Segurança Informática em Ambientes de Avaliação Escolar

Mestrado em Cibersegurança e Informática Forense

Trabalho de Projeto

Nuno Alexandre Pereira Anacleto

Leiria, julho de 2019

Mestrado em Cibersegurança e Informática Forense

Trabalho de Projeto

Segurança Informática em Ambientes de Avaliação Escolar

Nuno Alexandre Pereira Anacleto

Projeto de Mestrado realizado sob a orientação do Professor Doutor Patrício Rodrigues Domingues, Professor da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.

Leiria, julho de 2019

Originalidade e Direitos de Autor

O presente relatório de projeto é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Agradecimentos

Antes de mais, quero agradecer em geral, a todas as pessoas que contribuíram para a minha formação profissional e académica as quais me muniram da capacidade para elaborar o presente trabalho de projeto.

A conceção da aplicação intitulada de «PC Border», à qual este relatório é afeto, foi em parte conseguida, graças à utilização de *software* de terceiros os quais são essenciais ao seu funcionamento. A ferramenta «psExec» e o utilitário «USBDeview» concebidos pela Sysinternals e Nirsoft respetivamente, foram fundamentais para poder alcançar parte dos objetivos da referida aplicação. Sem estes dois *softwares* não teria sido possível conceber a aplicação, pelo menos com as funcionalidades com que foi, de modo a cumprir a função para a qual foi idealizada. Os meus parabéns e agradecimentos aos autores destes dois *softwares*.

Cabe-me igualmente agradecer ao Professor Doutor Luís Alexandre Lopes Frazão também da Escola superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, que, sendo possuidor de conhecimento na área em estudo, me deu a conhecer da capacidade que os sistemas operativos em análise têm de iniciar sessão sem intervenção humana, mesmo que as credenciais em utilização possuam senha definida.

Preza-me ainda agradecer ao meu orientador, Professor Doutor Patrício Rodrigues Domingues, pela forma como conduziu a orientação do presente trabalho. Foi instrumental para o sucesso do trabalho pela forma insistente, minuciosa e dedicada que prestou no papel de orientador, contribuindo para a chegar ao estado final da aplicação e do presente relatório.

Resumo

Nos dias que correm, os sistemas informáticos desempenham um papel fundamental na vida das pessoas bem como das organizações, pois tornaram-se imprescindíveis para o desempenho de muitas das suas atividades. O mesmo sucede com as empresas de formação profissional, escolas ou até outras entidades que providenciam formação aos próprios trabalhadores. Uma parte significativa de formações assenta em sistemas informáticos para efeitos de aprendizagem e de avaliação. Como em qualquer processo de avaliação, é necessário assegurar que esse processo seja transparente e, idealmente impenetrável a fraudes. Contudo, pela sua complexidade, os sistemas informáticos expõem uma vasta superfície de ataque que pode ser explorada por utilizadores maliciosos, especialmente nos momentos de avaliação, para, através da fraude obterem bons resultados.

Este trabalho tem como objetivo o estudo de meios e de formas de prevenção de utilização ilícita de tais tecnologias em sistemas Microsoft Windows bem como a criação de *software* para utilização nos momentos de avaliação em entidades de formação que, por motivos orçamentais, tecnológicos ou de puro desconhecimento, não o possam conseguir de outra forma.

Palavras-chave: *Segurança, TI, Pendrive, Monitorização, Controlo, Windows*

Abstract

Nowadays, information technology (IT) equipment plays a fundamental role in the lives of people as well as of organizations, as they became an indispensable commodity of their day to day activities. The same occurs with enterprises aimed at professional qualification, schools or even other entities that can qualify their own personnel. The highly flexible ways IT equipment can be used, is at the same time its greatest commodity and its main weakness. Indeed, the versatility of IT hardware and software can be put to good use in large automated systems, but it can also be abused by fraudsters to cheat in evaluations.

This main goal of this work is to study the ways and means of preventing fraudulent behaviour when Microsoft Windows systems are used for computer-based assessment of students. For this purpose, a low-cost software-based solution was developed. The emphasis of this solution is to minimise the computational and human resources needs, and as much as possible, to attain zero-configuration.

Keywords: *Security, IT, Flash drive, Monitorization, Control, Windows*

Índice

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Acrónimos

ACL	*Access Control List*
AD	*Active Directory*
ARP	*Address Resolution Protocol*
DP	*DisplayPort*
GUI	*Graphical User Interface*
IDE	*Integrated Development Environment*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
NTFS	*New Technology File System*
PC	*Personal Computer* (Computador Pessoal)
SID	*Security Identifier*
SO	Sistema Operativo
TCP	*Transmission Control Protocol*
TI	Tecnologias de Informação
USB	*Universal Serial Bus*
WMI	*Windows Management Instrumentation*
WOL	*Wake On LAN*

Capítulo 1 – Introdução

As Tecnologias de Informação (TI) de auxílio à formação de pessoas são diversas, desde o simples processador de texto, até às plataformas de ensino à distância que permitem efetuar a avaliação dos formandos.

As empresas ou instituições que tiram partido destas tecnologias também diferem entre si, umas estão mais adaptadas e outras menos. As razões para que haja diferenças na adaptabilidade destas entidades a estes sistemas tecnológicos podem ir do simples desconhecimento, passando pelo constrangimento orçamental, até mesmo a políticas funcionais da própria entidade.

Quando se lida com as TI, há que ter em consideração a Segurança Informática, que passa pela segurança física e lógica das infraestruturas, das redes e dos terminais a elas ligados. A Segurança Informática, na sua essência, protege a informação que cada um tem nos seus sistemas informáticos[1].

Assim sendo, as entidades que prestam serviços de formação e que estão menos capacitadas para a segurança informática, aquando dos momentos de avaliação dos seus formandos, podem estar a contribuir para uma incorreta avaliação dos mesmos, ou de formandos vindouros, sem sequer estarem cientes desse facto.

Um exemplo da utilização fraudulenta das TI, é a ligação de um dispositivo de armazenamento externo à máquina onde a avaliação está a decorrer, possibilitando a extração de uma cópia do exame efetuado.

No sentido de minimizar a utilização das TI de forma fraudulenta, existem alguns meios disponíveis para o efeito, mas nem todos estão sempre ao dispor dos administradores. As TI, por outro lado, são constituídas por mecanismos muito versáteis que permitem a existência de diversas formas de conseguir o mesmo objetivo – o desafio é identificá-las, conjugando-as de forma a obter os efeitos desejados.

1.1 Objetivos

O conceito de segurança nos sistemas informáticos refere-se aos cuidados, mecanismos e ferramentas que podem ser implementados para proteger a informação que as empresas possuem, principalmente a que é considerada sigilosa[2].

Com o presente trabalho, pretende-se o estudo e levantamento de informações necessárias para posterior criação de uma ferramenta capaz de alcançar vários objetivos. Estes objetivos procedem do princípio fundamental de permitir ao avaliador, com um simples toque do botão, isolar as máquinas onde decorrem as avaliações sem que para tal, comprometa os requisitos das próprias avaliações.

As máquinas alvo das avaliações, referidas anteriormente, farão parte dum Domínio A.D. que não será controlado pelos seus administradores locais ou, serão simplesmente *standalone*. Em ambos os casos, a forma de atingir os objetivos propostos, requererá perícia nas configurações que são diversamente específicas.

1.1.1 Vulnerabilidades

Na prossecução dos objetivos propostos, foram identificadas algumas vulnerabilidades a ultrapassar, sendo estas: os dispositivos de armazenamento em massa ligados aos portos USB (*Universal Serial BUS*); os leitores de CD, DVD ou Blu-ray; a própria rede informática; a «Área de transferência» (*clipboard*) e as aplicações utilizadas.

1.2 Contributos

Este trabalho teve como fator impulsionador uma necessidade real que uma entidade militar tem na formação e avaliação de militares no cumprimento da sua missão.

Os principais contributos deste projeto confluem para a criação de um *software – PC Border –* que confira a um docente/formador, apenas com conhecimentos informáticos na ótica do utilizador, a capacidade de facilmente limitar o acesso aos recursos que os utilizadores de uma estação de trabalho poderão ter:

i) Inibir a utilização de dispositivos de armazenamento que utilizam portos USB;
ii) Impedir a remoção de discos óticos dos seus leitores;
iii) Limitar o acesso à rede apenas ao estritamente necessário;

iv) Impedir a utilização da «Área de transferência»;
v) Limitar a utilização de aplicações consoante o necessário;
vi) Definir quais as contas de utilizador autorizadas.

O referido software preza ainda pela simplicidade e pela facilidade com que o operador configura as máquinas para diferentes objetivos, bem como, a capacidade de remotamente ligar as referidas máquinas, utilizando o protocolo Wake On LAN (WOL), e ainda, de iniciar automaticamente sessão nestas máquinas.

1.3 Organização do documento

Este documento encontra-se organizado da seguinte forma. O Capítulo 2 descreve o estado da arte, uma parte importante do trabalho científico, pois refere o que já foi descoberto e criado sobre os temas revelantes para o objetivo do trabalho. O Capítulo 3 descreve as restrições e requisitos, bem como, os pressupostos da solução implementada. Aqui são descritos os procedimentos e os princípios utilizados para alcançar os objetivos secundários. A unificação de cada objetivo secundário leva ao objetivo do trabalho. O Capítulo 4 refere os passos e a técnica utilizada na conceção do *software*. O Capítulo 1 reporta os testes efetuados na verificação da correta operação da aplicação concebida. No último capítulo são sintetizadas as principais conclusões.

Capítulo 2 Estado da Arte

Este capítulo apresenta o estado da arte das técnicas passíveis de serem utilizadas na prevenção e deteção de fraude nos processos de avaliação que assentam sobre plataformas informáticas.

2.1 Introdução

Atualmente no mercado, existem algumas ferramentas que permitem alcançar determinados objetivos, mas não existe nenhuma que consiga alcançar todas as necessidades de segurança que são recomendadas para um ambiente de avaliações. Num tal ambiente, será necessário desativar a capacidade de transferir informação pelos portos USB, cartões de memória ou leitores de discos óticos, impedir a transferência de dados pela rede, desativar as funções de «copiar» e de «colar», e ainda, impedir a utilização de aplicações que não sejam necessárias para as avaliações.

2.2 Portos USB e Thunderbolt

Os portos USB são o meio de implementação de um protocolo de ligação de periféricos a um computador. O desenvolvimento desta tecnologia começou em 1994[1]. Desde então esta tecnologia sofreu evoluções, principalmente na largura de banda. Começou na versão 1.0 e presentemente está na versão 3.2. As velocidades máximas de transferência são 12Mbps e 20Gbps respetivamente. A versão 2.0, que opera a uma velocidade máxima de 480Mbps, permite a transferência de ficheiros relativamente pequenos para um disco externo com grande eficiência. Os teóricos 60 megabytes por segundo são mais que suficiente para o efeito, especialmente quando se trata de documentos.

