de um antivírus e de um mecanismo que permita atualizar o mesmo independentemente da data em que se usa o protótipo. Para atualizar o antivírus a *password* é "123".

Figura 47 - Antivírus Clam AV e mecanismo de atualização[110]

[109] Imagem elaborada pelo autor
[110] Imagem elaborada pelo autor

3.6.3.4 Analisador de utilização de discos

Para que se possa analisar o conteúdo de qualquer dispositivo *USB* de memória que seja conectado ao protótipo, foi disponibilizada uma ferramenta de análise de conteúdos.

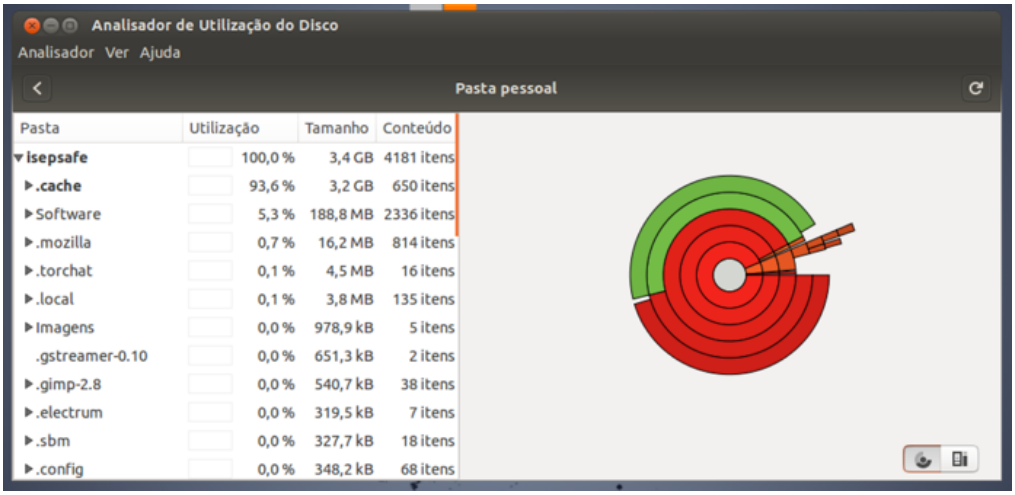

Figura 48 - Analisador de utilização de discos[111]

3.6.3.5 Cryptkeeper

Esta aplicação permite criar pastas seguras e encriptadas para poderem ser transportadas por dispositivos *USB* ou de memória.

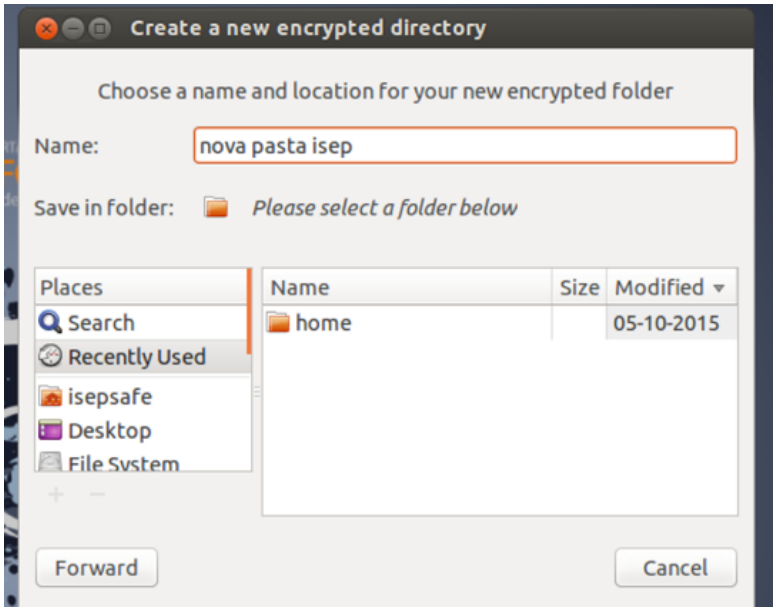

Figura 49 - Aspeto da aplicação Cryptkeeper[112]

[111] Imagem elaborada pelo autor
[112] Imagem elaborada pelo autor

3.6.3.6 Image Display

Para que seja possível visualizar imagens foi disponibilizado uma aplicação para o efeito. O *Image Display* contém ainda algumas ferramentas de edição de imagens.

Figura 50 - Aspeto do Image Display[113]

3.6.3.7 Firefox

Como principal âmbito deste trabalho está a capacidade de navegação *Web* anónima e segura. Considerando que a Rede *Tor* corre nativamente na máquina, o *Firefox* está disponível e configurado para poder utilizar automaticamente esta rede e permitir uma navegação anónima e segura. Este *browser* é disponibilizado pois o *Tor Browser,* também presente neste trabalho, tem outro objetivo que é o segundo circuito de segurança, possibilitando o acesso ao segundo nível da *Deepweb*. O Firefox permite uma utilização mais natural e similar aos *browsers* que não estão configurados para manter a segurança. Este permite a visualização de conteúdos em *flash*, permite interagir com scripts e caixas de interação com o utilizador que por norma permitem falhas de segurança e consequentemente facultar a terceiros a localização verdadeira do utilizador, a quem esteja a escutar os nós de saída da Rede *Tor*.

Embora a sua segurança não seja 100% (nada na realidade pode afirmar que o é), este *browser* tem um grau elevado de confiança e desde que não exista grande interação com o descrito anteriormente, o utilizador estará seguro.

[113] Imagem elaborada pelo autor

Na imagem seguinte pode-se observar a configuração do *Firefox* para usar o *proxy socks5* da rede *Tor*:

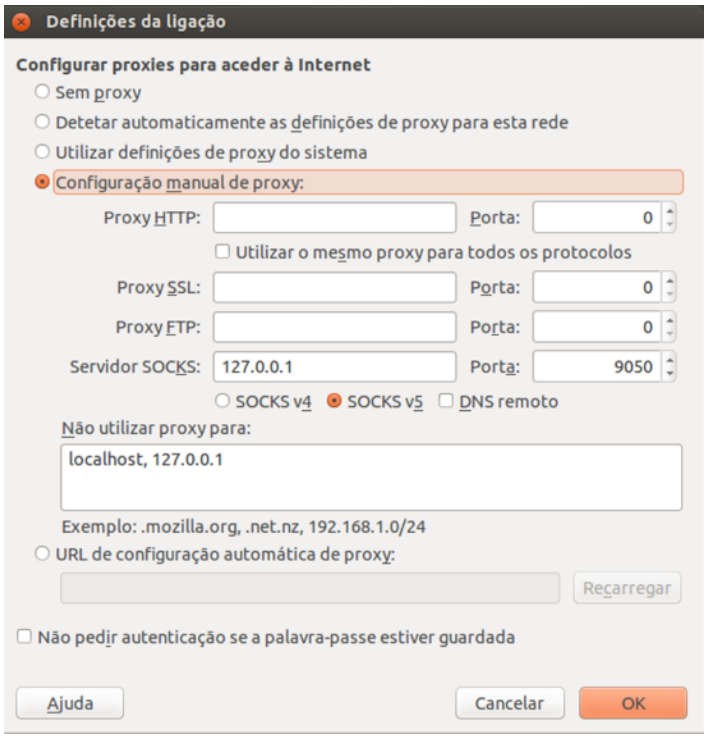

Figura 51 - Configuração Tor do Firefox[114]

3.6.3.8 HTTPS Everywhere

O uso comum dos *browsers* para navegar na *Web* é feito de forma automática para a maioria dos utilizadores. Muitos *websites* permitem que o utilizador faça a conexão por *https,* mas o desconhecimento por parte dos utilizadores faz com que não usem esta opção, pois esta requer o conhecimento da possibilidade por parte do *Website* destino. Para corrigir este tipo de situações, existem várias extensões para os *browsers* que forçam o uso da ligação por *https*, e a mais conhecida é o *HTTPS Everywhere*[115].

HTTPS Everywhere é uma extensão desenvolvida pela *Electronic Frontier Foundation* para os *browsers Google Chrome, Mozilla Firefox* e Opera, que ativa automaticamente o protocolo *HTTPS* (Hyper Text Transfer Protocol Secure ou protocolo de transferência de hipertexto seguro).

O projeto contém dois *browsers*, o *Firefox* e o *browser* do *Tor*. No *Tor Browser*, esta opção é nativa e apenas carece de alguns procedimentos de configuração, contudo no *Firefox* este não

[114] Imagem elaborada pelo autor
[115] Download em www.httpseverywhere.com

está nativamente disponível. Na imagem seguinte pode-se observar a janela de instalação da extensão.

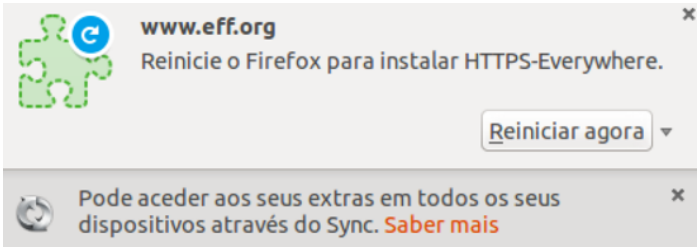

Figura 52 - Janela de instalação da extensão HTTPS Everywhere[116]

Uma componente importante do *Https Everywhere* é o *SSL Observatory,* que foi introduzida na versão 2.0.1. Este analisa o certificado digital para determinar se a entidade que emitiu o certificado é vulnerável ou foi comprometida, de forma a garantir que o utilizador não está vulnerável a ataques *man-in-the-middle*. Considerando que na Rede *Tor* podem existir vulnerabilidades no tráfego à saída da rede por não estar encriptado o *website* de destino, esta extensão assume uma importante medida de acréscimo de segurança. Na imagem seguinte, pode-se observar a janela de configuração do *SSL Observatory* e como esta informa o utilizador do tratamento que dá à informação e do propósito da existência e da configuração do mesmo.

Figura 53 - Configuração do SSL Observatory[117]

[116] Imagem elaborada pelo autor
[117] Imagem elaborada pelo autor

Na seguinte imagem, pode-se verificar que, existindo a disponibilidade de ligação *HTTPS* e sendo o certificado deste seguro, a ligação é efetuada de forma segura.

Figura 54 - Abertura automática do Website do ISEP em *HTTPS*[118]

3.6.3.9 Tor Browser

O *Tor Browser* é disponibilizado neste protótipo com duas intenções. A primeira permitir uma navegação *Web* mais segura do que a possível com o *Firefox* pois o *Tor Browser* não permite automaticamente o uso de *pluggins* como *flash*, *scripts*, publicidade e qualquer outro mecanismo de interação com o utilizador que leve à localização do mesmo. Mas, mais importante que o descrito anteriormente, este permite uma dupla camada de segurança pois o mesmo navega em cima do *proxy Tor* configurado como rede nativa. Este pequeno facto torna este protótipo único entre todos os que foram analisados no estado da arte e considerados os mais avançados sistemas de navegação *Web* segura e anónima do mercado.

Como se poderá observar na imagem seguinte onde estão lado-a-lado os dois *browsers*, a localização de não é a mesma.

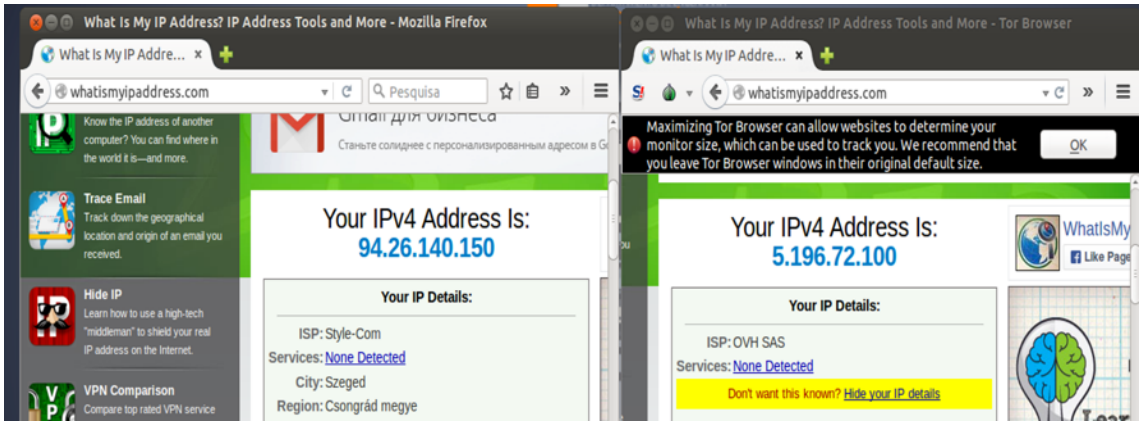

Figura 55 - Comparativo de localização entre Firefox e Tor Browser[119]

[118] Imagem elaborada pelo autor
[119] Imagem elaborada pelo autor

3.6.3.10 Ferramentas de chat Pidgin + OTR, Tor Chat e Skype

Uma forma essencial na comunicação segura entre pessoas são as ferramentas de conversação instantânea disponíveis em múltiplas plataformas. Do *Facebook* ao *Google* e ao *Skype*, são várias as opções disponíveis. Com exceção do *Skype,* que usa um sistema de comunicações ponto a ponto encriptado, a maioria das plataformas de conversação disponíveis não é segura e com recurso a ferramentas de espionagem de protocolos de rede, colocam em risco os seus utilizadores. Uma solução viável é usar um agregador de programas de *chat* (programas de conversação). No âmbito deste trabalho estão disponíveis três, *Pidgin*, *Tor Chat* e *Skype*, mas apenas se descreverá o *Pidgin*.