A tecnologia «*Thunderbolt*»[2] [3], que utiliza o cobre como meio de comunicação, teve origem na tecnologia «*Light Peak*»[3] [4], que tencionava tirar partido de fibra ótica para comunicação

[1] http://www.allusb.com/usb-history
[2] https://newsroom.intel.com/news-releases/thunderbolt-technology-the-fastest-data-connection-to-your-pc-just-arrived/
[3] https://blog.macsales.com/37190-thunderbolt-3-a-brief-history-of-thunderbolt

multimédia. Lançada pela primeira vez em 2011, a «*Thunderbolt*» tinha uma largura de banda de 10Gbps e capacidade para ligar dispositivos de armazenamento externo, pois combina os BUS «*PCI Express*» (PCIe) e *DisplayPort* (DP)[4] numa só ligação. Esta tecnologia sofreu duas evoluções, cada uma duplicando a largura de banda. Sendo a mais rápida tecnologia para ligação de dispositivos de armazenamento externo à data, cerca do dobro da USB 3.2, é mais utilizada nos computadores Apple Macintosh.

2.2.1 Software disponível

USB Disabler Pro

O *software* «USB Disabler Pro[5]» [5] da empresa «IntelliAdmin, LCC» tem a capacidade de bloquear dispositivos de armazenamento externo que utilizam portos USB, sem afetar o normal funcionamento de outros periféricos, tais como, ratos, impressoras, leitores biométricos, etc. No ato da instalação, este programa requer que seja identificado um administrador ou um grupo de administradores, os quais terão capacidade de controlar este *software*, autorizando ou negando os diversos equipamentos de armazenamento externo que possam ser ligados na máquina onde está a ser executado. Um administrador do programa tem a possibilidade de definir se o *software* apresenta ou não um alerta quando um dispositivo for introduzido. Após a introdução de um dispositivo e se os alertas estiverem ativos, este programa apresenta uma caixa de diálogo, informando o utilizador que o equipamento introduzido passou a estar na lista dos dispositivos não autorizados conforme se apresenta na Figura 1.

Figura 1 – Alerta de novo equipamento

[4] https://www.dell.com/support/article/pt/pt/ptbsdt1/sln300756/frequently-asked-questions-faqs-about-the-thunderbolt-port-on-a-dell-pc
[5] http://www.intelliadmin.com/index.php/usb-disabler-pro/

Carregando no botão «Add to allow list» (ver Figura 1), um administrador, mesmo na sessão de qualquer outro utilizador sem privilégios de administração, pode autorizar que determinado equipamento passe a estar autorizado, bastando fornecer as suas credenciais conforme é indicado Figura 2.

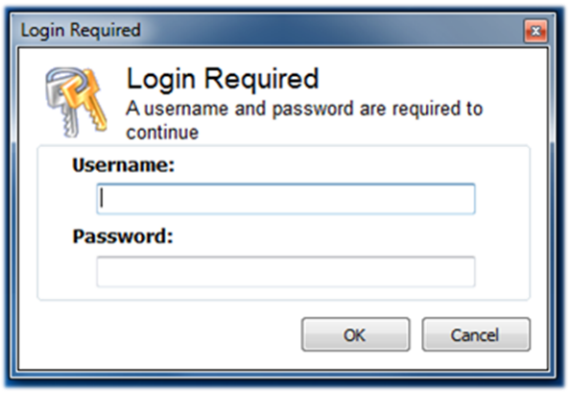

Figura 2 – Diálogo de *Login*

O programa é bastante intuitivo na sua utilização, mas torna-se um pouco confuso na identificação de quais os dispositivos que estão autorizados especialmente quando são de modelos iguais. A Figura 3 representa a janela onde é possível definir o estado dos dispositivos que se encontram registados.

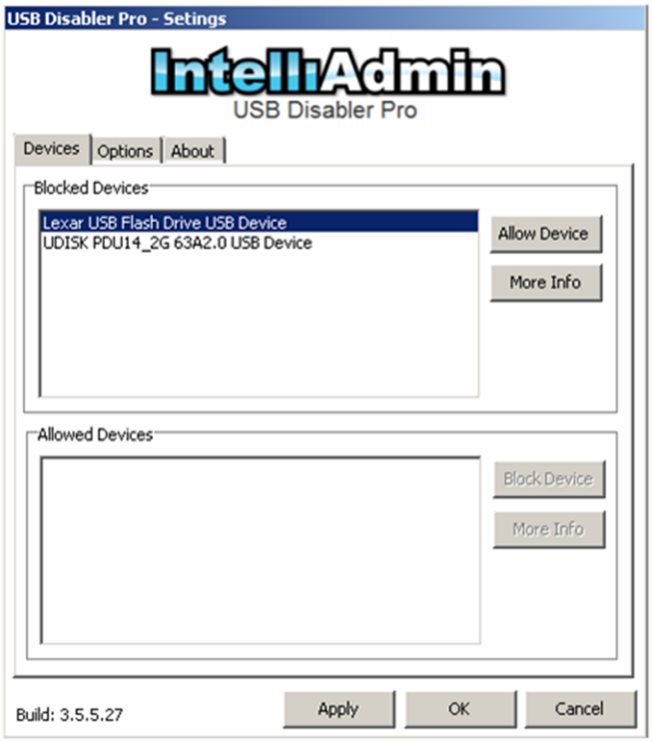

Figura 3 – Estado dos dispositivos

Este *software* tem a opção de alertar ou não o utilizador sempre que um dispositivo de armazenamento USB seja introduzido. Permite ainda que qualquer administrador tenha sempre acesso aos seus equipamentos, tal como demonstrado na Figura 4.

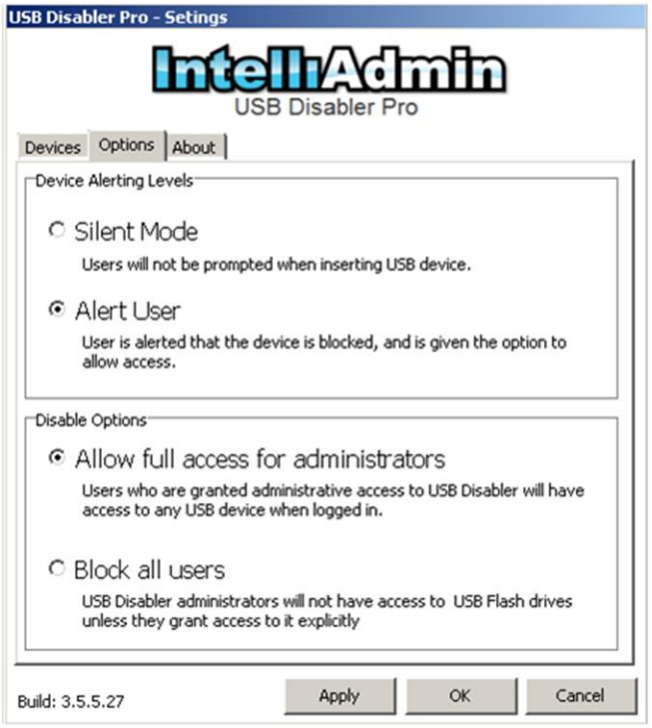

Figura 4 - Configurações

O programa, no entanto, não foi concebido para ser gerido centralmente, exigindo que em qualquer alteração, o administrador tenha de efetuar, de alguma forma, um acesso interativo com a máquina em questão. Este facto, torna impraticável a sua utilização em salas de aula com um número significativo de máquinas. Tem uma outra grande desvantagem, é que uma vez instalado, não permite ser colocado em modo 'inativo', tornando-se num fardo para o administrador cada vez que estas máquinas não estejam a ser utilizadas para avaliações e que a utilização destes dispositivos de armazenamento externo esteja efetivamente permitida a qualquer dos formandos.

Figura 5 – Fim do período experimental

Na versão com compilação 3.5.5.27, a única que foi testada, foi identificado um «*bug*», pelo facto de continuar a bloquear os dispositivos, mesmo após expirar o período de graça. Na Figura 5, consegue ver-se a mensagem onde a aplicação informa que já não está a bloquear os equipamentos USB, mas, no entanto, o certo é que não se consegue ter acesso ao equipamento, pois a sua letra de unidade de disco continua a ser removida.

Windows USB Blocker

A Figura 6 representa um *software* designado de «Windows USB Blocker»[6] [6] que pode ser utilizado através de um GUI ou executado por *script*, mas apenas permite bloquear ou desbloquear indiferenciadamente qualquer dispositivo de armazenamento externo ligado a um porto USB. Os comandos disponíveis por linha de comandos são:

```
WindowsUSBBlocker.exe [ /block | /unblock | /status | /help]
```

Figura 6 – Windows USB Blocker

[6] https://securityxploded.com/windows-usb-blocker.php

USB-Block

Um terceiro *software*[7] com capacidades muito semelhantes ao primeiro utilitário apresentado, indica que permite o bloqueio, para além dos dispositivos de armazenamento externo via USB, o bloqueio de unidades de rede, de leitores de CD/DVD/BR e ainda de discos internos que não façam parte do sistema operativo. A Figura 7 mostra a interface da aplicação.

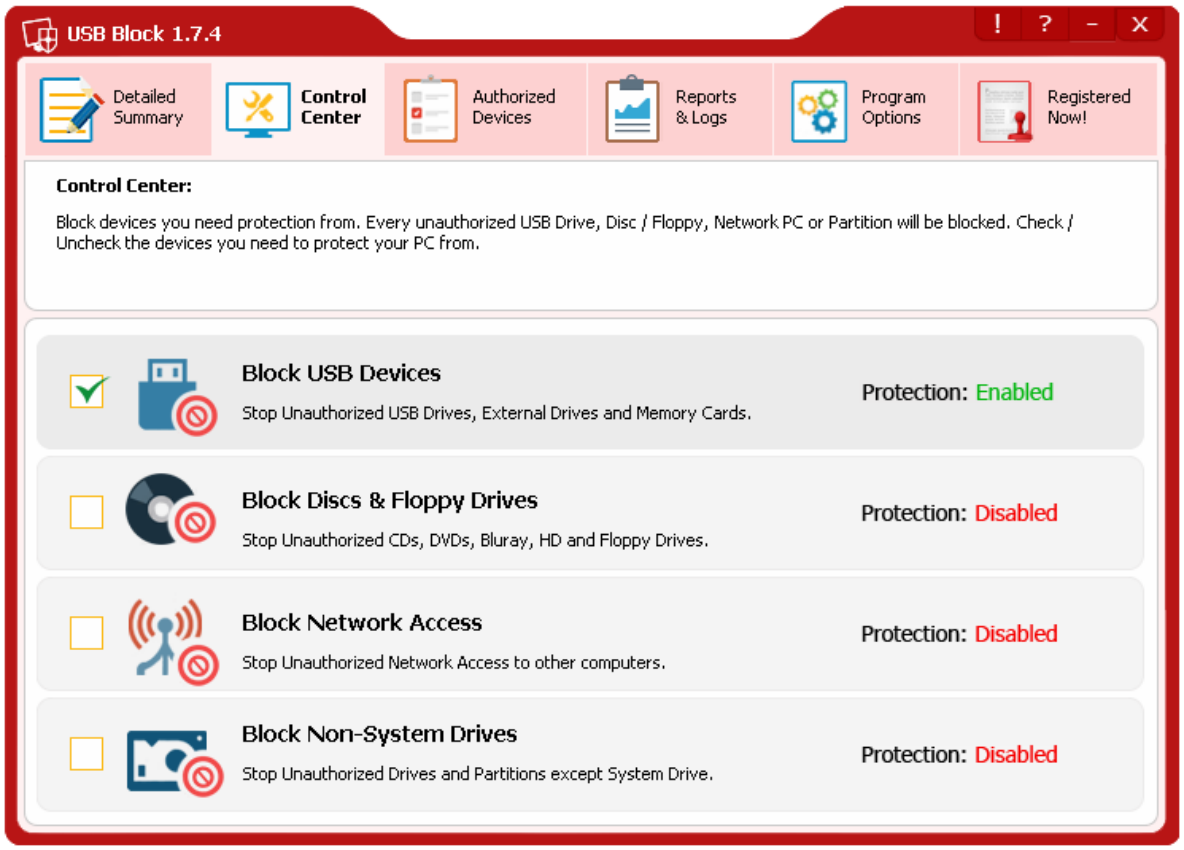

Figura 7 – Aplicação USB Block 1.7.4

Com um período *trial* agregado a um número limitado de bloqueios efetuados, esta aplicação designada de «USB-Block» que até fornece *logs* de eventos ocorridos nos dispositivos que controla, funciona de forma reativa e não proativa. É uma aplicação com um avanço significativo em relação ao «USB Disabler Pro», contendo todas as suas funcionalidades e outras mais. Possui uma funcionalidade extra que é a de bloquear o acesso a unidades de rede e impressoras. Esta funcionalidade é excelente, pois ambos os dispositivos são passíveis de serem utilizados em avaliações com o fim constituir uma fraude. Uma outra novidade que tem, é o facto de detetar tentativas de violação da própria aplicação, quer por remoção, quer por

[7] http://www.newsoftwares.net/usb-block/

eliminação direta dos seus ficheiros, quer ainda por tentativas falhadas de acesso à interface gráfica. A Figura 8 apresenta os detalhes da aplicação.