- ***PIDGIN*** - Desenvolvido por Mark Spencer, já reconhecido por desenvolver a plataforma de telefonia sobre IP para sistemas operativos Unix, o *Pdgin* funciona em várias plataformas, incluindo *Microsoft Windows*, *Linux*, *Mac OS X* - através da biblioteca *libgaim* e sob o nome de *Adium, SkyOS, Qtopia*. Esta ferramenta está disponível no protótipo e devidamente configurada para o uso seguro pois todo o seu conteúdo de comunicação está encriptado com recurso ao protocolo *ORT (Off the Record Messaging)*. O *OTR* é um protocolo criptográfico que encripta as conversas de mensagens instantâneas. Este utiliza uma combinação do algoritmo *AES* de chave simétrica de 128 *bits* e método de troca de chaves *Diffie-Hellman 120* com 1536 *bits*, e a função *hash SHA-1*. Além de autenticação e criptografia, *OTR* providencia um elevado anonimato e uma forte criptografia maleável. Nas seguintes imagens pode-se observar a sua localização e configurações de uso.

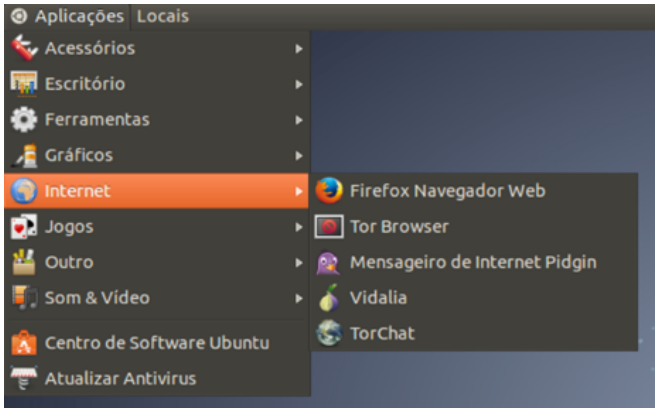

Figura 56 - Localização no menu do Pidgin[121]

[120] Diffie Hellman foi o criador de um protocolo de troca de chaves de segurança. O Diffie Hellman Protocol - https://pt.wikipedia.org/wiki/Diffie-Hellman

[121] Imagem elaborada pelo autor

Podemos escolher o tipo de ligação para que seja possível usar uma conta que habitualmente é usada noutros ambientes através dos seus protocolos, por exemplo, *Facebook, Bonjour* ou o *Google Talk*.

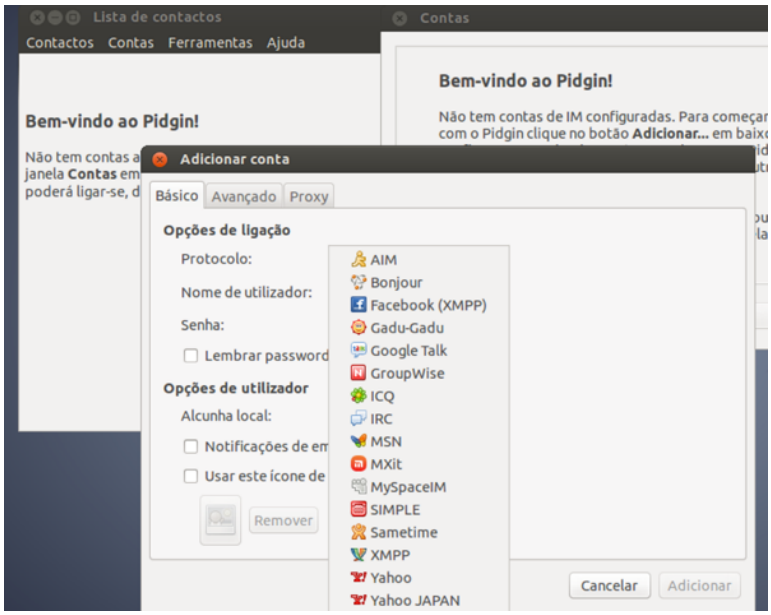

Figura 57 - Escolha do protocolo a usar no Pidgin[122]

3.6.3.11 Electrum Bit Coin Wallet

O *Electrum BitCoin Wallet* é uma carteira digital para a gestão da moeda virtual *BitCoin*. Este aplicativo, desenvolvido em 2011, é uma reputada aplicação de gestão da moeda. Com um portefólio de segurança cliente-servidor elevado, usa um conjunto de senhas privadas e públicas para manter a segurança da carteira. Está disponível neste protótipo por ser simples e seguro.

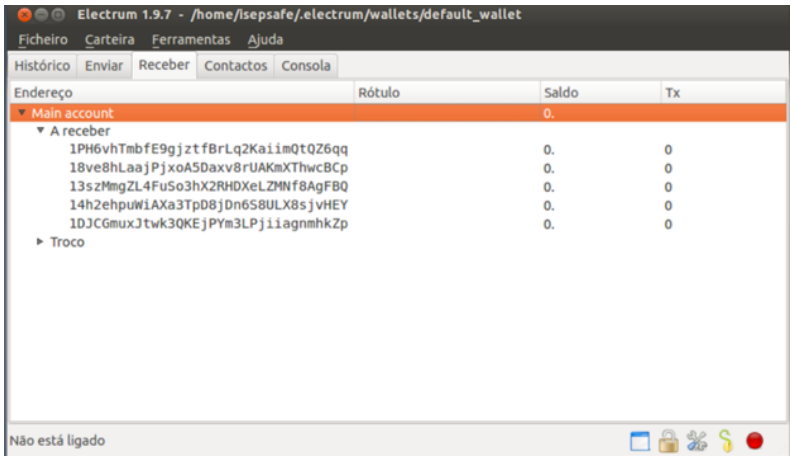

Figura 58 - Electrum BitCoin Wallet[123]

[122] Imagem elaborada pelo autor

3.6.3.12 BleachBit

O *BleachBit* é uma ferramenta que permite apagar automaticamente qualquer histórico ou dados de navegação, bem como "lixo" acumulado na cache do sistema operativo. Por ser um *LiveDVD,* este corre a partir da memória do sistema anfitrião e como os recursos são limitados, em caso de excesso poderá tornar o protótipo mais lento e mais inseguro por conter demasiada informação do uso. Para evitar ter de reiniciar o protótipo, o uso do *BleachBit* é aconselhável.

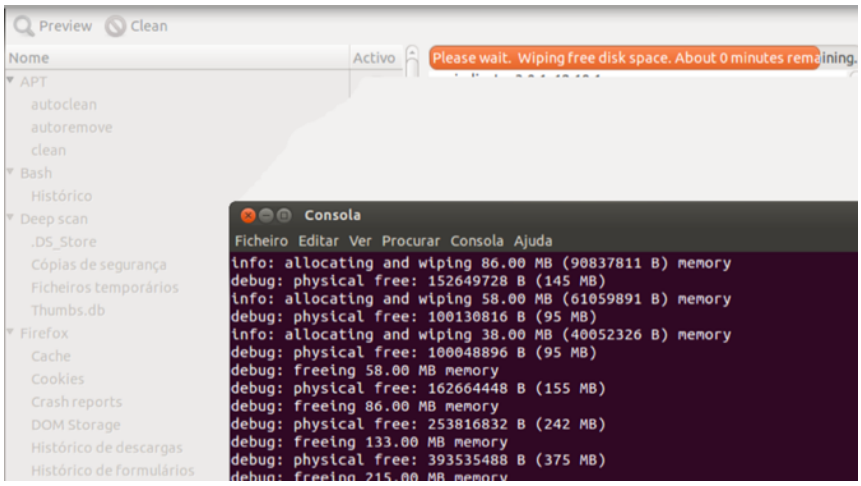

Figura 59 - Uso do BleachBit para limpar 3.2 Gb de informação desnecessária[124]

3.7 Os passos finais e resultado do protótipo

A elaboração de uma descrição completa de um desenvolvimento não é sempre simples, neste caso particular, o número de aplicações e de configurações necessárias à elaboração inviabilizam descrever todos os passos de elaboração do protótipo e descrever todas as aplicações e como interagem entre si, não obstante, o procedimento de finalização importa conhecer.

Após a conclusão de todos os passos de ajuste e configuração do protótipo, foi necessário materializar o resultado num produto. A ideia sempre foi a criação de um *LiveDVD* que permitisse integrar de forma completa todo o trabalho realizado e não só os programas, como é mais simples de fazer. O essencial foi fazer a transformação dos ajustes ao *Ubuntu* selecionado para este trabalho, em vez de fazer uma sessão *live*. De muitas opções existentes procedeu-se à materialização do protótipo a partir da linha de comandos, fazendo uma cópia

[123] Imagem elaborada pelo autor
[124] Imagem elaborada pelo autor

integral de todo o sistema, uma espécie de *backup* geral em que tudo se guarda. Um tipo de fotografia do sistema desenvolvido.

Esta fotografia foi depois transformada num ficheiro *.iso*, alcançando assim o objetivo final, que será demonstrado no ponto seguinte deste capítulo.

3.7.1 Estrutura e construção do *LiveDVD*

Importa saber que o *LiveDVD* é apenas uma estrutura que não permite a escrita. Um elemento primordial deste trabalho é precisamente a impossibilidade de escrita no suporte físico, pois assim garante-se a não contaminação dele mesmo. Uma vez que o *Ubuntu* necessitou de escrever em algumas pastas do sistema de forma a poder funcionar devidamente, como por exemplo as pastas */dev, /proc, /var, /temp,* criou-se na *RAM* os diretórios de forma a poder escrever neles, para tal usou-se o *aufs2*[125], que é um programa que permite a escrita em qualquer pasta. Uma vez desligado o sistema, perdem-se as alterações.

Considerando que o tamanho da versão final é igual aos recursos que foram atribuídos na máquina virtual, e considerando que o *Ubuntu* tem em média 5*Gb* de tamanho, recorreu-se ao *squashfs*[126] para comprimir a informação. Para montar o *root filesystem* de forma comprimida e perceber que ficheiros e serviços (como o *kernel*) iniciam automaticamente, recorreu-se ao *initramfs127*. De seguida pode-se observar o código da estrutura da árvore de diretoria do protótipo:

```
(CD ROOT)
|-------+casper
|       |-------filesystem.${FORMAT}
|       |-------filesystem.manifest
|       |-------filesystem.manifest-desktop
|       |-------vmlinuz |
|-------initrd.img
|
|-------+boot
|       |--------+grub
|       |
|       |        |--------grub.cfg
|       |
|-------memtest86+
|
|--------md5sum.txt
```

[125] Aufs2 - http://www.filesystems.org/project-unionfs.html
[126] Squashfs - http://squashfs.sourceforge.net/
[127] Initramfs - http://www.*Linux*devices.com/articles/AT4017834659.html

- /casper/filesystem.${FORMAT}: Este é o contentor do *filesystem* do *Linux* que foi copiado da versão configurada;
- /casper/filesystem.manifest: Permitiu a instalação do protótipo num *DVD* pois procede ao controlo dos conteúdos presentes no *DVD*. Numa possível situação de instalação, procederia à contagem do conteúdo instalado versus o que está presente no *DVD*;
- /casper/filesystem.manifest-desktop: Igual à explicação anterior, mas relativo ao conteúdo do ambiente de trabalho;
- /casper/vmlinuz: Procedeu à cópia do *kernel* do *Linux;*
- /casper/initrd.img: Contém as customizações necessárias para fazer o *LiveDVD*;
- /boot/grub/grub.cfg: Ficheiro que contém as opções de iniciação (menu);
- /boot/memtest86: Funcionalidade de teste de memória;
- /md5sum.txt: Ficheiro que contém o inventário do conteúdo do *LiveDVD*.