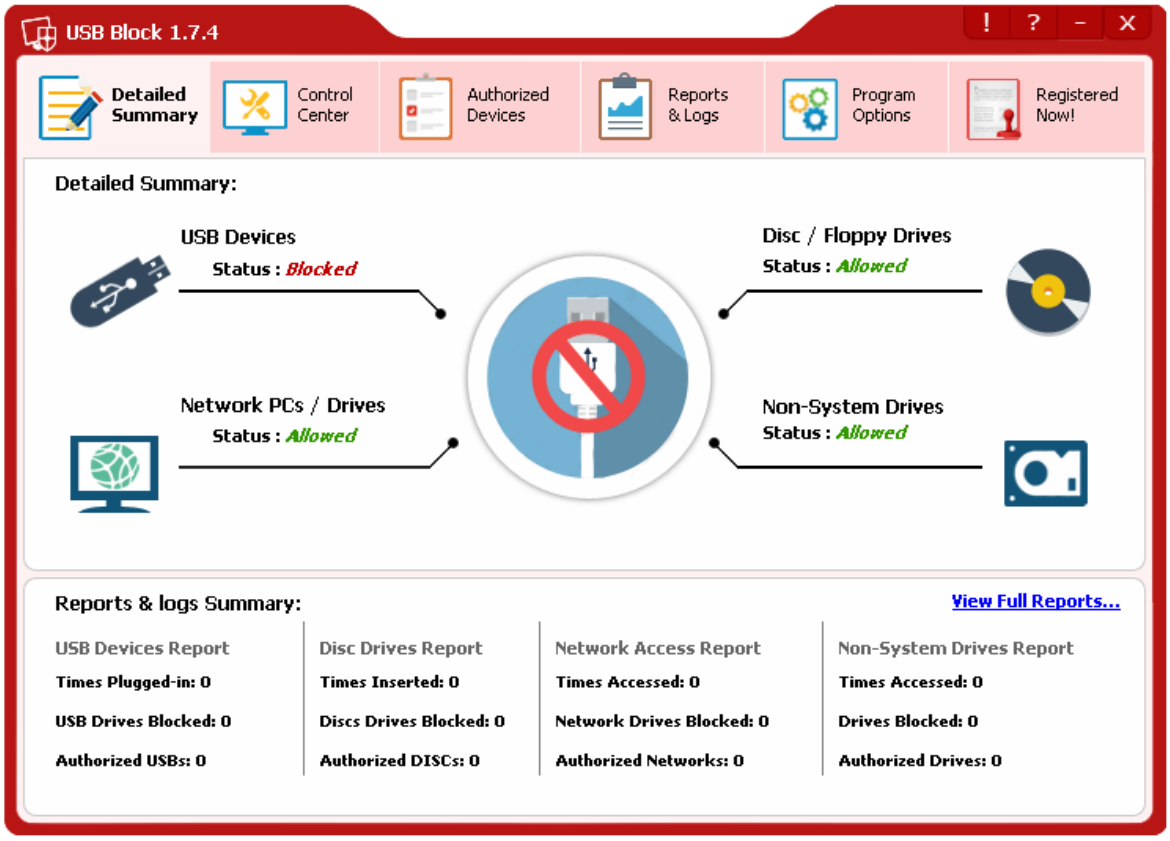

Figura 8 – Aplicação USB Block (Detalhes)

Infelizmente, tal como o primeiro *software*, esta aplicação não foi concebida para ser administrada centralmente, logo não permite o controlo de diversas máquinas. Foi também detetado que, no equipamento testado, a aplicação não funcionou como esperado, permitindo que todas as unidades de armazenamento USB funcionassem sem bloqueio. Apresenta ainda um funcionamento nada suave, pois não responde de imediato aos comandos dados pelo utilizador e, ao deslocar-se pelo ecrã, fá-lo com atrasos.

NoDrives Manager

Uma nova e intrigante abordagem à inibição de acesso aos dispositivos de armazenamento de dados é conseguida pelo utilitário «NoDrives Manager»[8] [7] representado na Figura 9. Este utilitário simplesmente mascara as letras das unidades de disco, impedindo que o utilizador consiga ver as ditas unidades. Desta forma, no entanto, não é executado qualquer tipo de

[8] http://nodrvman.sourceforge.net/

bloqueio e, se o utilizador souber qual a letra da unidade de armazenamento que pretende utilizar, conseguirá na mesma obter acesso aos ficheiros lá existentes.

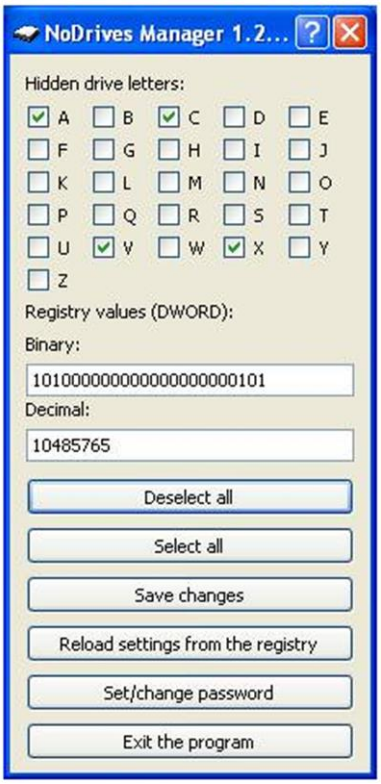

Figura 9 – Aplicação «NoDrives Manager»

A própria Microsoft refere duas formas [9] [8] de impedir o acesso aos dispositivos de armazenamento externo cuja interface de comunicação é um porto USB. Uma das formas é através da negação de acesso a dois ficheiros que são *drivers* dos equipamentos. Estes ficheiros, com os nomes «*Usbstor.pnf*» e «*Usbstor.inf*», encontram-se na diretoria «Inf» que, por sua vez, se encontra na «*Windows*». Para negar o acesso a estes ficheiros, tem de explicitamente negar-se as permissões «*Full Control*» aos utilizadores e à conta «*SYSTEM*». A outra forma, é através da alteração de um valor na *Registry* do próprio sistema operativo. A chave «Start» na *hive* «HKLM\SYSTEM\CurrentControlSet\services\USBSTOR» é o registo que indica se um dispositivo de armazenamento via USB é ou não iniciado. Por omissão, o valor é «3», mas alterando para «4», consegue-se que estes equipamentos não sejam montados. Ao alterar esta chave para «4», o gestor de dispositivos do Windows dá a indicação que o controlador está desativo. Estas formas de impedir o acesso aos dispositivos de armazenamento externos pelo

[9] https://support.microsoft.com/en-us/help/823732/how-can-i-prevent-users-from-connecting-to-a-usb-storage-device

porto USB, apenas funcionam se o dispositivo ainda não tiver sido colocado, ou seja, se for efetuada qualquer uma destas alterações com um destes equipamentos já introduzidos, ele continuará a funcionar normalmente.

O Windows, por outro lado, regista o número de série de cada dispositivo USB que é inserido no sistema. Esta identificação é única para cada dispositivo, logo permite distinguir qual o equipamento a que se refere. Esta particularidade é explorada pelo *software* que seguidamente se descreve.

USBDeview

Até agora, as soluções apresentadas, ou necessitam de licenças pagas, e/ou não produzem os resultados desejados. Por outro lado, o utilitário «USBDeview»[10] [9], que não necessita de instalação e é *freeware*, permite bloquear de forma eficaz e com bastante simplicidade, qualquer

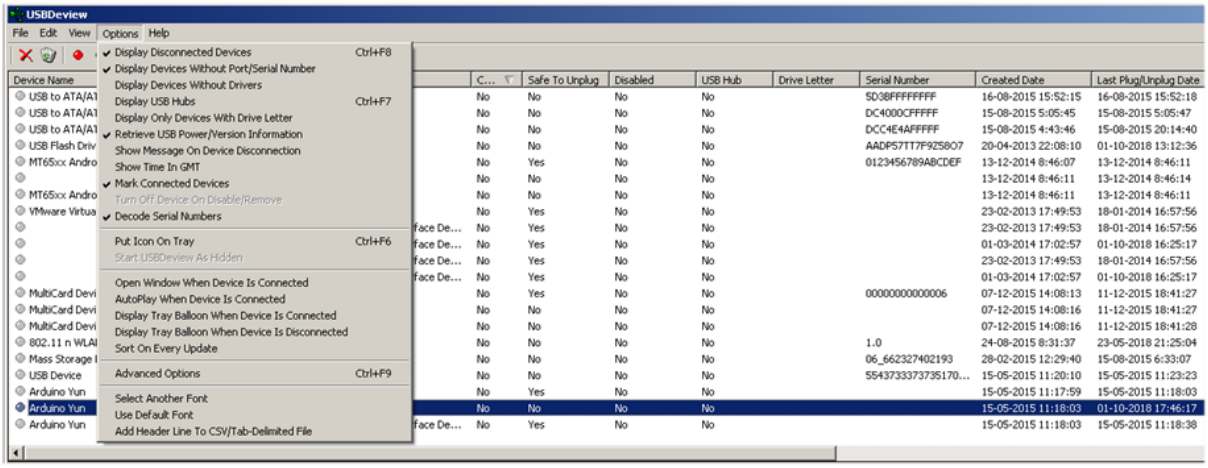

Figura 10 – O utilitário USBDeview

equipamento ligado por porto USB independentemente da sua funcionalidade. A Figura 10 apresenta de relance este utilitário. Não sendo concebido para ser «amigo do utilizador» é, no entanto, uma ferramenta bastante poderosa na gestão de todos os equipamentos USB ligados à máquina local ou até em máquinas remotas. Pelo detalhe da informação que apresenta, é excelente para auxiliar numa análise forense. Este utilitário tem a capacidade de exportar para diversos formatos os resultados obtidos, incluindo HTML e XML. A capacidade que também possui de ser utilizado através de linha de comandos, tanto para verificar o estado dos dispositivos, como para os configurar e pelo facto de ser *freeware*, faz deste utilitário uma

[10] https://www.nirsoft.net/utils/usb_devices_view.html

ferramenta bastante útil e pronta para combinar no funcionamento de outros *softwares*. A Tabela 1 faz comparação dos *softwares* apresentados, evidenciando as suas características mais relevantes. Um breve resumo da referida tabela passa por referir que o «Tipo de Administração» indica se o *software* possui a capacidade de manipular máquinas remotas ou apenas a máquina na qual está a ser executado. A capacidade de bloquear determinado equipamento USB baseado no seu número de série ou ID (Identificação) próprio, é indicado pelo «Bloqueio Seletivo». Em «Utilização de *Daemon*» são indicados os *softwares* que necessitam de uma componente própria em permanente execução. Por fim, a apreciação global destes *softwares* é baseada nas suas funcionalidades e na eficácia do seu funcionamento.