Preparação do ambiente e criação de variáveis:

```
export WORK=~/work
export CD=~/cd
export FORMAT=squashfs
export FS_DIR=casper
Criação do diretório temporário e estrutura de diretorias:
sudo mkdir -p ${CD}/{${FS_DIR},boot/grub} ${WORK}/rootfs
```

Instalação de pacotes necessários no sistema base:

```
sudo apt-get update
sudo apt-get install grub2 xorriso squashfs-tools quem
```

Copiar a instalação para o novo *filesystem*, *rsync* e não *copy*:

```
sudo rsync -av --one-file-system --exclude=/proc/* --exclude=/dev/* \
--exclude=/sys/* --exclude=/tmp/* --exclude=/home/* --exclude=/lost+found \
--exclude=/var/tmp/* --exclude=/boot/grub/* --exclude=/root/* \
--exclude=/var/mail/* --exclude=/var/spool/* --exclude=/media/* \
--exclude=/etc/fstab --exclude=/etc/mtab --exclude=/etc/hosts \
--exclude=/etc/timezone --exclude=/etc/shadow* --exclude=/etc/gshadow* \
--exclude=/etc/X11/xorg.conf* --exclude=/etc/gdm/custom.conf \
--exclude=/etc/lightdm/lightdm.conf        --exclude=${WORK}/rootfs        /
${WORK}/rootfs
sudo cp -av /boot/* ${WORK}/rootfs/boot
```

Copiar o conteúdo da diretoria */home* e ficheiros de configuração:

```
CONFIG='.config .bashrc'|cd ~ && for i in $CONFIG
do
sudo cp -rpv --parents $i ${WORK}/rootfs/etc/skel
done
```

***Chroot* ao novo sistema e proceder a modificações necessárias:**

```
sudo mount  --bind /dev/ ${WORK}/rootfs/dev
sudo mount -t proc proc ${WORK}/rootfs/proc
sudo mount -t sysfs sysfs ${WORK}/rootfs/sys
sudo mount -o bind /run ${WORK}/rootfs/run
sudo chroot ${WORK}/rootfs /bin/bash
```

Instalação de pacotes de idiomas necessários para o *LiveDVD*:

```
LANG=
apt-get update
apt-get install casper lupin-casper
```

Instalador necessário para a versão a entregar ao júri:

```
apt-get install ubiquity ubiquity-frontend-gtk
Note: People using kde replace the previous command with: (chroot)
apt-get install ubiquity ubiquity-frontend-kde
```

Pacotes necessários para situações de emergência:

```
sudo apt-get install gparted ms-sys testdisk wipe partimage xfsprogs
reiserfsprogs jfsutils ntfs-3g ntfsprogs dosfstools mtools
```

Atualizar o *initramfs*:

```
depmod -a $(uname -r)
update-initramfs -u -k $(uname -r)
```

Remover os utilizadores adicionais:

```
for i in `cat /etc/passwd | awk -F":" '{print $1}'`
do
        uid=`cat /etc/passwd | grep "^${i}:" | awk -F":" '{print $3}'`
        [ "$uid" -gt "998" -a   "$uid" -ne "65534"   ] && userdel --force
${i} 2> /dev/null
done
```

Limpar a *cache apt-get*, ficheiros *log*:

```
apt-get clean
find /var/log -regex '.*?[0-9].*?' -exec rm -v {} \;
find /var/log -type f | while read file
do
        cat /dev/null | tee $file
done
rm /etc/resolv.conf /etc/hostname
exit
```

Preparar a árvore de diretoria do *LiveDVD*:

```
export kversion=`cd ${WORK}/rootfs/boot && ls -1 vmlinuz-* | tail -1 | sed
's@vmlinuz-@@'`
sudo cp -vp ${WORK}/rootfs/boot/vmlinuz-${kversion} ${CD}/${FS_DIR}/vmlinuz
sudo        cp        -vp        ${WORK}/rootfs/boot/initrd.img-${kversion}
${CD}/${FS_DIR}/initrd.img
sudo cp -vp ${WORK}/rootfs/boot/memtest86+.bin ${CD}/boot
```

Gerar o ficheiro de manifesto:

```
sudo   chroot   ${WORK}/rootfs   dpkg-query   -W   --showformat='${Package}
${Version}\n' | sudo tee ${CD}/${FS_DIR}/filesystem.manifest
sudo cp -v ${CD}/${FS_DIR}/filesystem.manifest{,-desktop}
sudo cp -v ${CD}/${FS_DIR}/filesystem.manifest{,-desktop}
sudo cp -v ${CD}/${FS_DIR}/filesystem.manifest{,-desktop}
```

Desmontar diretorias:

```
sudo umount ${WORK}/rootfs/proc
sudo umount ${WORK}/rootfs/sys
sudo umount ${WORK}/rootfs/dev
```

Converter a diretoria de ficheiros em *squashfs*:

```
sudo   mksquashfs   ${WORK}/rootfs   ${CD}/${FS_DIR}/filesystem.${FORMAT}   -
noappend
```

Criar o filesystem:

```
echo -n $(sudo du -s --block-size=1 ${WORK}/rootfs | tail -1 | awk '{print
$1}') | sudo tee ${CD}/${FS_DIR}/filesystem.size
```

Calcular o MD5:

```
find ${CD} -type f -print0 | xargs -0 md5sum | sed "s@${CD}@.@" | grep -v
md5sum.txt | sudo tee -a ${CD}/md5sum.txt
```

Criar o menu inicial (*grub*):

```
sudo gedit ${CD}/boot/grub/grub.cfg
set default="0"
set timeout=10
Live "Iniciar em LiveDVD – Isep - Web Anónima e Segura" {
Linux /casper/vmlinuz boot=casper quiet splash
initrd /casper/initrd.img
}
Modo Seguranca " Isep - Web Anónima e Segura " {
Linux /casper/vmlinuz boot=casper xforcevesa quiet splash
initrd /casper/initrd.img
}
Instalacao "iniciar modo de instalação – Não disponivel" {
Linux /casper/vmlinuz boot=casper textonly quiet splash
initrd /casper/initrd.img
}
memtest "Teste de memoria" {
Linux /casper/vmlinuz boot=casper persistent quiet splash
initrd /casper/initrd.img
}
hd "Iniciar Sistema Operativo instalado no HD" {
set root=(hd0)
chainloader +1
}
```

Criar o ficheiro *.ISO*

```
sudo grub-mkrescue -o ~/live-cd.iso ${CD}
sudo grub-mkrescue -o ~/live-cd.iso ${CD}
[ -d "$WORK" ] && rm -r $WORK $CD
```

Para concluir o processo anterior, foi suficiente usar a aplicação de criação de *DVD* para gravar o ficheiro *.ISO.*

3.7.2 Resultado final do protótipo

O protótipo desenvolvido é ferramenta estável, similar graficamente a muitos outros sistemas operativos, mas com a sua identidade própria.

Por ser um *LiveDVD* contém um menu personalizado que identifica claramente a sua origem e contém as opções a apresentar ao utilizador. O seu aspeto foi personalizado para conter a clara identificação do ISEP e o nome do projeto.

Na lista seguinte e imagem posterior é possível observar o menu inicial ou menu de *boot* para que se proceda a uma das cinco opções:

- ***Live*** – Iniciar o *LiveDVD* ISEP *Web* anónima e segura;
- **Modo de segurança** – Iniciar o *LiveDVD* ISEP *Web* anónima e segura;
- **Modo de Instalação** – Não disponível;
- ***Memtest*** – Teste de memória;
- ***HD*** – Iniciar a partir do disco rígido do computador.

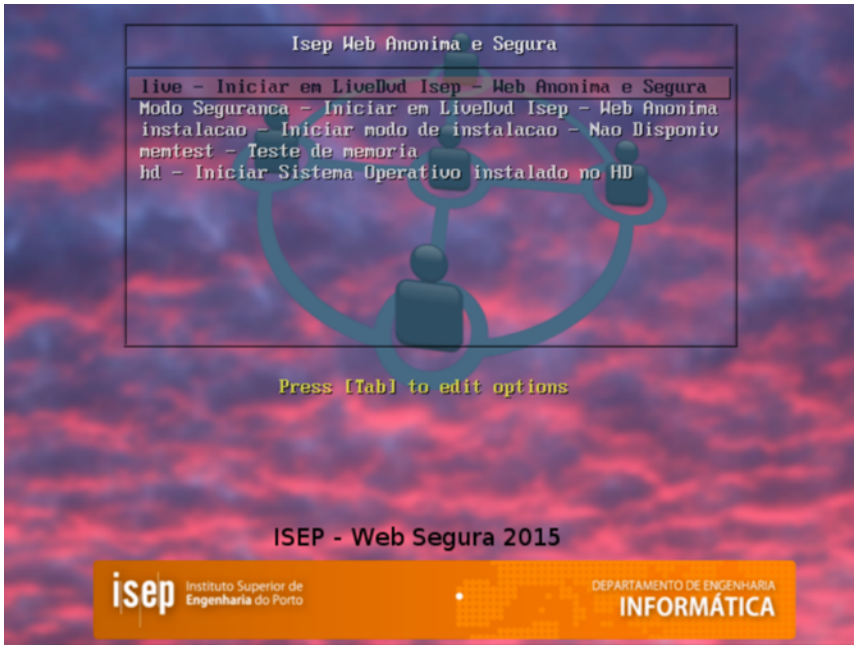

Figura 60 - Imagem do menu inicial ou boot menu[128]

A aparência gráfica do *Gnome Classic* permite que o *LiveDVD* apresente ao utilizador uma experiência agradável e comum aos sistemas *Ubuntu*, que consistem em quatro pontos:

- Ambiente de trabalho com ícones de atalho;
- Menu no canto superior esquerdo com as opções Aplicações e Locais;
- Informação de contexto e informações de sistema no canto superior direito;
- Atalho para o ambiente de trabalho no canto inferior esquerdo.

O ambiente de trabalho consiste na disponibilização dos pontos anteriores e os ícones de atalho para o uso da *Web*, acesso ao computador e pasta do utilizador (*home*).

[128] Imagem elaborada pelo autor

Na imagem seguinte pode-se observar isso mesmo:

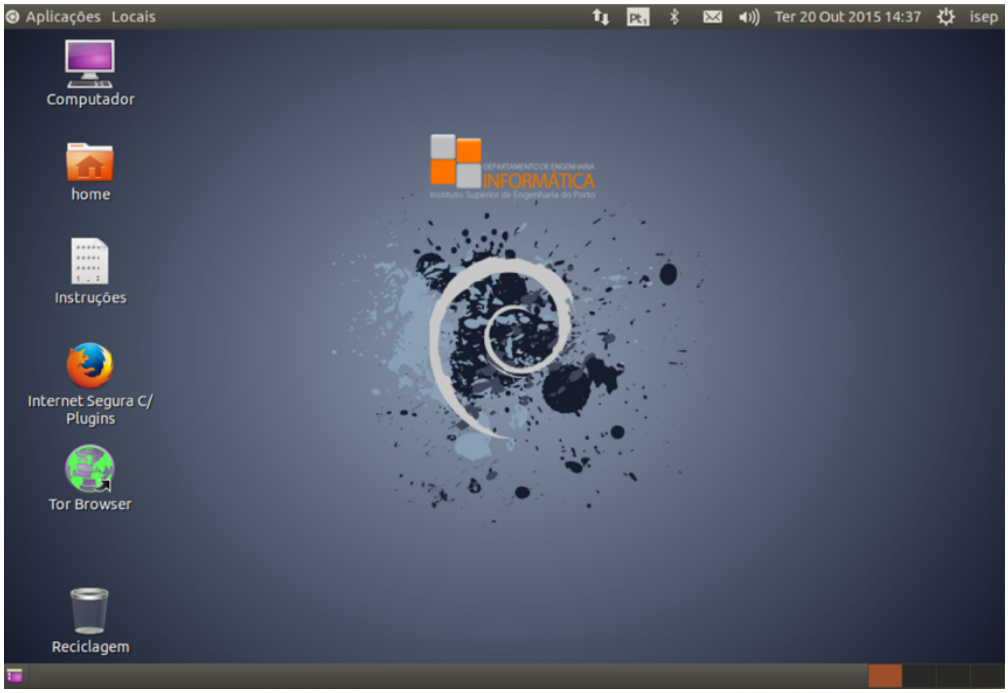

Figura 61 - Ambiente de trabalho do protótipo[129]

No canto superior esquerdo estão localizados os atalhos para as aplicações que estão disponíveis bem como as ferramentas de gestão do sistema operativo. Existe ainda o menu Locais, onde é possível encontrar os repositórios tradicionais de imagens, músicas e a pasta de transferências. Todo o propósito é que o ambiente de trabalho seja o mais aproximado do normal, no sentido de providenciar conforto e segurança no uso do *LiveDVD*.