Tabela 1 – Resumo das aplicações de bloqueio de dispositivos de armazenamento USB

DESIGNAÇÃO DO SOFTWARE	USB Disabler Pro	Windows USB Blocker	USB Block	NoDrives Manager	USBDeview
TIPO DE ADMINISTRAÇÃO	local	local	local	local	remota
BLOQUEIO SELETIVO	sim	não	sim	não	sim
FEEDBACK AO UTILIZADOR	sim	não	sim	não	não
DIFERENCIAÇÃO ENTRE UTILIZADOR E ADMINISTRADOR	sim	não	não	não	não
AMIGO DO UTILIZADOR	sim	sim	sim	sim	não
UTILIZAÇÃO DE *DAEMON*	sim	não	sim	não	não
OPÇÃO LINHA DE COMANDOS	não	sim	não	não	sim
APRECIAÇÃO GLOBAL	boa	fraca	média	fraca	excelente

2.3 Utilização da rede

Uma rede informática pode ser constituída por equipamentos que utilizam o meio ambiente, os cabos de cobre ou a fibra ótica como meio de transmissão. Estes equipamentos, por sua vez, utilizam ainda tecnologias e protocolos diferenciados entre si. Como exemplo, ambos o *Wireless* e o *Bluetooth* utilizam ondas eletromagnéticas como forma de propagação, no entanto, as tecnologias e protocolos que empregam são bastante diferentes. As larguras de banda empregues também variam bastante. Presentemente, embora a diversidade existente, a comunicação entre máquinas é maioritariamente efetuada com recurso ao protocolo de comunicação TCP/IP. Este protocolo atualmente existe em duas versões, a versão 4 (IPv4) e a versão 6 (IPv6). A primeira definição do protocolo IPv4 surgiu em janeiro de 1980 documentada pela RFC760 [10]. A primeira proposta da versão IPv6 surgiu em dezembro de 1995 através da RFC1883 [11]. Em dezembro de 1998, surgiu o primeiro esboço [12] desta

versão, dando origem às primeiras redes a operar em IPv6, mas foi só em julho de 2017 que surgiu a norma definitiva da versão conforme documentado pela RFC8200 [13]. Cerca de 23 anos após os primeiros traços desta última versão, o IPv4 continua a reinar, mesmo estando esgotados todos os blocos de endereços públicos que os *Regional Internet Registry* (RIR) têm para distribuir.

Existem atualmente vários equipamentos de rede para análise e controlo de tráfego, desde o simples *router*, até aos sistemas mais complexos de *Intrusion Prevention System* (IPS), no entanto, estes exigem dois ou mais segmentos de rede diferentes. Enquanto todo o tráfego que transita de uma rede para outra é processado por estes equipamentos, a circulação de determinado tipo de tráfego dentro da mesma rede é feita com recurso a uma tabela de endereços (ARP) que os equipamentos possuem. Estas tabelas permitem associar um endereço IP com o respetivo endereço MAC (*Media Access Control*), indicando o porto físico onde o destino se encontra conectado. A maneira menos complexa e totalmente independente de impossibilitar a circulação de tráfego dentro do mesmo segmento de rede é impedir que ele lá seja colocado. Assim, inviabilizando a informação destas tabelas, consegue-se impedir a circulação de tráfego na mesma rede sem que este seja processado por qualquer equipamento.

2.3.1 Tráfego roteado

Com roteamentos estáticos, consegue-se reencaminhar o tráfego por onde se considerar mais apropriado, ou caso se pretenda que ele não chegue a sair da máquina, encaminhá-lo por onde se sabe não ter saída. No exemplo apresentado na Figura 11, consegue-se reparar que a rota «por omissão», identificada pelo destino de rede «0.0.0.0», sai pela *interface* com o IP 192.168.0.8 e tem como destino o equipamento com o IP 192.168.0.1 que é a «*Default Gateway*» ou roteador (*router*) para outras redes.

Figura 11 – Rota «por omissão»

É possível alterar esta rota encaminhando o tráfego para outro destino, utilizando, para tal, o comando '*route ADD 0.0.0.0 MASK 0.0.0.0 x.y.z.k*', onde «x.y.z.k» é o IP de destino. Pode

também ser eliminada, o que deixa a máquina sem saber por onde deve enviar o tráfego com destino a uma rede que não a sua. A Figura 12 mostra-nos que é realmente possível eliminar a rota «por omissão» através de linha de comandos. O comando a executar para obter este resultado é «*route DELETE 0.0.0.0*».

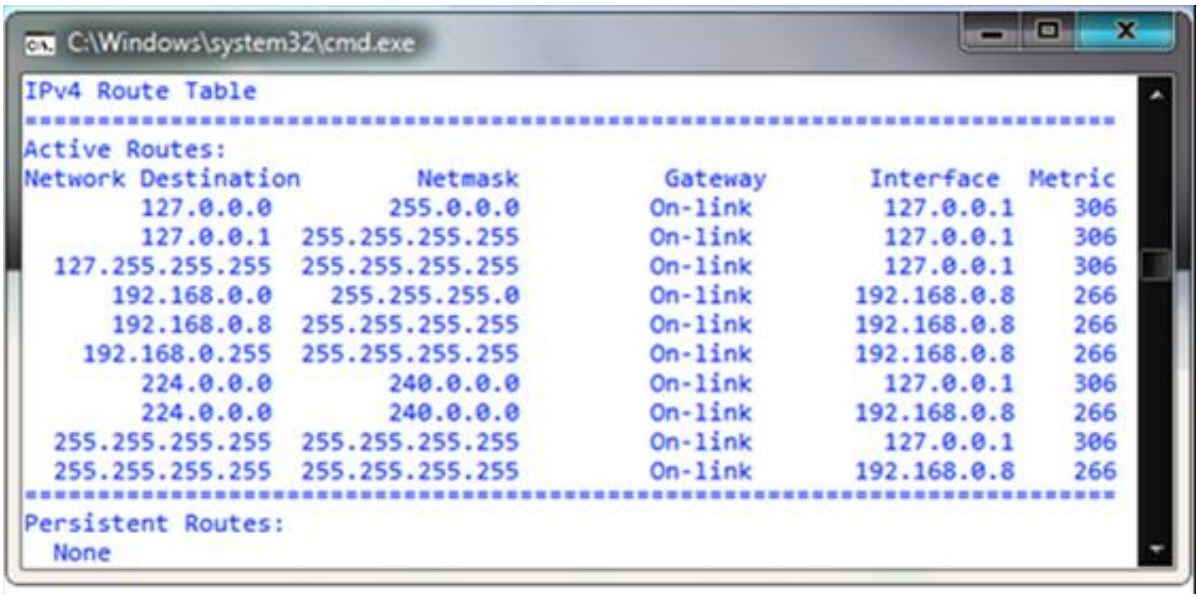

Figura 12 – Auxência da rota «por omissão»

2.3.2 Tráfego dentro de um segmento de rede

Na comunicação dentro do mesmo segmento de rede, a máquina que pretende iniciar uma sessão vai pesquisar a sua tabela de ARP (*Address Resolution Protocol*) e, caso não contenha a entrada para o IP de destino, injeta um pacote *broadcast* ARP de *layer 2* pela interface de rede correspondente, que é posteriormente distribuído por todo o segmento de rede a que pertence. O equipamento com o endereço IP enviado no pedido ARP responde com um «ARP reply» que é dirigido somente à máquina que fez o pedido. Após a receção da resposta, ambas as máquinas ficam conhecedoras do «*MAC address*» da outra e acrescentam-no à sua tabela de ARP. Neste momento, a comunicação é feita sem recurso à camada 3 (*layer* 3), logo a alteração de rotas não serve de nada. Nesta situação, para impedir determinado tráfego de sair de uma máquina, é necessário recorrer a uma *firewall* ou à manipulação da própria tabela de ARP da máquina.

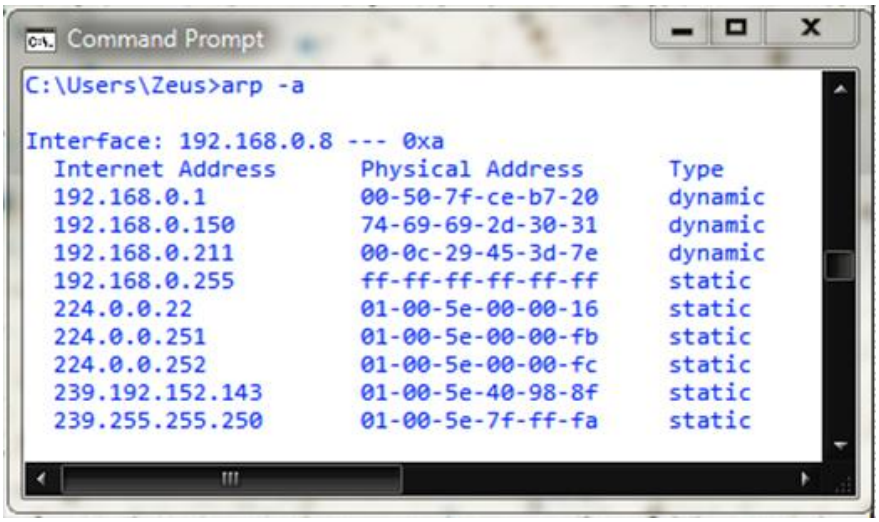

Figura 13 – Tabela de ARP

O comando «arp -a» identificado na Figura 13 mostra as entradas existentes na tabela ARP da máquina. Após executar o comando «arp -s 192.168.0.150 74-69-69-2d-30-34», passou a existir uma entrada estática na tabela de ARP, indicando que todo o tráfego com o destino IP de «192.168.0.150» será encaminhado para quem tem o MAC-Address «74-69-69-2d-30-34», o que faz com que estre tráfego seja impedido de chegar ao seu destino conforme retratado na Figura 14.

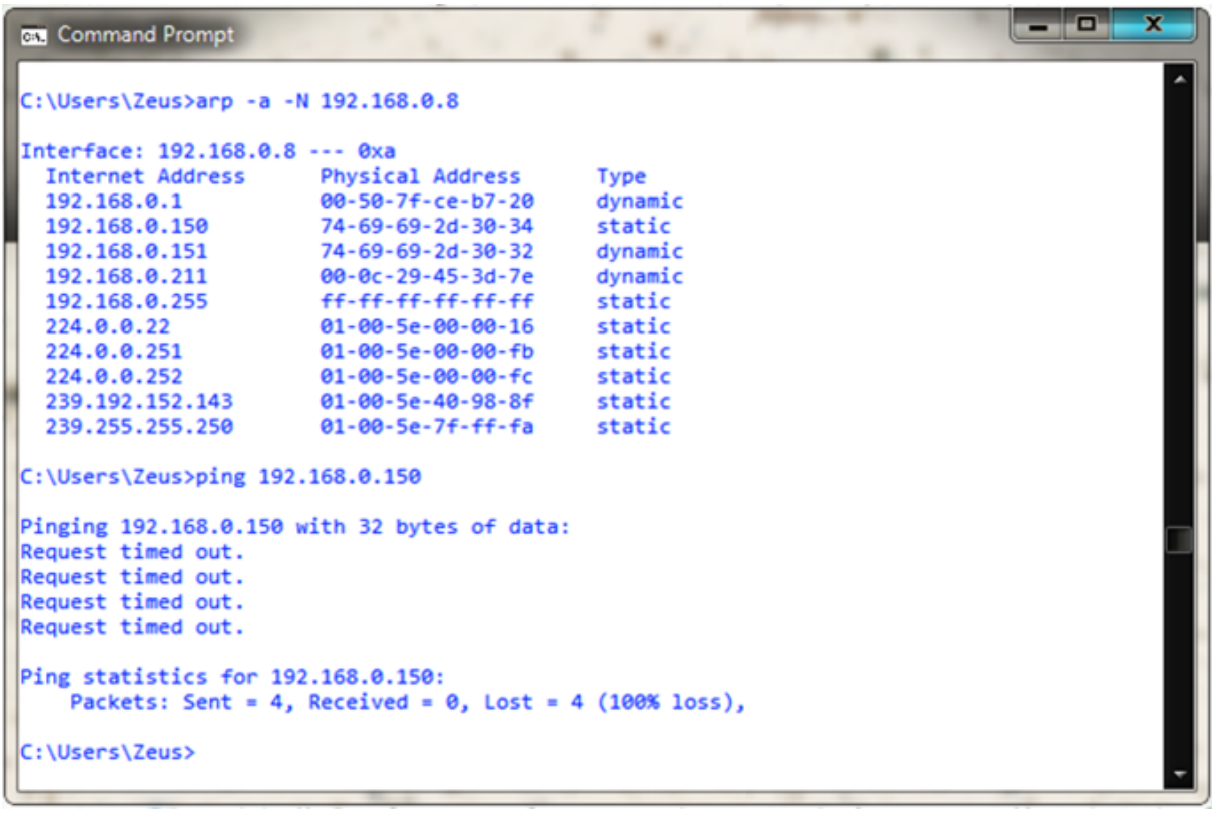

Figura 14 – Alteração da Tabela de ARP

Para desfazer a ação anterior e normalizar o sistema, o comando «arp -d 192.168.0.150» consegue esse feito. A Figura 15 retrata o resultado da utilização do referido comando.

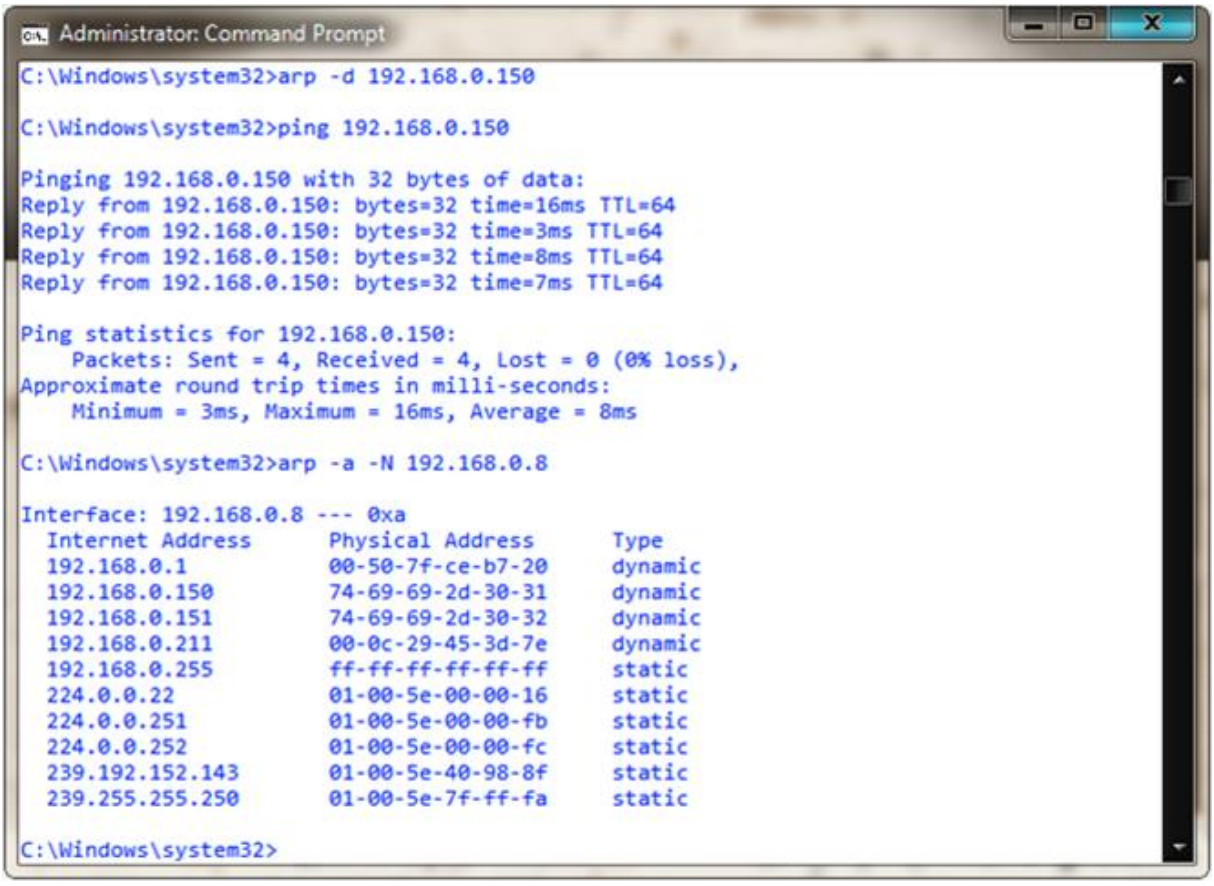

Figura 15 – Eliminação de entradas na tabela de ARP

O único entrave a esta solução, é o facto que, se a máquina já estiver a comunicar com o destino em questão na altura da redefinição, não se consegue apagar a associação dinâmica para introduzir uma estática em tempo útil.

2.4 Utilização da «Área de transferência»

A «Área de transferência» é uma zona da memória RAM (*Random Access Memory*) que é independente de cada utilizador. Quando a ideia é copiar determinado tipo de informação, quer esteja em ficheiro, quer esteja alojado na internet ou em qualquer outro local, a capacidade de «copiar» e «colar» é muito útil. Estas duas ações tiram partido da «Área de transferência». Infelizmente para o caso, não é possível desativar esta zona especial da memória do sistema operativo Windows e terá de se recorrer à criatividade para conseguir impedir a sua utilização

ou inutilizar[11] [14] o seu conteúdo. Existem algumas aplicações que conseguem restringir o acesso a esta área impedindo a opção de copiar, colar e recortar entre outras. A aplicação nomeada de «Prevent»[12] [15], concebida por Ritesh Kawadkar, aparenta conseguir, desabilitar as funções de copiar, colar, recortar e eliminar, entre outras. Ela fá-lo de uma forma mista, pois consegue efetivamente desabilitar as funções copiar e recortar do próprio sistema operativo, mas não das suas aplicações. As aplicações, p. ex. «WordPad», têm estas funções ativas, mas logo após a sua utilização, a aplicação que está a correr em *background* limpa de imediato a «Área de transferência». A Figura 16 retrata a interface gráfica da aplicação.

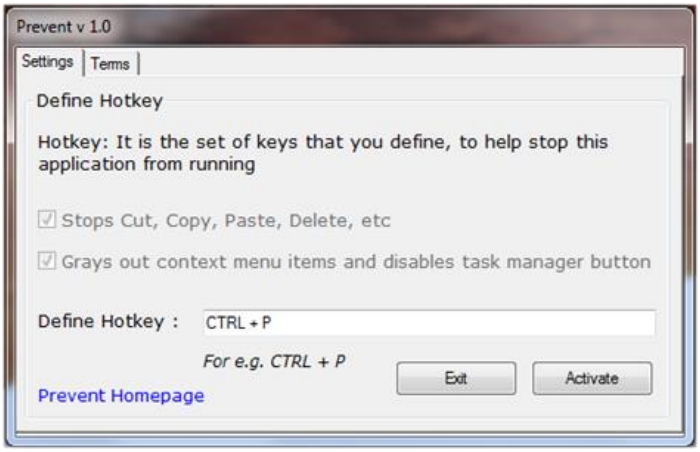

Figura 16 – A Aplicação «Prevent»

Em alternativa à utilização de aplicações específicas, prende-se a possibilidade de remapear as teclas do teclado, alterar-lhes as suas funções ou, simplesmente, desativá-las. Um teclado simples é um dispositivo de 'entrada', onde, a cada tecla e a cada combinação de teclas, é atribuída um «scancode»[13] [16]. Este «scancode» não passa de um código de 16-bit com o qual o sistema consegue determinar qual ou quais as teclas que foram carregadas. A chave «Scancode Map», do tipo «REG_BINARY», que pode ser acrescentada à *hive* «HKLM\SYSTEM\CurrentControlSet\Control\Keyboard Layout» do *Registry* do Windows[14] [17], é composta pelo mínimo de 5 grupos de 4 *bytes* cada, conforme apresentado na Figura 17.

[11] https://www.makeuseof.com/tag/5-tips-manage-windows-clipboard-like-pro/
[12] http://madgeektools.blogspot.com/2018/05/prevent-v-10-restrict-cut-copy-paste.html
[13] https://docs.microsoft.com/en-us/previous-versions/visualstudio/visual-studio-6.0/aa299374(v=vs.60)
[14] https://www.experts-exchange.com/articles/2155/Keyboard-Remapping-CAPSLOCK-to-Ctrl-and-Beyond.html

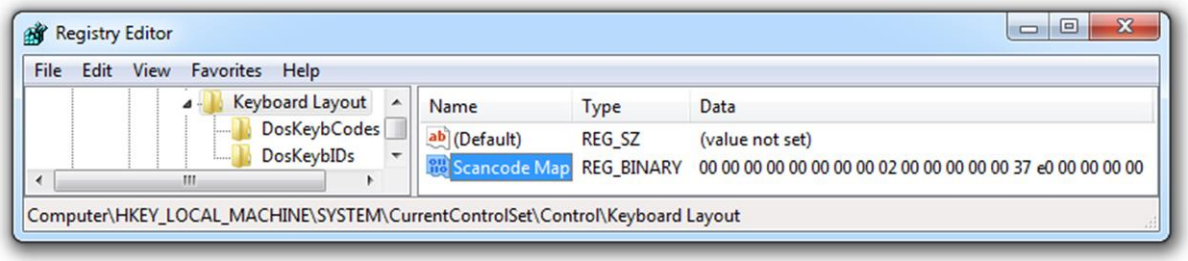

Figura 17 – Chave «Scancode Map» no *Registry* do Windows

O primeiro e segundo grupos indicam, respetivamente, a versão e as *flags* do cabeçalho, o terceiro indica o número de entradas onde é incluído o «NULL terminator» localizado no último grupo e que é todo composto por '0'. Os restantes grupos indicam o mapeamento entre o código de execução e a tecla. Por outro lado, existem algumas aplicações no mercado que tiram partido desta funcionalidade para permitir aos utilizadores alterar a posição das teclas. A Figura 18 dá exemplo de uma dessas aplicações, o «KeyTweak».