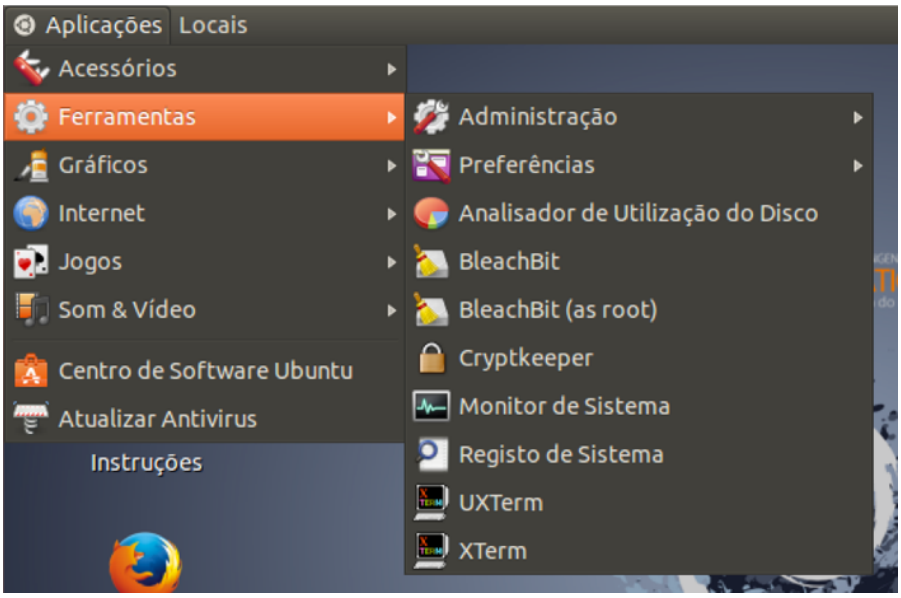

Figura 62 - Menu de Aplicações e Locais[130]

[129] Imagem elaborada pelo autor

No canto superior direito encontra-se a informação de contexto do sistema, como a rede, horas e data, informação sobre o volume do som e o apoio à introdução de texto consistente em dois teclados predefinidos, Windows, *Linux* e Mac OSX. Para desligar o protótipo basta clicar em cima da conta a uso (isep) e o menu de opções abrirá.

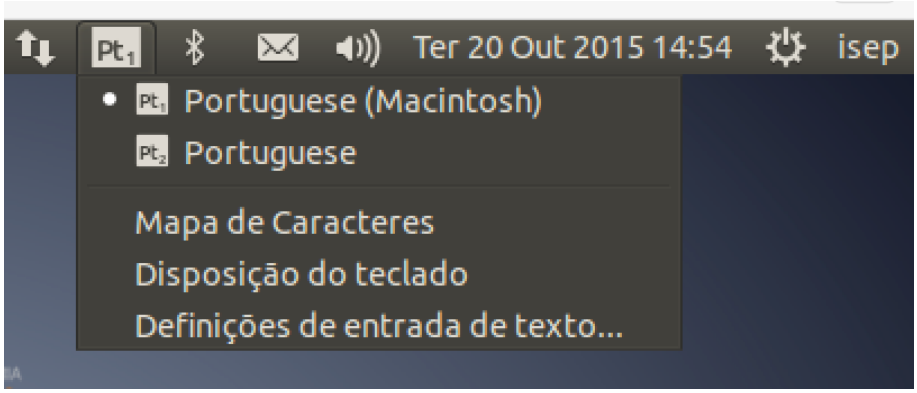

Figura 63 - Menu de contexto e informação de sistema[131]

Em conclusão, no seguinte conjunto de imagens pode-se verificar o âmbito do protótipo alcançado. A figura 64 apresenta a localização da máquina *host,* onde está instalada a máquina virtual onde está montado o protótipo. Como é possível observar a sua localização é o datacenter da PT Comunicações na cidade de Lisboa, com o *IP* 37.189.165.195.

[130] Imagem elaborada pelo autor
[131] Imagem elaborada pelo autor

3.7.2.1 Localização a máquina host (anfitrião)

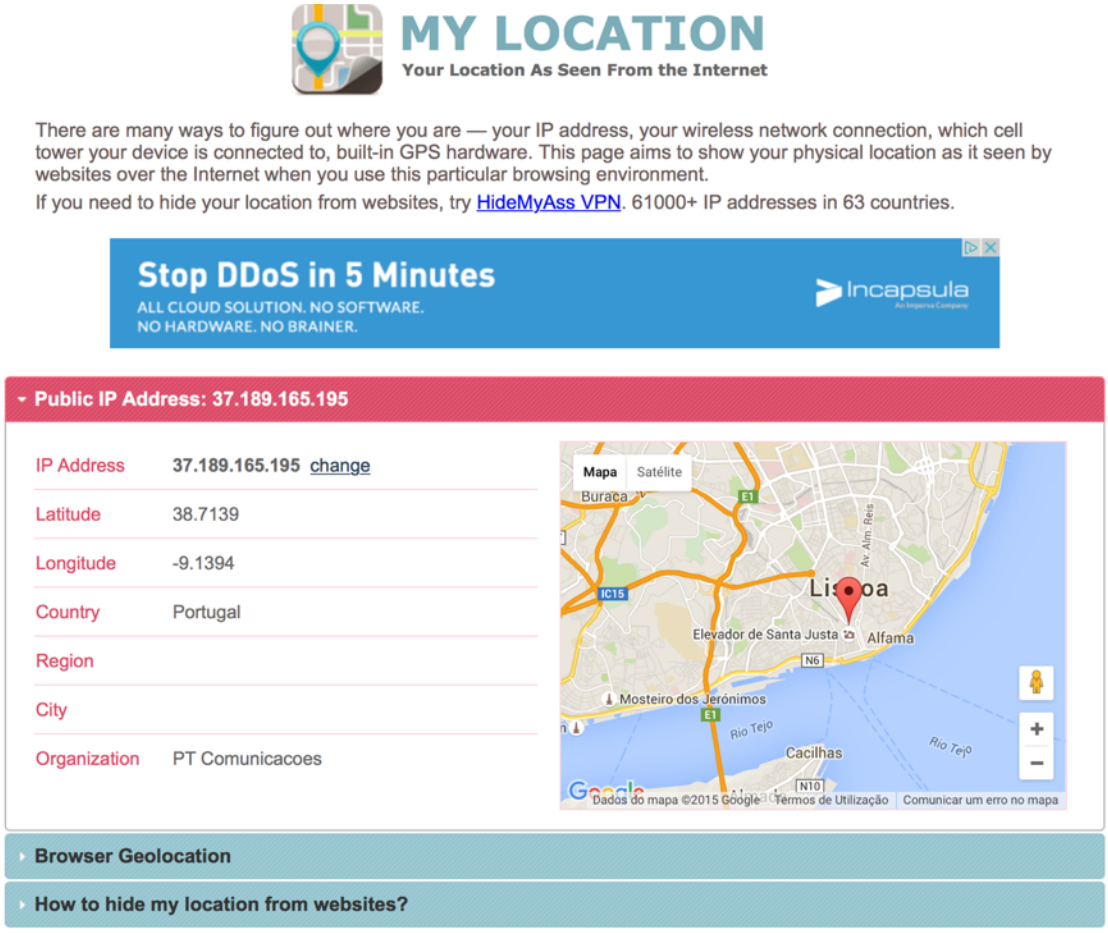

Figura 64 - Localização na Web do host do protótipo[132]

Na figura 65, pode-se observar o *browser Firefox* aberto dentro do protótipo onde é possível verificar que o *IP* atribuído ao mesmo é o 5.199.142.195, localizado perto da cidade de Marburo na Alemanha.

[132] Imagem elaborada pelo autor

3.7.2.2 Localização do Firefox no protótipo

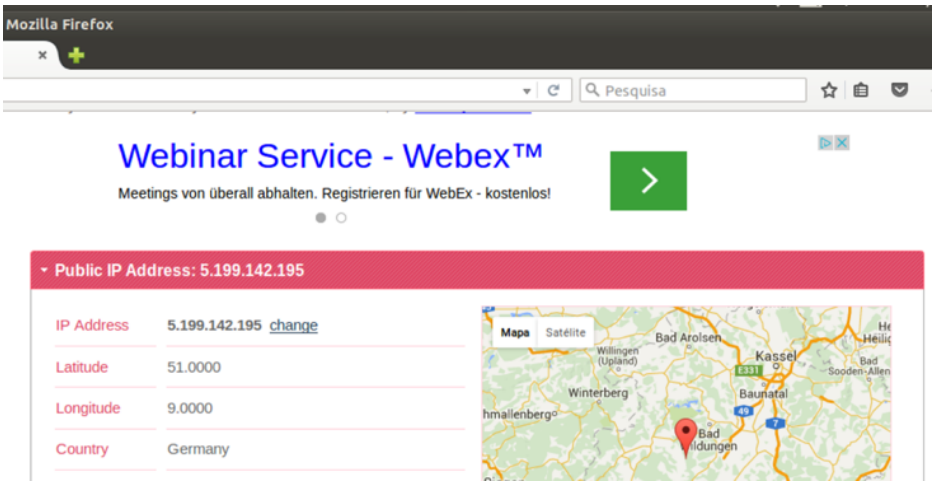

Figura 65 - Localização do protótipo com recurso ao Firefox[133]

3.7.2.3 Localização do protótipo com o Tor Browser

Por fim, a seguinte figura apresenta a localização com recurso ao *Tor Browser*. Relembra-se que no protótipo desenvolvido, o *Tor Browser* é o mecanismo redundante que assenta no *proxy socks5* configurado para encaminhar todo o tráfego *Web*. Esta configuração permite utilizar o automatismo que altera a localização do protótipo a cada cinco minutos e em cima deste, criar uma nova *VPN* de comunicação que também altera a sua localização e as rotas de comunicação a cada cinco minutos. Este facto, permite que a localização ou leitura do conteúdo dos dados do utilizador seja uma tarefa difícil, mesmo que seja possível perceber que se está a usar a rede *Tor* com recurso a sinalizadores de tráfego.

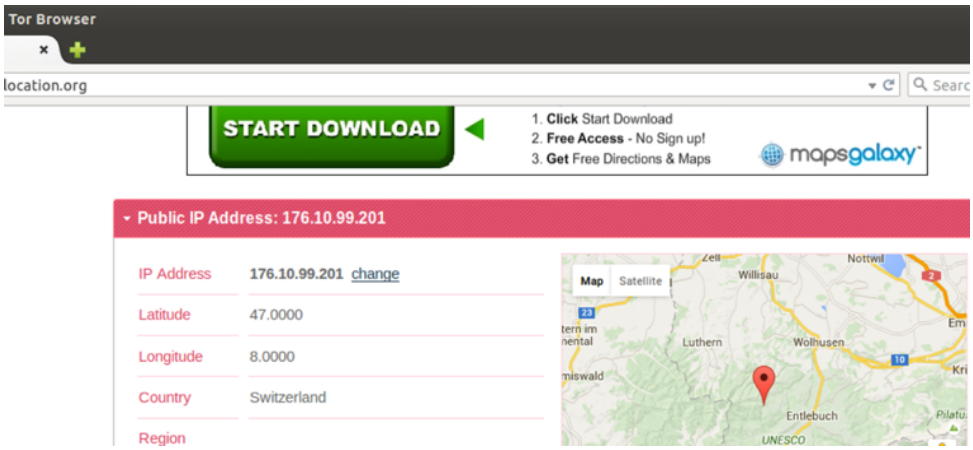

Figura 66 - Localização do protótipo com recurso ao Tor Browser[134]

[133] Imagem elaborada pelo autor
[134] Imagem elaborada pelo autor

4 Análise dos resultados

Um sistema operativo que seja diferente do *Windows* é comummente considerado mais complexo pois a resistência à mudança é intrínseca no desenvolvimento de sistemas de informação. Um trabalho desta índole deve aferir o seu potencial, o nível de exigência aos utilizadores e o grau de dificuldade de uso. Para uma pessoa com bases de tecnologia na sua formação, é mais natural e tem menos impacto o uso do protótipo que recorre a máquinas virtuais e à necessidade de configurar a *bios.* Por outro lado, se uma pessoa sente necessidade de segurança e então a necessidade de um sistema que mantenha o anonimato, já deverá estar mais entrosada com os mecanismos comuns e comerciais de uso de tecnologia, como por exemplo o conceito de máquinas virtuais. É certo que nos últimos anos houve um acrescento do uso das tecnologias de informação, com suporte nos dispositivos móveis, nomeadamente os *smartphones,* originando a inclusão tecnológica das gerações mais velhas.