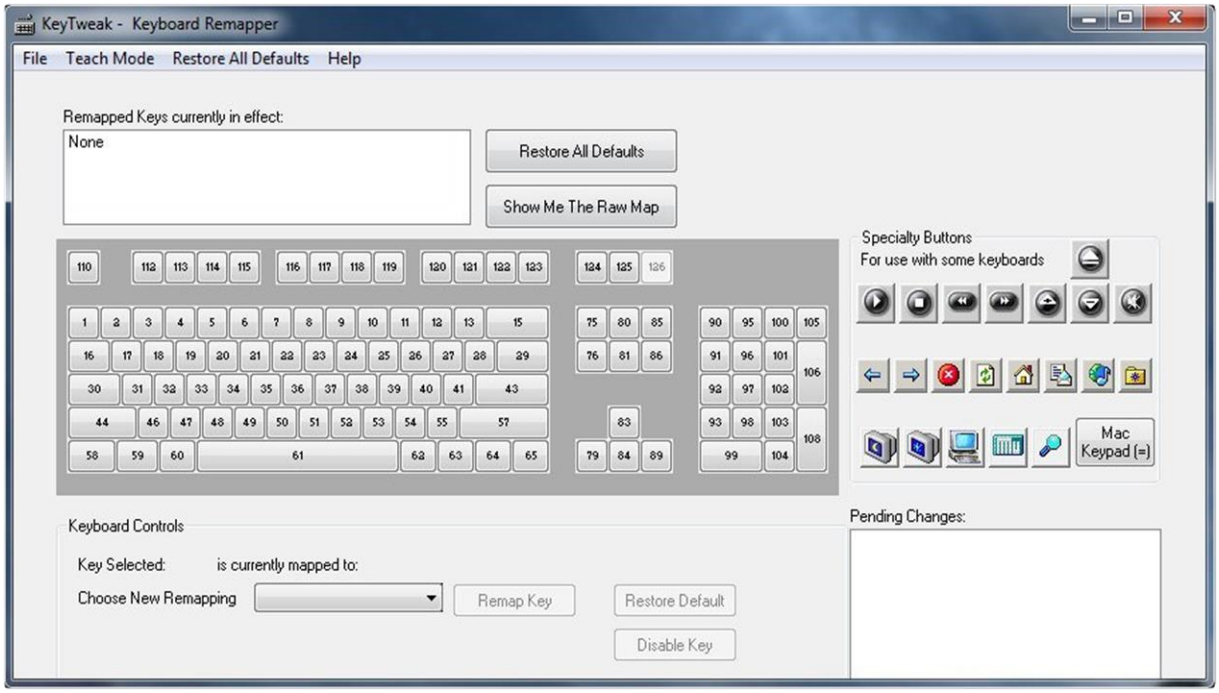

Figura 18 – O utilitário «KeyTweak»

Infelizmente com esta abordagem, é necessário reiniciar o computador, pois só dessa forma se consegue reiniciar o controlador do teclado para que as alterações possam surtir efeito. Existem algumas outras aplicações capazes de remapear as teclas, mas requerem que estejam em execução para que possa ser observado o seu efeito. A própria Microsoft tem um utilitário que permite a criação de disposições de teclados denominada de «Microsoft Keyboard Layout Creator».

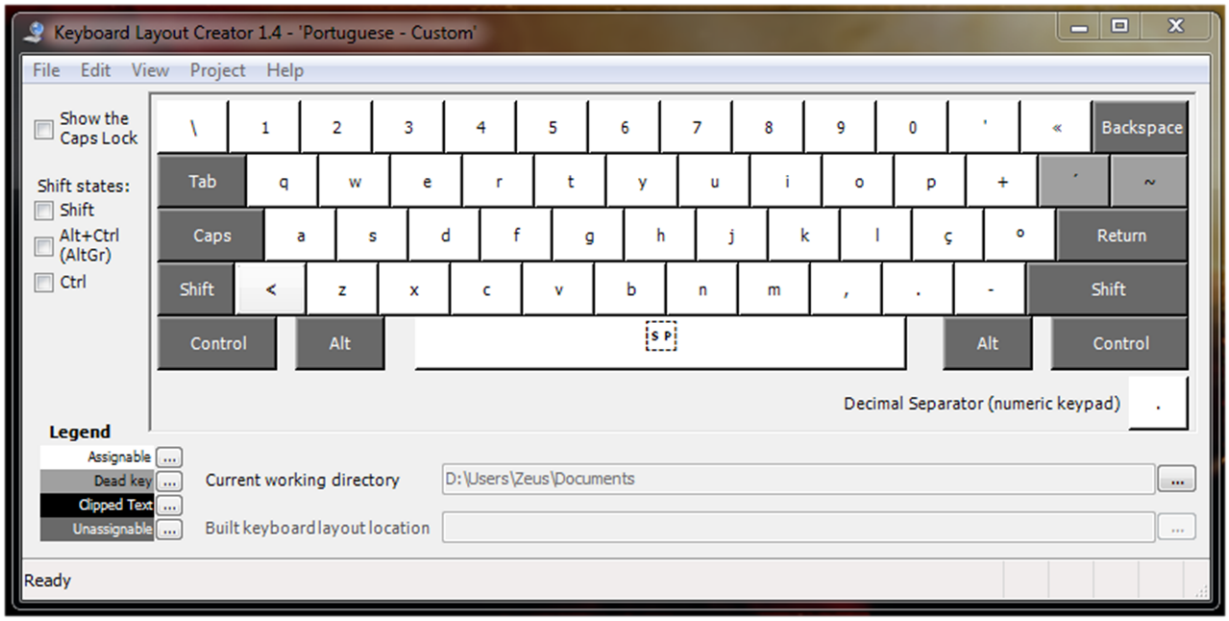

Figura 19 – Microsoft Keyboard Layout Creator 1.4

Esta aplicação, além de permitir remapear as teclas, permite também atribuir uma sequência de caracteres a uma só tecla, no entanto, não permite afetar todas as teclas existentes no teclado. As teclas apresentadas a cinzento escuro, conforme se pode visualizar na Figura 19, não podem ser remapeadas.

2.5 Utilização de programas pré-definidos

A utilização de certas aplicações pode comprometer a tarefa em mãos, felizmente existem algumas formas de combater esta situação. Ao utilizar o editor de «Políticas de Computador Local» (gpedit.msc) para aceder à configuração do «AppLocker», pode definir-se quais os ficheiros que serão permitidos executar. A Figura 20 mostra onde se pode aceder à configuração desta funcionalidade.

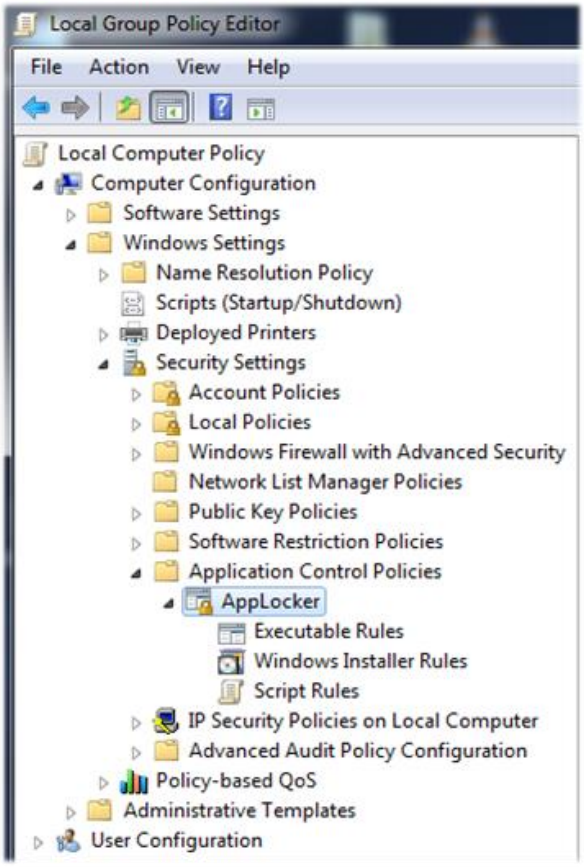

Figura 20 – Política de Computador Local «AppLocker»

Também é possível impedir o acesso a determinados ficheiros[15] [18] através da manipulação do *Registry*. Terá de se acrescentar uma chave com o nome de «Explorer» dentro de «HKCU\Software\Microsoft\Windows\CurrentVersion\Policies», e dentro dessa chave terá ainda de se acrescentar um registo designado de «DisallowRun» e atribuir-lhe o valor «1» conforme se pode observar na Figura 21.

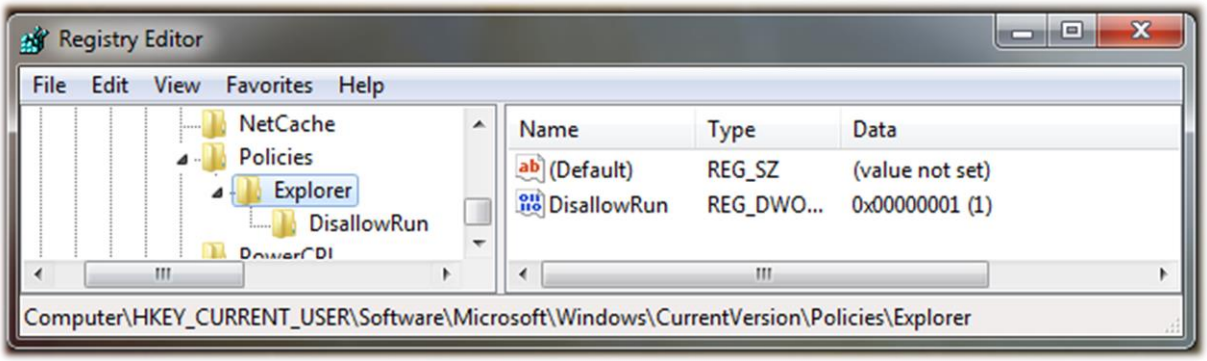

Figura 21 – Atribuição de políticas ao «Explorer» via *Registry*

[15] https://www.howtogeek.com/howto/8739/restrict-users-to-run-only-specified-programs-in-windows-7/

Dentro da chave «Explorer» terá de se criar uma outra chave, também ela chamada de «DisallowRun». Uma vez criada esta estrutura, é só indicar qual ou quais as aplicações que se querem bloquear. Esta indicação é feita com registos sequenciais, começando no número «1», conforme se pode visualizar na Figura 22. O valor deste registo é o nome completo do ficheiro executável da aplicação que se quer bloquear.