Neste capítulo pretendem-se apresentar os resultados do inquérito *online,* realizado para a avaliação do protótipo desenvolvido. É caracterizado o público-alvo na sua idade e o género, área de formação, conhecimentos relativos à configuração necessária do anfitrião para receber diretamente o *LiveDVD* na unidade de *DVD* ou por máquina virtual, bem como se verificou se a sua localização é a real ou a mascarada e também se sentiu segurança no uso da ferramenta.

O processo de inquérito foi efetuado pela *Web* e foi respondido por 60 pessoas, divididas entre o Instituto Superior de Engenharia do Porto e o ISLA – Instituto Politécnico de Gestão e Tecnologia, onde concluem os seus estudos de mestrado nas mais diversas áreas. A recolha de dados foi depois processada no *Excel* para a construção dos gráficos de suporte.

4.1 Problemáticas estudadas

Responderam ao inquérito colocado *online* 60 pessoas, tendo sido efetuadas duas demonstrações práticas a três grupos de 20 pessoas. O protótipo foi instalado nos computadores dos participantes e submetido a teste de usabilidade e de eficácia no que concerne ao mascaramento da localização. Os gráficos seguintes são fruto do tratamento da informação numa folha de cálculo após a exportação do *Google Drive* do inquérito criado no *Google Forms*[135] *e* trabalhados numa *pivot table.*

[135] Google Forms, plataforma de formulários do Google – https://docs.google.com/forms

O resultado desta análise pode ser observado *online:*

https://docs.google.com/forms/d/1ooH2Ia4JJ4sD40Xd9zKFEjx_I2qV1a99sV9YGVNnRLc/viewanalytics#start=publishanalytics

No gráfico seguinte pode-se verificar a distribuição das idades dos participantes. 76% dos inquiridos compreendem uma idade entre os 18 e os 28 anos, 17% dos inquiridos estão entre os 29 e os 39 anos, 5% entre os 40 e os 50 anos e 2% acima dos 51 anos.

Este exercício permitiu verificar que a grande maioria dos inquiridos é jovem ou jovem adulto.

4.1.1.1 Idade da População-Alvo

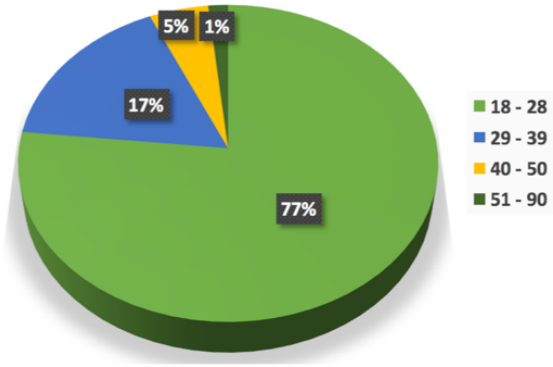

Figura 67 - Distribuição da população quanto à idade[136]

4.1.1.2 Género da População-Alvo

Este gráfico permite verificar que 78% dos inquiridos são do sexo masculino e os restantes 22% do feminino, concluindo que a população feminina está em clara minoria na amostra.

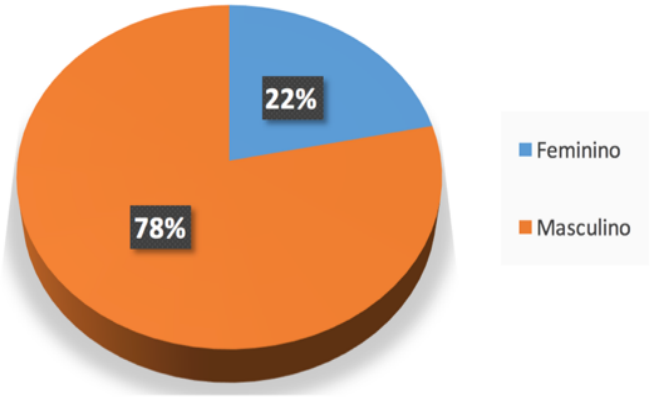

Figura 68 - Distribuição da população-alvo quanto ao género[137]

[136] Imagem elaborada pelo autor
[137] Imagem elaborada pelo autor

4.1.1.3 Área de Formação

Relativamente à área de formação dos inquiridos, esta recolha de dados permitiu perceber que a grande maioria, 83% (50 pessoas), possuem formação em informática, seguido de 7% (4 pessoas) em ciências sociais e outros 7% (4 pessoas) em ciências jurídicas. Na área da saúde e declarados como sem formação específica estão 2 pessoas, num total de 3%.

A imagem seguinte permite perceber que a maioria dos inquiridos está familiarizada com as tecnologias empregues no protótipo.

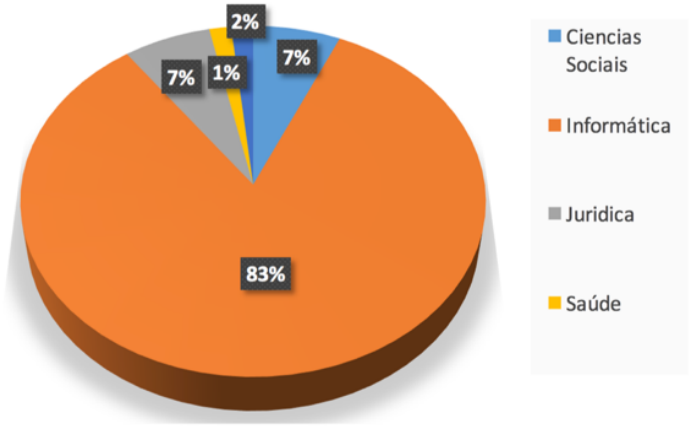

Figura 69 - Distribuição da População-Alvo relativamente à formação[138]

Ainda dentro da área da formação, no gráfico seguinte pode-se observar a distribuição de géneros de acordo com a área de formação, sendo claro que a maioria é do sexo masculino e têm como formação a área da informática.

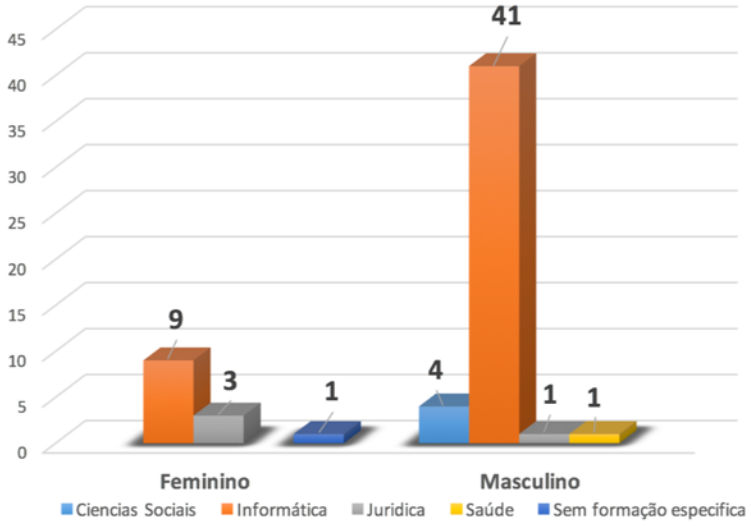

Figura 70 - Distribuição de área de formação considerando o género[139]

[138] Imagem elaborada pelo autor

4.1.1.4 Sabe iniciar o seu computador através da unidade de CD/DVD?

Relativamente aos conhecimentos dos inquiridos quanto ao facto de saberem iniciar o seu computador a partir da unidade de *CD/DVD*, com base na amostra, conclui-se que sabem, pois o resultado foi de 73% afirmativo, 15% negativo e 12% afirma não possuir unidade de *CD/DVD*.

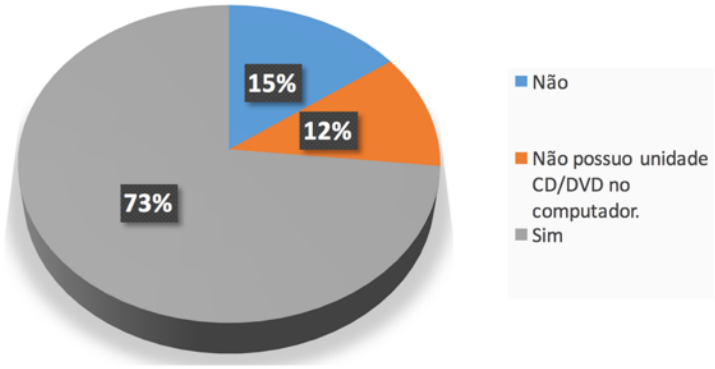

Figura 71 - Distribuição relativa ao conhecimento de iniciar o *PC* pela unidade de *CD/DVD*

Ainda relativamente à questão de conhecimentos sobre a configuração de iniciação a partir da unidade de *CD/DVD*, é possível analisar na imagem seguinte a distribuição de respostas de acordo com a formação dos participantes. Verificam-se 43 respostas positivas no eixo de formação em informática e que apenas 3 participantes não possuem conhecimento para iniciar o seu computador a partir da unidade de *CD/DVD*. Verifica-se também que nas áreas de formação em saúde e jurídica não houve respostas positivas à questão, assinalando a falta de conhecimentos técnicos por parte destes participantes.

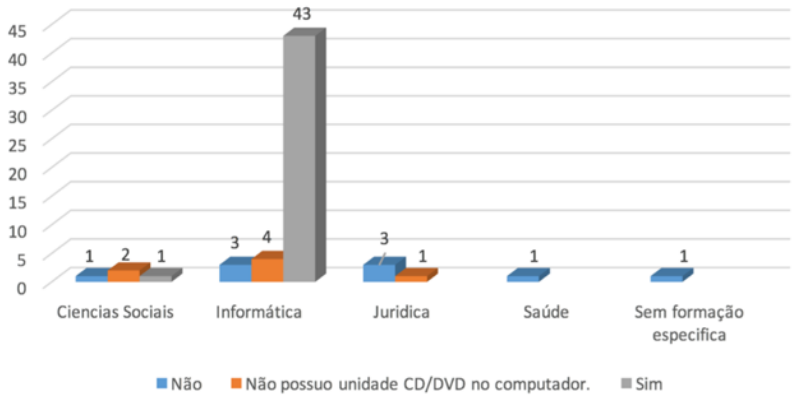

Figura 72 - Distribuição de conhecimentos técnicos com base na área de formação[140]

[139] Imagem elaborada pelo autor
[140] Imagem elaborada pelo autor

4.1.1.5 Já alguma vez usou uma máquina virtual?

Relativamente à questão colocada sobre se os participantes já teriam utilizado uma máquina virtual, 92% dos inquiridos afirmam já ter usado anteriormente uma máquina virtual, enquanto apenas 8% afirmam não o ter feito. Isto leva à conclusão que o possível uso maioritário do protótipo seja feito com recurso a um programa de virtualização de *hardware* e *software*.

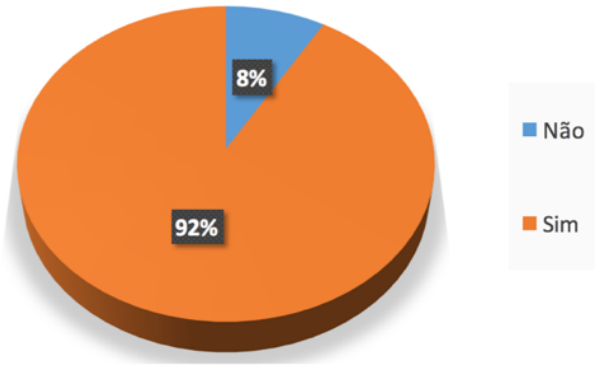

Figura 73 - Distribuição quanto ao uso de máquinas virtuais[141]

Ainda relativamente à questão anterior do uso de máquinas virtuais, no gráfico seguinte pode-se observar a distribuição das respostas quanto à área de formação.

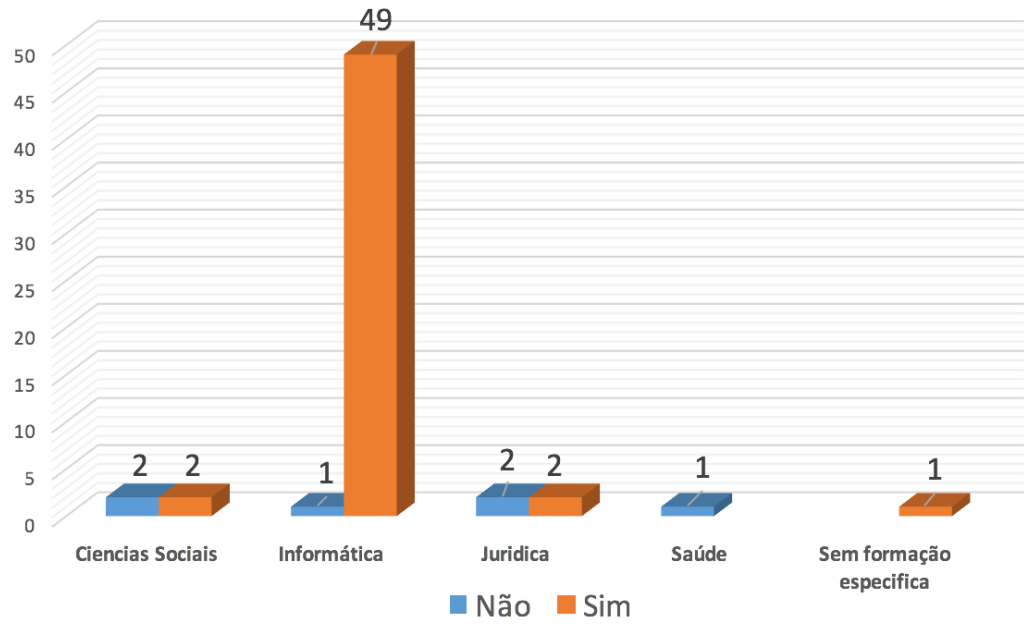

Figura 74 - distribuição de respostas sobre a utilização do *Linux*, quanto à área de formação[142]

[141] Imagem elaborada pelo autor

4.1.1.6 Já usou antes um sistema Linux?

Quanto ao uso de um sistema operativo *Linux*, 85% dos participantes já usaram um sistema deste género anteriormente, tendo respondido negativamente apenas 15% dos inquiridos.

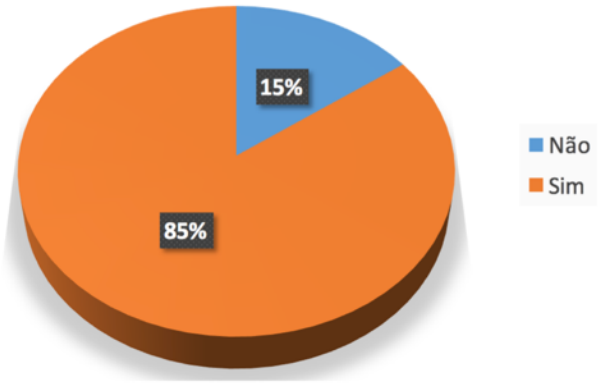

Figura 75 - Distribuição quanto ao uso anteriormente de um SO *Linux*[143]

Ainda relativamente à questão em análise, no gráfico seguinte observa-se a distribuição em função da área de formação dos participantes.

No grupo de respostas não foi possível identificar resultado positivo dos participantes com formação na área da saúde e nos participantes que declaram não ter formação específica.

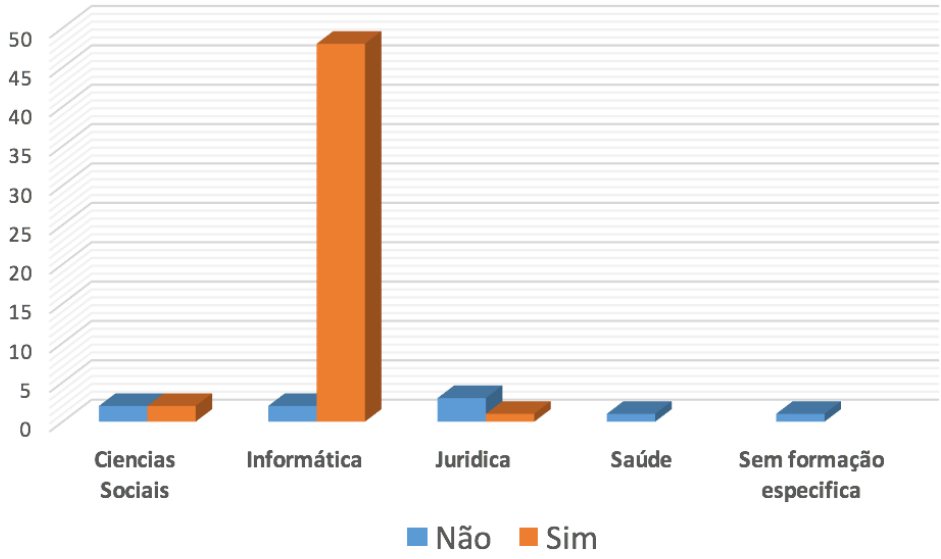

Figura 76 - Distribuição de respostas quanto à área de formação[144]

[142] Imagem elaborada pelo autor
[143] Imagem elaborada pelo autor
[144] Imagem elaborada pelo autor

4.1.1.7 Usou o LiveDVD (protótipo) com recurso a máquina virtual?

No seguinte ponto conclui-se que 83% dos inquiridos (50 participantes) usou o protótipo numa máquina virtual, 4% (2 participantes) informa que não o fizeram e 13% da amostra (8 participantes) usaram diretamente a unidade de *CD/DVD*.

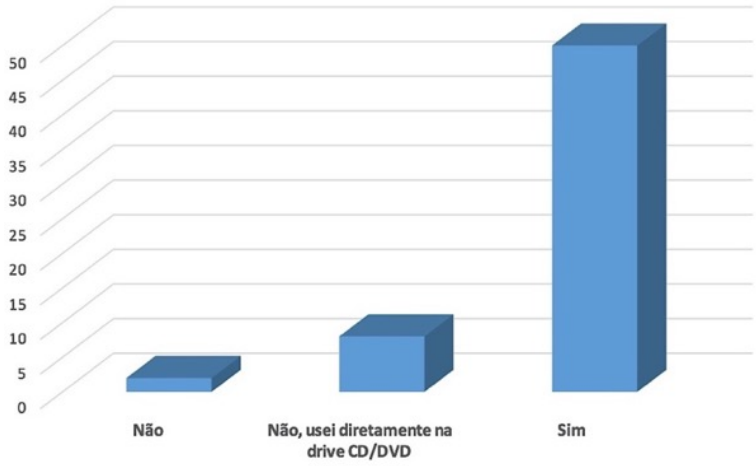

Figura 77 - Distribuição quanto à forma de uso do protótipo[145]

Consegue-se perceber que a maioria dos inquiridos usou efetivamente a máquina virtual para testar o protótipo, o que leva a concluir que é necessário que o protótipo esteja disponível *online* para que possa ser transferido para a máquina dos potenciais utilizadores.

4.1.1.8 Ao usar o Browser Tor e ao pesquisar no Google a sua localização que resultado obteve?

Relativamente ao resultado da pesquisa no uso do protótipo em teste à sua eficácia de segurança, todos os inquiridos afirmaram obter uma localização virtual diferente da sua real, noutro país, atestando a efetividade funcional do protótipo quanto ao seu âmbito.

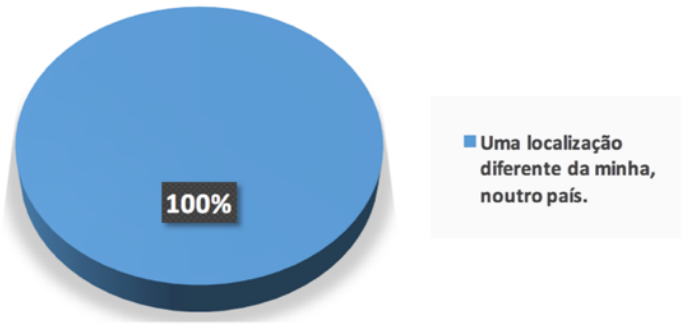

Figura 78 - Aferição dos resultados do uso da Rede *Tor*

[145] Imagem elaborada pelo autor

4.1.1.9 Ao usar o browser Firefox e ao pesquisar no Google a sua localização que resultado obteve?

Relativamente ao resultado obtido no uso do protótipo em teste à sua eficácia e segurança, 98% dos inquiridos afirma terem verificado uma localização diferente à sua, noutro país.

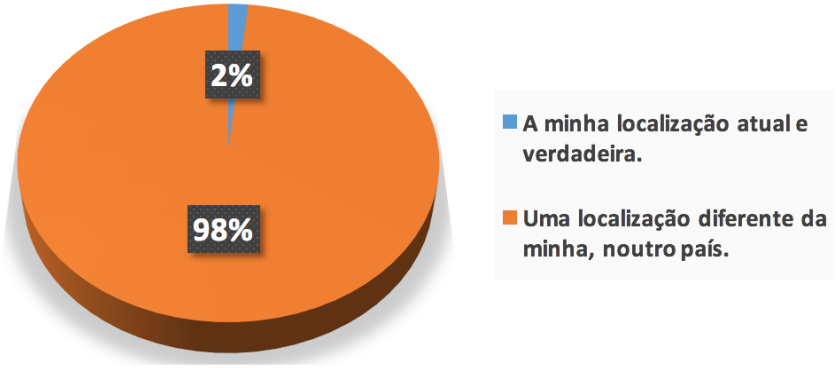

Figura 79 - Aferição do resultado do uso do *Firefox*[146]

4.1.1.10 Contagem de caso a resposta à pergunta anterior seja "Uma localização diferente da minha, noutro país" sentiu-se seguro com o nível de segurança do LiveDVD?

Relativamente a esta questão, após a utilização e verificação da efetividade relativamente ao compromisso de manter a localização do utilizador confidencial e relação à sua real localização, 93% dos participantes deste inquérito afirmaram sentirem-se seguros com o nível de segurança do protótipo, chegando-se à conclusão que este cria uma sensação de segurança.

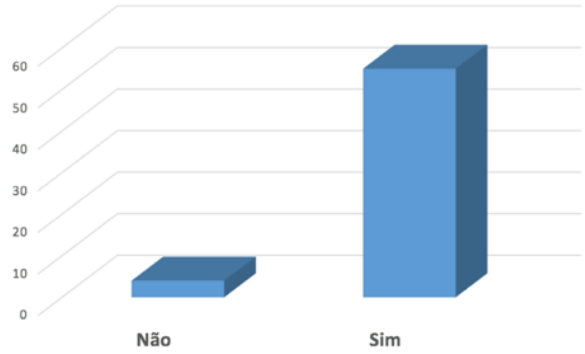

Figura 80 - Aferição relativa à segurança do protótipo[147]

[146] Imagem elaborada pelo autor
[147] Imagem elaborada pelo autor

4.1.1.11 O aspeto geral do sistema operativo é apelativo?

Por último, como se pode ver na figura seguinte, 95% dos participantes considera o sistema operativo proposto em que consiste o protótipo agradável e fácil de usar.