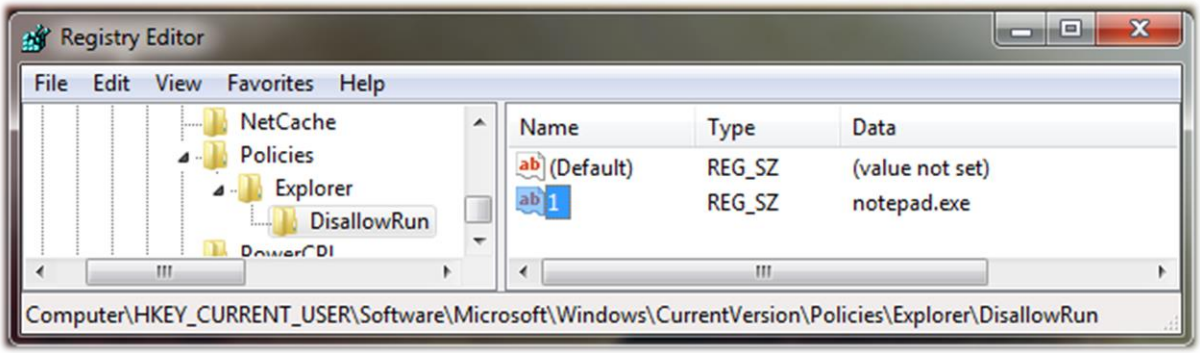

Figura 22 – Bloquear aplicação via *Registry*

Quando se tentar arrancar com uma aplicação que foi definida como bloqueada por este meio, o sistema impede de imediato o seu funcionamento, apresentando a mensagem que nos indica a Figura 23. A inclusão ou alteração destes registos surte imediatamente efeito, não sendo necessário reiniciar o computador, nem a sessão do utilizador.

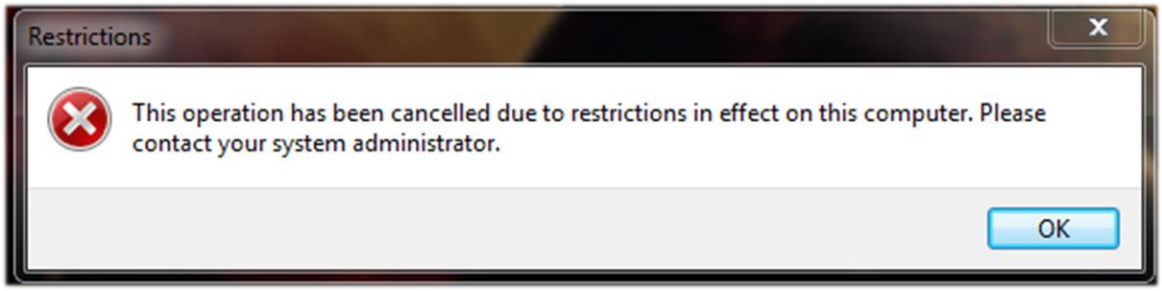

Figura 23 – Mensagem do sistema «Aplicação bloqueada»

Semelhantemente a esta forma, é possível fazer o inverso e apenas permitir a execução de ficheiros executáveis previamente definidos. Para esta ação, é necessário criar um registo designado de «RestrictRun» e atribuir-lhe o valor «1». É também necessário criar uma chave com o mesmo nome, à semelhança de como é feito para o «DisallowRun». Após criar estas duas entradas e identificar os executáveis, é necessário reiniciar a sessão do utilizador para que as alterações surtam efeito. É importante reter que, visto esta alteração surtir efeito no utilizador da sessão ativa, é necessário acrescentar o «regedit.exe» como um dos executáveis autorizados, pois caso contrário, não conseguirá reverter a situação.

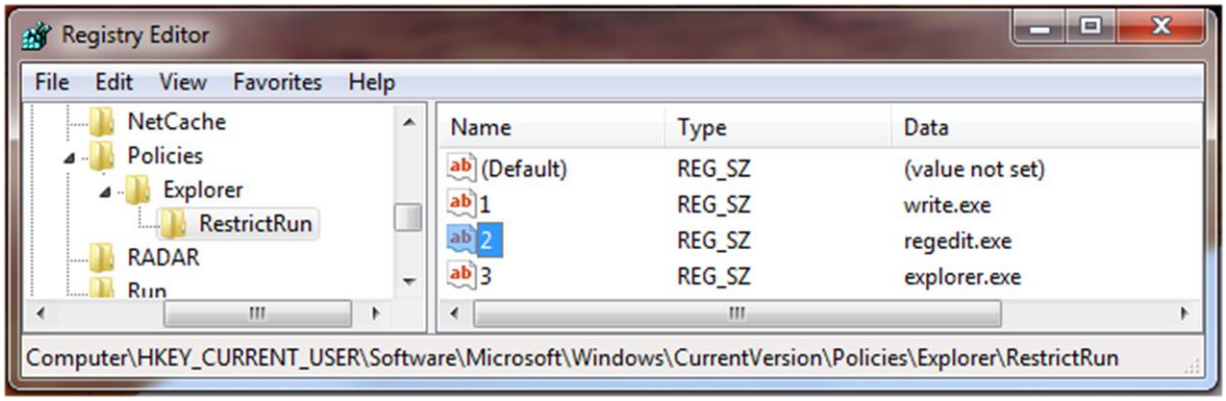

Figura 24 – Autorizar aplicação via *Registry*

A Figura 24 exemplifica o que é necessário para permitir definir quais os executáveis que poderão ser executados.

Existem alguns utilitários que conseguem impedir que sejam executados os ficheiros de outras aplicações e temos como exemplo o «Smart Windows App Blocker»[16] [19]. A Figura 25 apresenta a interface desta aplicação.

Figura 25 – Smart Windows App Blocker

Tanto quanto foi possível pesquisar, não existe nenhum utilitário que faça o inverso, ou seja, que bloqueie todas as aplicações, à exceção das que forem expressamente definidas.

[16] https://smart-windows-app-blocker.en.softonic.com/

2.6 Administração remota

O que no passado era impossível, presentemente, tirando partido de ligações dedicadas ou da internet, uma sede de empresa pode estar ligada a um escritório do outro lado do globo. Com esta realidade, a administração dos sistemas está de certa forma facilitada. Uma pequena equipa de administradores pode gerir uma infraestrutura enorme tirando partido de ferramentas de administração remota. Existem várias ferramentas, no entanto, há um pacote intitulado de «PsTools»[17] que contém ferramentas concebidas por Mark Russinovich para a Sysinternals, uma subsidiária da corporação Microsoft, que é bastante útil. A ferramenta intitulada de «PsExec»[18] que pertencente ao referido pacote é capaz de criar e executar processos noutras máquinas mesmo que estas não pertençam ao mesmo domínio.

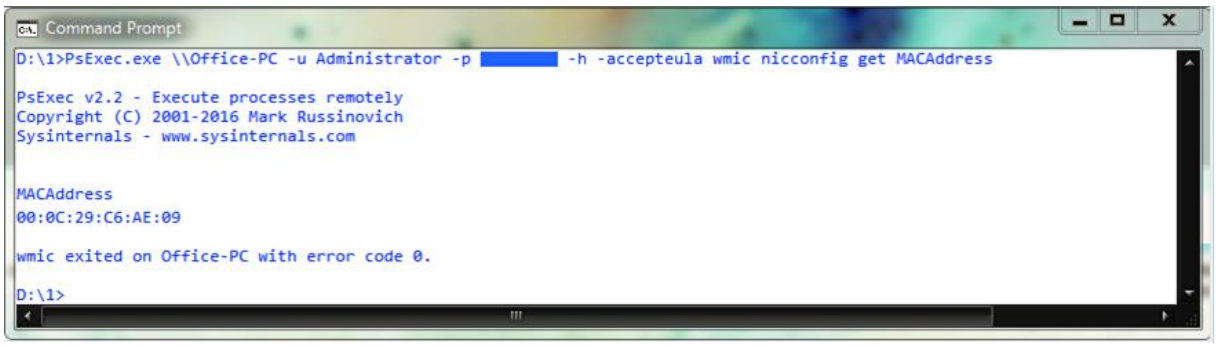

Figura 26 – Exemplo de utilização da ferramenta «PsExec»

A Figura 26 mostra como, neste exemplo é possível obter com alguma facilidade o endereço «MAC-ADDRESS» de uma máquina remota que não é sequer membro do mesmo domínio. O acesso é possível graças ao facto de a ferramenta permitir o fornecimento e utilização de credenciais através da inclusão das opções «-u» e «-p» na sua chamada. Esta ferramenta é gratuita e tem muito poucas restrições no que diz respeito à sua utilização, o que juntamente com o variado leque de opções, faz dela uma das melhores amigas de um administrador audaz. Segundo alguns autores[19], tem, no entanto, uma vulnerabilidade que se presencia ao transmitir as credenciais em claro. Para averiguar da visibilidade das credenciais aquando da transmissão, foram capturados sequências de pacotes de rede. Nos referidos pacotes não foram identificadas credenciais de acesso, pelo que se levanta a hipótese que a captura de credenciais de acesso não seja trivial.

[17] https://docs.microsoft.com/en-us/sysinternals/downloads/pstools
[18] https://docs.microsoft.com/en-us/sysinternals/downloads/psexec
[19] https://www.itprotoday.com/compute-engines/psexec

O protocolo *Wake-On-LAN*[20] (WOL), desenvolvido pela «Advanced Micro Devices (AMD)» e pela «Hewlett Packard (HP)», possibilita ligar uma máquina remotamente desde que a interface de rede e a máquina alvo disponham dessa funcionalidade. Havendo esta possibilidade, p. ex., a atualização das máquinas pode ser agendada para períodos nos quais estas se encontrem desligadas. No entanto, existe uma restrição que é imposta pelo facto deste protocolo utilizar um pacote do tipo *broadcast* para chegar ao equipamento pretendido. Como os *broadcast* não transitam de rede para rede, obriga a que a máquina originadora do pedido e a máquina alvo estejam na mesma rede ou em alternativa, que haja um servidor «*SleepServer*» na mesma rede da máquina alvo que execute o pedido. Existe ainda roteadores capazes de distinguir estes pacotes dos restantes, encaminhando-os para o destino correto, mas nem todos suportam esta funcionalidade. A capacidade de ligar máquinas em redes distintas não deve ser confundido com a utilização de «*port-forwarding*» disponível na maioria dos roteadores domésticos.

2.7 Síntese

Em suma, o mercado presentemente apresenta a maioria das ferramentas necessárias ao cumprimento dos objetivos propostos neste trabalho. Porém, algumas destas ferramentas não são computacionalmente integráveis, não possuem licenças que o permitam ou exigem que haja um *daemon* a correr em permanência, o que vai contra a natureza e os princípios dos objetivos do trabalho.

[20] https://wiki.wireshark.org/WakeOnLAN

Capítulo 3 – Descrição da Solução

Neste capítulo pretende dar-se a conhecer todos os aspetos que levam à conceção do *software* designado de «PC Border», desde as necessidades dos utilizadores, até às exigências impostas pela tecnologia utilizada.