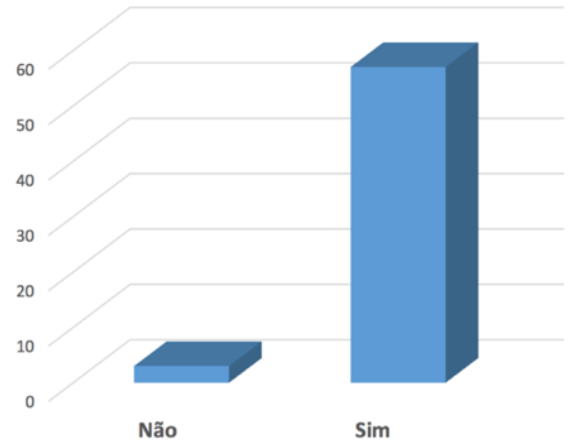

Figura 81 - Distribuição quanto à agradabilidade do sistema[148]

[148] Imagem elaborada pelo autor

5 Conclusões e trabalho futuro

Este trabalho tinha como objetivo inicial criar um protótipo que fosse capaz de de ultrapassar a problemática da insegurança *online* pela captura de informação privada e dos bloqueios de acesso por mecanismos de censura.

No estado da arte foram identificadas as mais correntes soluções no mercado e utilizadas por um número incalculável de pessoas. Umas são completamente *open source* e outras, que para garantir uma melhor segurança, solicitam ao utilizador para sobrescrever uma conta *premium* com um valor a pagar pelos serviços.

No desenvolvimento do protótipo existiu sempre uma preocupação em criar uma solução única entre as que se podem observar no estado da arte e até numa pequena pesquisa pela *Web,* e que não estivesse votada ao fracasso e à não evolução. Este é, sem dúvida, um projeto que tem potencial de sucesso. O elemento diferenciador entre os semelhantes é o facto de não ser possível instalar no disco rígido (exceto a versão de análise entregue ao painel de júri), não estar disponível num suporte físico de memória (*pen USB*) exposto a ataques e infeções, e por último, um sistema redundante de anonimato.

Ao iniciar o *Tor Browser*, este corre já dentro do *proxy* interno, que encaminha todo o tráfego pela rede *Tor*, criando assim dois circuitos opostos que renovam a cada cinco minutos, tornando virtualmente impossível seguir o utilizador. Associar este panorama à factualidade de não retenção das informações nem registos de uso torna este protótipo eficiente na sua tarefa.

Este tema colocou desafios complexos e que requereram muito estudo para a compreensão e concatenação de toda a informação num resultado útil. Conhecer as ameaças na *Web*, como estas operam como indivíduos ou organizações e a forma de as ultrapassar, foi fundamental para a reunião das aplicações úteis a disponibilizar ao utilizador e alcançar o âmbito proposto.

5.1 Principais conclusões do presente trabalho

Este trabalho permitiu verificar a evolução do uso da *Web* e perceber o grau de gravidade das ameaças, com a análise detalhada dos mecanismos de encriptação e as tecnologias em prática nos dias correntes. Ao analisar os principais meios de ataque e o *modus operandis* dos piratas informáticos, contribuiu também para perceber o melhor tipo de protótipo a desenvolver.

Através da recolha de informação por questionário, percebeu-se que a maioria das pessoas tem conhecimentos informáticos para ter uma postura proactiva na tarefa de manter segura os seus sistemas de informação. Conclui-se que a maioria das pessoas formadas em tecnologia são do sexo masculino e, portanto, deverá a sociedade promover medidas de inclusão de pessoas do sexo feminino nos estudos de tecnologias, assim potenciando a passagem de conhecimento entre géneros e levando a um maior esclarecimento do uso da tecnologia de forma eficiente e segura.

Concluiu-se que a grande parte dos inquiridos estudantes de mestrado são na sua maioria jovens e do sexo masculino. Percebeu-se que também há um grande número de jovens e jovens adultos que está confortável com o uso das tecnologias, também independentemente da área de formação. No seguinte gráfico, pode-se observar que o uso de sistemas operativos *Linux* e o uso de máquinas virtuais está equilibradamente distribuído por área de formação e idade.

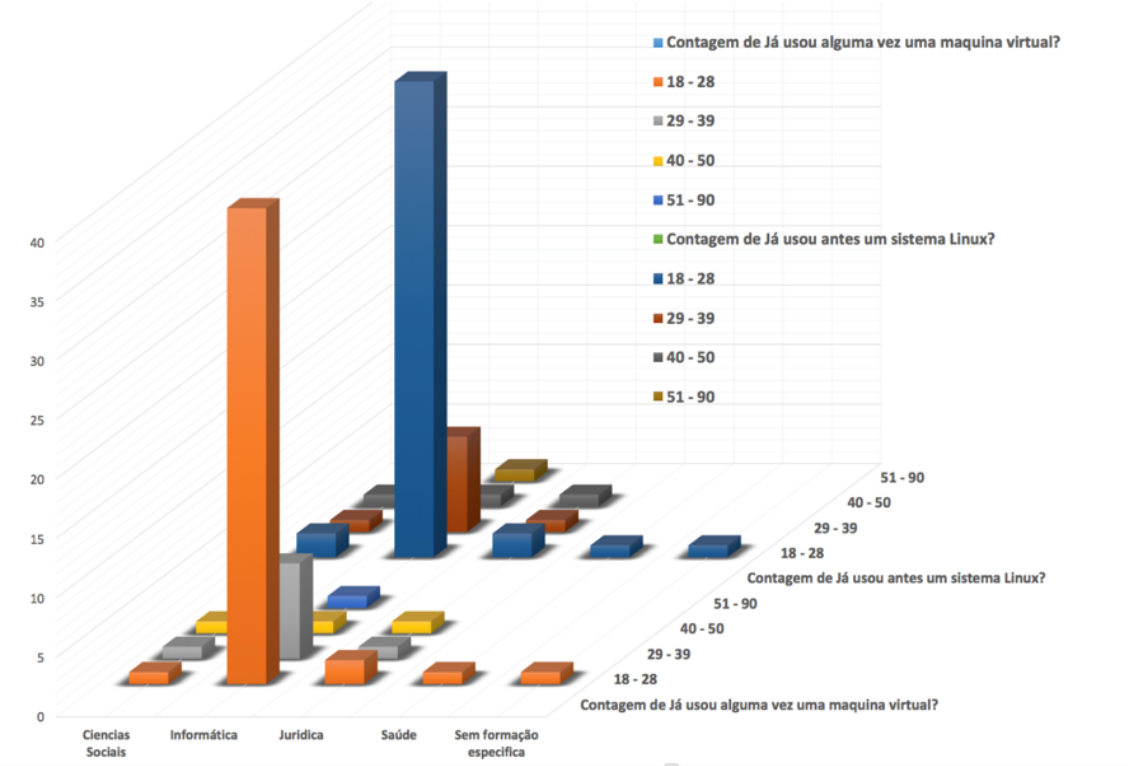

Figura 82 - Gráfico de aferição de competências tecnológicas[149]

Conclui-se que a maioria dos inquiridos neste trabalho não terá grandes dificuldades no uso deste protótipo por já estar familiarizado com as tecnologias nele disponível.

[149] Imagem elaborada pelo autor

Por último, conclui-se que o protótipo consegue efetivamente esconder a verdadeira localização do utilizador, que com recurso a mecanismos internos, ocultos e automáticos consegue ultrapassar as barreiras de censura à informação e que o seu provável uso será a utilização com recurso a uma máquina virtual e que é aprazível aos utilizadores.

5.2 Trabalho futuro

Este trabalho foi imensamente proveitoso pois permitiu conhecer de forma muito detalhada toda a problemática relacionada com a segurança de sistemas de informação e os desafios que enfrentam os seus utilizadores na *Web*.

No decorrer deste trabalho, foram desenvolvidas duas possibilidades de continuidade deste projeto. Uma versão de *Linux From Scratch* e uma versão de *Ubuntu Server* que necessitam de ser concluídas e disponibilizadas a terceiros para teste. Uma possibilidade é também a continuidade deste projeto por uma das vias descritas acima, no âmbito de uma dissertação de mestrado do *ISEP*.

No futuro, o autor identifica a intenção de criar um departamento de estudos de segurança informática idêntico ao existente noutras instituições de ensino superior em Portugal, sendo uma delas a entidade que desenvolve a única alternativa de origem portuguesa no mercado atualmente, o *C3PIV* da Universidade do Porto. Tenciona ainda prosseguir em 2015 o doutoramento em engenharia informática na Universidade de Trás-os-Montes e Alto Douro, onde já procedeu à candidatura para este ano lectivo, onde irá dar continuidade a este trabalho.

Referências

[Alan Calder and Steve Watking, 2015] Calder A., Watking S., IT Governance - An International Guide to Data Security and ISO27001/ISO27002, 6th edition, Kogan Page

[Alexander Avakov, 2012] Avakov A., The Surreal Diary of an Unwilling Spy, Xlibris Corporation

[André Zúquete, 2014] Zúquete A., Segurança em Redes Informáticas, 4ª edição, FCA

[Andrew Clement, 2014] Clement A., NSA Surveillance: Exploring the Geographies of Internet Interception, https://www.ideals.illinois.edu/bitstream/handle/2142/47305/119_ready.pdf, [último acesso Out 2015]

[António Filho, 2004] Filho A., Segurança da Informação, http://www.espacoacademico.com.br/042/42amsf.htm, [último acesso Mar 2015]

[Barton Gellman and Laura Poitras, 2013] Gellman B., Poitras L., U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-Internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, [último acesso Fev 2015]

[Barton Gellman and Matt DeLong, S/D] Gellman B., DeLong M., One month, hundreds of millions of records collected, http://apps.washingtonpost.com/g/page/world/one-month-hundreds-of-millions-of-records-collected/554/, [último acesso Out 2015]

[Bill Blunden, 2014] Blunden B., Cheung V., Behold a Pale Farce - Cyberwar, Threat Inflation, & the Malware Industrial Complex, Trine Day

[Brian Shea, 2002] Shea B., Have You Locked the Castle Gate?: Home and Small Business Computer Security, Addison-Wesley Professional

[Bruce Schneider, 2015] Schneider B., Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, W. W. Norton & Company

[Bruno Garracho, 2009] Garracho B., Tese de Mestrado em Segurança Informática, Securing critical utility systems & network infrastructures, http://repositorio.ul.pt/handle/10451/4127, [último acesso Jun 2015]

[Byron Acohido, 2013] Acohido B., Latest PRISM disclosures shouldn't worry consumers, http://www.usatoday.com/story/cybertruth/2013/09/05/latest-prism-disclosures-shouldnt-worry-consumers/2773495/, [último acesso Jan 2015]

[Charlie Savage, 2013] Savage C., US confirms that it gathers *online* data overseas, http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html, [último acesso Mar 2015]

[Christian Gross, S/D] Gross C., Mass surveillance of Nsa/GCQ, http://www.they-know.org/assets/surveillance-system-poster.pdf, [último acesso Out 2015]

[Christopher Adam et al., 2012] Adam C., Thorne M., Fuzz M., Hyde A., Nuñez A., Phillips J., Safadi B., Erkalovic A., Trew B., The Open *Web*, Christopher Adams

[Christopher Kern et al., 2007] Kern C., Kesavan A., DaswaniN., Foundations of Security: What Every Programmer Needs to Know, Apress

[Daniel Barret et al., 2005] Barret D., Silverman R., Byrnes R., SSH, The Secure Shell: The Definitive Guide: The Definitive Guide, O'Reilly Media Inc.

[David Kravets, 2013] Kravets D., NSA LEAK VINDICATES AT&T WHISTLEBLOWER, http://www.wired.com/2013/06/nsa-whistleblower-klein/, [último acesso Mar 2015]

[David Leigh and Luke Harding, 2013] Leigh D., Harding L., WikiLeaks: Inside Julian Assange's War on Secrecy, Faber & Faber

[David S. Whitley, 2009] Whitley D., Cave Paintings and the Human Spirit: The Origin of Creativity and Belief, Prometheus Books

[Edmundo Monteiro and Fernando Boavida, 2011] Monteiro e., Boavida F., Engenharia de Redes Informáticas, 10ª edição, FCA

[Elizabeth Zwicky et al., 2000] Zwicky E., Cooper S., Chapman D., Building Internet Firewalls, O'Reilly Media Inc.

[Elliot Cohen, 2014] Cohen E., Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance, P. Macmillan

[Eric Raymond, 1997]	Raymond E., New Hacker's Dictionary, Library of Congress
[Fabio Locati, 2015]	Locati F., OpenStack Cloud Security, Packt Publishing Ltd
[Fernando Boavida et al., 2013]	Boavida F., Bernardes M., Vapi P., Administração de Redes Informáticas, 2ª edição, FCA
[Fernando Pereira and Rui Guerreiro, 2012]	Pereira F., Guerreiro R., *Linux*, 4ª edição, FCA
[Filipa Sousa, 2014]	Sousa F., Pen do C3P vai garantir navegação anónima, http://informacao.canalsuperior.pt/sala-geek/17116, [último acesso Jul 2015]
[Filomena Lopes et al.,2009]	Lopes F. C., Morais P. M., Carvalho A., Carvalho J., Desenvolvimento de Sistemas de Informação, FCA
[Frederic Lardinois, 2013]	Lardinois, F., Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program, http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/, [último acesso Mai 2015]
[Free *Software* Foundation]	Free *Software* Foundation, Diretrizes para Distribuições de Sistemas Livres, http://www.gnu.org/distros/free-system-distribution-guidelines.pt-br.html, [último acesso Dez 2014]
[Gary Shelly and Jennifer Campbell, 2012]	Shelly G., Campbell J., Discovering the Internet: Complete, Cengage Learning
[Gianluca Mezzofiore, 2013]	Mezzofiore G., NSA Whistleblower Edward Snowden: Washington Snoopers are Criminals, http://www.ibtimes.co.uk/nsa-whistleblower-edward-snowden-479709, [último acesso Jan 2015]
[Greg Walton, 2001]	Walton G., China's Golden Shield Corporations and the Development of Surveillance in The Peoples Republic of China, 1st Edition, Enter
[Hermann Walker, 2009]	Walker H., Improving Internet Access to Help Small Business Compete in a Global Economy, Nova Science Publishers, Incorporated
[Internet Live Stats, 2015]	Internet Live Stats, Dados referentes ao número de utilizadores ligados à Internet em 2015 -

http://www.Internetlivestats.com/Internet-users/, [último acesso Out 2015]

[James Bamford, 2013] Bamford J., They know much more than you think, http://www.nybooks.com/articles/archives/2013/aug/15/nsa-they-know-much-more-you-think/, [último acesso Mar 2015]

[James Bamford, 2013] Bamford J., Connecting the Dots on PRISM, Phone Surveillance, and the NSA's Massive Spy Center, http://www.wired.com/2013/06/nsa-prism-verizon-surveillance/, [último acesso Fev 2015]

[James Derian, 2009] Darian J., Virtuous War: Mapping the Military-Industrial-Media-Entertainment-Network, Routledge

[Javier Lopez et al., 2015] Lopez, J., Ray I., Crispo B., Risks and Security of Internet and Systems: 9th International Conference, CRiSIS 2014, Trento, Italy, August 27-29, 2014, Revised Selected Papers, Springer

[Jonathan Zittrain and Benjamim Edelman, 2003] Zitrtrain J., Edelman B., Empirical Analysis of Internet Filtering in China, Harvard, https://cyber.law.harvard.edu/filtering/china/, [último acesso Ago 2015]

[Jorge Granjal, Edmundo Monteiro, S/D] Granjal J., Monteiro E., Mecanismos de Segurança, http://www1.ci.uc.pt/crc98/comfin23/comfin23.html, [último acesso Jan 2015]

[Julien Assange, 2013] Assange J., The Spy Files, https://twitter.com/wikileaks/status/342812446534283264, [último acesso Mar 2015]

[*Linux* Counter, 2015] *Linux* Counter, Statistics about the *Linux* distributions, https://www.*Linux*counter.net/statistics/distributions, [último acesso Dez 2014]

[Luis Porto, 2011] Porto L., Segurança da Informação, Universidade Federal S. João Del-Rei, http://repositorio.ufla.br/jspui/bitstream/1/5355/1/mono-LuisFernandoPorto_0.pdf, [último acesso Mar 2015]

[Marcelo Carvalho, 2006] Carvalho M., Estruturado (DHT) baseado fora do algoritmo Kademlia. Trajetória da internet no brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança,

Universidade Federal do Rio de Janeiro, http://www.cos.ufrj.br/uploadfile/1430748034.pdf, [último acesso Dez 2015]

[Mario Barcena and Candid Wueest, 2014] Barcena M., Wueest C., Insecurity of the Internet of Things, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/insecurity-in-the-internet-of-things.pdf [último acesso Ago 2014]

[Markus Jakobsson, 2012] Jakobsson M., The Death of the Internet, John Wiley & Sons

[Martin Brinkmann, 2014] Brinkmann M., Mozilla improves Security for Bugzilla after security breach, http://www.ghacks.net/2015/09/04/mozilla-improves-security-for-bugzilla-after-security-breach/, [último acesso Set 2015]

[Mark Zuckerberg, 2015] Zuckerberg M., On Monday, 1 in 7 people on Earth used Facebook to connect with their friends and family, https://www.facebook.com/zuck/posts/10102329188394581, [último acesso: Out 2015]

[Michael Woodrow, 2014] Woodrow M., Cyber Security 2.0 & the History of the Internet, Lulu.com

[Michael Whitmam and Herbet Mattord, 2001] Whitman M., Mattord H., The principles of Information Security, Cegage Learning

[Mike Power, 2014] Power M., Drugs Unlimited: The Web Revolution That's Changing How the World Gets High, Macmillan

[Nancy Lind and Erik Rankin, 15] Lind N., Rankin E., Privacy in the Digital Age: 21st-Century Challenges to the Fourth Amendment [2 volumes]: 21st-Century Challenges to the Fourth Amendment, ABC Clio

[Neil Huges, 2002] Huges N., China's Economic Challenge: Smashing the Iron Rice Bowl, M.E. Sharpe

[Nildo Ello, 2015] Ello N., Descomplicando Passo A Passo Deep *Web*, Clube de Autores

[Nuno Coelho, 2012] Coelho N., Plano Diretor Informática Inovamais SA, 1ª edição, Inovaformação SA

[Osvaldo Santos, 2011] Santo O., Firewalls – Soluções Praticas, FCA

[Pamela Philips, 2013] Philips P., Foias for Prism Information, NSA, https://www.nsa.gov/public_info/_files/media_leaks_task_force/PRISM_*Email*.pdf, [último acesso Jan 2015]

[Paul O'Day, 2013] O'Day P., NSA Surveillance: How it's happening and why you should care, http://commons.pacificu.edu/cgi/viewcontent.cgi?article=1026&context=inter13, [último acesso Jan 2015]

[Paulo, et al., 2008] Santos P., Bessa R., Pimentel C., CyberWar – O Fenómeno, as tecnologias e os atores, FCA

[Pedro Franco, 2014] Franco P., Understanding Bitcoin: Cryptography, Engineering and Economics, John Wiley & Sons

[Pedro Silva et al., 2003] Silva P., Carvalho H., Torres C., Segurança dos Sistemas de Informação: Gestão estratégica da segurança empresarial, 1ª Edição, Centro Atlântico

[Pplware, 2015] Simões P., Dados dos utilizadores do euromilhões.com roubados, http://pplware.sapo.pt/informacao/alerta-dados-dos-utilizadores-do-euromilhoes-com-roubados/ [último acesso Ago 2014]

[Rebecca Makinnon, 2012] Makinnon R., Consent of the Networked: The Worldwide Struggle for Internet Freedom, Basic Books

[Reuters, 2015] Reuters, Ataque contra Ashley Madison causa calafrios em *sites* de encontro, http://br.reuters.com/article/internetNews/idBRKCN0QT1CV20150824, [último acesso Ago 2015]

[Richard Neiva, 2015] Neiva R., Fiber-optics cables could be the key to nsa snooping, http://www.cnet.com/news/fiber-optic-cables-could-be-the-key-to-nsa-snooping, [último acesso Jul 2015]

[Rob Waugh, 2015] Waugh R., Two suicides linked to Ashley Madison hack, http://metro.co.uk/2015/08/24/policeman-kills-himself-after-being-exposed-in-ashley-madison-leak-5358396/ [último acesso Out 2015]

[Robert Moore, 2010] Moore R., Cibercrime Investigating High-Technology Computer Crime, 1st edition, Routledg

[Rodrigo Rocha, 2013] Rocha R., Deteção em tempo real de ataques de negação de serviço na rede de origem usando um classificador bayesiano simples, Universidade Católica de Minas Gerais, https://*sites*.google.com/site/rcorcs/technical-reports/undergraduatedegreedissertationmajorpaperportuguese, [último acesso Dez 2014]

[Roger Dingledine, 2014] Dingledine R., Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government, https://pando.com/2014/07/16/tor-spooks/, [último acesso Ago 2015]

[Ronald Deibert et al., 2008] Deibert R., Palfrey J., Rohozinski R., Zittrain J., Stain ., Access Denied: The Practice and Policy of Global Internet Filtering, MIT Press

[Sam Murugesan, 2009] Murugesan S., Handbook of Research on *Web* 2.0, 3.0, and X.0: Technologies, Business, and Social Applications: Technologies, Business, and Social Applications, Information Science Refrence

[Sarosh Kuruvilla et al., 2011] Kuruvilla S., Lee C., Gallegher M., From Iron Rice Bowl to Informalization: Markets, Workers, and the State in a Changing China, Cornell Univertity Press

[Stuart Sumner, 2015] Sumner S., You: For Sale: Protecting Your Personal Data and Privacy *Online*, Syngress

[T. Ylonen and Lonvick C., 2006] Ylonen T., Lonvick C., The Secure Shell Transport Layer protocol, RFC 4253, https://www.ietf.org/rfc/rfc4253.txt, [último acesso Fev2015]

[Tim O'Reilly, 2009] O'Reilly T., What is *Web* 2.0, O'reilly Media Inc

[Tom Carpenter, 2011] Carpenter T., Microsoft Windows Operating System Essentials, John Wiley & Sons

[Thomas Hyslip, 2014]. Hyslip T., Top Hacks and Attacks of 2014, Thomas Hyslip

[University of Toronto, 2015] University of Toronto, Andrew Clement PHD Professor, http://www3.fis.utoronto.ca/faculty/clement/, [último acesso Set 2015]

[Wikipedia, S/D] Wikipedia, DarkNet, Redes Virtuais Privadas e https://pt.wikipedia.org/wiki/Darknet, [último acesso Dez 2014]

[Wikipedia, S/D] Wikipedia, Muscular Survailance Program, https://en.wikipedia.org/wiki/MUSCULAR_ (surveillance_program), [último acesso Ago 2015]

[Wired.com, 2015] Wired.com, Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise, http://archive.wired.com/politics/security/news/2007/09/embassy_hacks?currentPage=all, [último acesso Set 2015]

Anexo 1 – Formulário Navegação Web Anónima e Segura

Navegação Web Anónima e Segura

Descrição do formulário

Idade
- ○ 18 - 28
- ○ 29 - 39
- ○ 40 - 50
- ○ 51 - 90

Género
- ○ Masculino
- ○ Feminino

Àrea de Formação
Exemplo: Saúde, Tecnologia
- ○ Ciencias Sociais
- ○ Informática
- ○ Saúde
- ○ Juridica
- ○ Sem formação especifica

Já usou alguma vez uma maquina virtual?
Exemplo: VirtualBox, VMWare
- ○ Sim
- ○ Não

Sabe iniciar o seu computador através da unidade de CD/DVD?
Arrancar um CD/DVD pelo dispositivo CD/DVD em vez do Disco Rígido.
- ○ Sim
- ○ Não
- ○ Não possuo unidade CD/DVD no computador.

Já usou antes um sistema Linux?
Exemplo: Ubuntu, CentOS, etc.
- ○ Sim
- ○ Não

Usou o LiveDVD (protótipo) com recurso a máquina virtual?
- ☐ Sim
- ☐ Não
- ☐ Não, usei diretamente na drive CD/DVD

Ao usar o Browser TOR e ao pesquisar no Google a sua localização que resultado obteve?
Exemplo para colcoar no google: What is my location
- ☐ A minha localização actual e verdadeira.
- ☐ Uma localização diferente da minha, noutro pais.

Ao usar o Browser Firefox e ao pesquisar no Google a sua localização que resultado obteve?
Exemplo para colcoar no google: What is my location

- [ ] A minha localização atual e verdadeira.
- [ ] Uma localização diferente da minha, noutro país.

Caso a resposta à pergunta anterior seja "Uma localização diferente da minha, noutro país" sentiu-se seguro com o nível de segurança do LiveDVD?

- [ ] Sim
- [ ] Não

O aspecto geral do sistema operativo é apelativo?
Exemplo: Usabilidade, Menus, Icones, etc.

- ( ) Sim
- ( ) Não