3.1 Enquadramento

Em muitos casos, as entidades deparam-se com dificuldades a nível intelectual, financeiro e tecnológico no cumprimento da sua missão. Em casos raros, o problema é de natureza burocrática, onde a cadeia hierárquica não apoia adequadamente as necessidades dos departamentos de um nível inferior. Neste caso e numa infraestrutura a operar em ambiente Microsoft Windows, as políticas de domínio da *Active Directory* (AD), que são geridas por um departamento em posição mais elevada, poderão não ser as adequadas aos departamentos de formação, especialmente se estes forem bastante dinâmicos e se houver falta de mão-de-obra. Assim, implica que a solução a conceber, seja capaz de operar sem recorrer a configurações de políticas de AD e, até mesmo, em máquinas que não pertençam a qualquer domínio AD.

As dificuldades financeiras podem, por outro lado, ditar que as máquinas existentes devam ser utilizadas o máximo tempo possível, adiando a aquisição de novos equipamentos. Este caso, juntamente com o facto de que a Microsoft está a garantir um suporte aos seus sistemas operativos por períodos muito curtos[21], força a que os sistemas sejam atualizados para a versão mais recente, o que requer que a solução apresentada seja o mais leve possível para as máquinas. Posto isto, é de evitar ao máximo a execução de código nestas máquinas, o que põe de parte a utilização de *daemons*, ou seja, a instalação e execução permanente de software.

Na conceção de qualquer *software*, há que ter em atenção a interação com as pessoas. A interface deve ser «*user-friendly*», ou por outras palavras, amiga do utilizador. Deve ser bastante intuitiva e para além de possuir uma combinação de cores atrativa, deve possibilitar a sua utilização por pessoas daltónicas. Este aspeto torna-se mais evidente quando se trata de

[21] https://support.microsoft.com/en-ca/help/13853/windows-lifecycle-fact-sheet

pessoas com alguma idade, ou com pouca apetência para assuntos do foro tecnológico, especialmente quando o tempo disponível é um fator importante. Em suma, a solução apresentada deve ser bastante fácil de interpretar e simples de utilizar.

As salas de aulas equipadas para utilização de meios informáticos, podem ser diversas e encontrarem-se em locais distantes, o que eventualmente torna o acesso físico a estes equipamentos pouco eficaz para a pessoa responsável pela avaliação a decorrer. Esta realidade, com o facto de as máquinas no arranque demorarem o seu tempo a libertar os recursos necessários para a tarefa a executar, faz com que seja boa ideia possuir uma forma prática e rápida de ligar estes equipamentos. Um cenário onde se torna evidente esta capacidade é, por exemplo, a existência de duas salas de aulas localizadas em edifícios diferentes e que serão palco para a avaliação de uma determinada disciplina. Isto, juntamente com o facto de haver falta de mão de obra, facilita bastante o responsável por ter as máquinas prontas à hora programada, especialmente se a avaliação for logo ao primeiro tempo da manhã, ou se este responsável tenha ainda outras tarefas com que se preocupar.

3.2 Análise de Requisitos

Este tópico é composto por três partes, «Requisitos de Utilizador», «Requisitos de Sistema» e por uma análise de importância dos requisitos.

Em «Requisitos do Utilizador» são transcritas as necessidades dos utilizadores, ou seja, os responsáveis pelas avaliações, e o que esperam do *software* a ser criado.

Em «Requisitos do Sistema» são detalhados todos os aspetos funcionais que o *software* a conceber deve observar

3.2.1 Requisitos de Utilizador

a) O *software* deve bloquear todos os acessos a dados de e para os computadores dos formandos a serem avaliados, especialmente na utilização de *pens* USB.
b) O *software* deve bloquear a utilização de aplicações não autorizadas.
c) O *software* deve bloquear a utilização da *web*, à exceção dos sites autorizados.
d) O *software* deve estar disponível em português, francês e inglês.
e) O *software* deve ser de utilização simples e intuitiva.
f) O *software* só deve poder ser utilizado pelos docentes.
g) O *software* deve funcionar em sistema operativo Microsoft Windows 7 e posterior.

3.2.2 Requisitos do Sistema

i) O sistema deve ser versátil e adaptável às alterações.
ii) O sistema deve conter uma conta de administração incorporada que não seja possível eliminar.
iii) O sistema deve permitir alterar a senha da conta de administrador incorporada.
iv) O sistema deve permitir autenticação por contas locais ou de domínio AD.
v) Ao iniciar a aplicação, o sistema deve autenticar o utilizador, reconhecendo se é administrador ou docente.
vi) Ao guardar as configurações, o sistema deve cifrar os dados antes de os escrever em ficheiro.
vii) O sistema deve guardar os dados em ficheiro próprio e no mesmo diretório onde se encontra a aplicação.
viii) O sistema deve guardar um registo dos acessos a sessões efetuados na aplicação.
ix) A componente gráfica deve apresentar uma disposição linear dos componentes de forma a facilitar a perceção de utilização ao docente.
x) O sistema deve incluir uma forma para facilmente mudar a língua de apresentação.
xi) O sistema deve ser capaz de impedir que seja retirada ou introduzida informação no computador do formando quer através da rede, quer através de dispositivos de armazenamento externo ou ainda através do próprio computador.
xii) O sistema deve bloquear a execução de aplicações não autorizadas.
xiii) O sistema deve permitir a configuração de acessos de informação autorizados.
xiv) O sistema deve permitir a configuração de equipamentos de armazenamento externo autorizados.
xv) O sistema deve permitir configurar os diversos tipos de bloqueio.
xvi) O sistema deve permitir ao docente escolher quais os tipos de bloqueio que pretende utilizar.
xvii) O sistema deve conseguir repor as configurações originais do computador do formando uma vez terminada a ação de bloqueio.
xviii) O sistema deve ter a capacidade de funcionar em redes que operam com o protocolo IPv6.
xix) O sistema não deve operar com *daemons*.

Os requisitos mencionados têm importâncias diferentes no que diz respeito à implementação. Assim sendo, a Tabela 2 indica-nos o grau de importância e uma breve descrição de cada um dos requisitos.

Tabela 2 – Grau de importância e descrição dos requisitos

REQUISITO	DESCRIÇÃO	IMPORTÂNCIA
i)	A versatilidade exige não necessitar de instalação prévia	Média
ii)	Uma conta incorporada de administração garante o contínuo funcionamento da aplicação	Média
iii)	A conta incorporada de administrador é pré-definida. A impossibilidade de a alterar pode ser uma quebra de segurança	Média
iv)	Utilização de contas de domínio AD Utilização de contas locais	Alta Média
v)	Permitir apenas a utilização por docentes ou administradores	Alta
vi)	A cifragem de dados é fulcral pois entre outras estão as configurações e credenciais de acesso	Alta
vii)	O sistema deve ser independente e não depender de sistemas externos	Alta
viii)	O registo de acessos permite saber se houve tentativas de acesso não-autorizado ao sistema	Baixa
ix)	O sistema deve permitir, através de senso comum, a rápida familiarização de utilizadores novatos	Alta
x)	Alteração da língua de apresentação. Alguma da formação é dada por docentes estrangeiros	Média
xi)	A razão de existência do software	Alta
xii)	A utilização de aplicações diversas pode ser uma falha grave	Alta
xiii)	A utilização de plataformas de Ensino à Distância é uma realidade	Alta
xiv)	Bloqueio seletivo de equipamentos de armazenamento externo. É uma comodidade, não uma necessidade	Baixa
xv)	As avaliações têm naturezas diferentes, logo as configurações de controlo são forçosamente diferentes	Alta
xvi)	Independência na utilização da aplicação	Alta
xvii)	O sistema não deve deixar pegada digital permitindo o correto funcionamento do PC no futuro	Alta
xviii)	A possibilidade de operar sobre IPv6 é uma previsão para um futuro distante, não uma necessidade imediata	Baixa
xix)	A não utilização de código de execução permanente, poupa recursos ao sistema	Média

3.3 Pressupostos

Um formando desesperado pode tomar a iniciativa de utilizar os portos USB da máquina utilizada na execução do seu teste de avaliação, com o intuito de copiar o teste ou como meio para obtenção de informação não autorizada. A capacidade de bloquear todos os dispositivos de armazenamento externo que utilizam os portos USB de uma tal máquina é uma solução inicial, no entanto e devido a eventuais conhecimentos reduzidos do avaliador, pode ser necessário que este tenha a capacidade de ligar o seu próprio dispositivo de armazenamento externo para, p. ex., recolher os testes efetuados. Num tal cenário onde os portos USB estivessem bloqueados, o formador encontrar-se-ia impossibilitado de recolher os referidos testes sem que para tal desbloqueasse a máquina em questão. Será então uma mais-valia executar o bloqueio seletivo dos equipamentos, tendo como base o seu número de série. Para possibilitar esta funcionalidade, terá de se recorrer a um registo ou base de dados onde estejam identificados os dispositivos que estão autorizados a funcionar mesmo em condições de bloqueio. É, pois, assim necessário incluir o bloqueio seletivo dos dispositivos USB na conceção do *software*.

O bloqueio dos portos USB durante uma prova, por si só não resolve o problema que se propõe solucionar, pois se a máquina utilizada para a avaliação for a mesma que é utilizada na formação, abre portas para que o formando possa executar a ação fraudulenta de forma diferida. O formando pode precaver-se e colocar «o material» objeto de fraude na máquina antes do momento de avaliação, ou pode até guardar o teste na própria máquina e retirá-lo numa próxima oportunidade.

Uma forma alternativa de retirar ou colocar informação numa máquina pode passar pela utilização da rede, quer seja tirando partido de um *fileshare*, quer de um serviço de *webmail*, quer ainda de outras formas variadas. Perante este facto, torna-se também necessário controlar os acessos efetuados pela rede.

É sempre boa ideia optar por ser proativo em vez de reativo, e no que diz respeito à seleção da informação que se quer retirar, é preferível impedir a utilização da «Área de transferência» do sistema operativo e assim impossibilitar a extração de certo tipo de informação, sendo um importante primeiro passo antes de impedir a sua transferência para outro local de armazenamento.

Uma pessoa suficientemente motivada e com alguma criatividade pode conseguir aquilo que ainda não foi previsto e, neste sentido, é preferível permitir a execução de apenas os executáveis estritamente necessários para o bom funcionamento do sistema operativo, bem como, para a execução da tarefa em mãos.

3.4 Casos de Uso (*Use Cases*)

Os «Casos de uso» são uma forma de definir por escrito toda a interação que um utilizador terá com determinado *software* que se pretende construir. Descreve todos os passos possíveis na utilização desse *software*, incluindo os caminhos principais e secundários. São esboços que servirão como ponto de partida para a criação do *software*. A aplicação será concebida observando os seguintes casos de uso:

- Definir a língua da Interface.
- Carregar uma lista de PCs – Um agrupamento de computadores destinados a receber a mesma configuração.
- Criar lista de PCs.
- Eliminar lista de PCs.
- Adicionar PCs a uma lista.
- Remover PCs de uma lista.
- Editar definições de PC – Definir funcionamento sobre Domínio de AD ou Grupo de Trabalho com respetivas credenciais de administração.
- Ligar os PCs da lista ativa – Nos PCs com esta capacidade, utiliza o protocolo WOL para ligar um computador que se encontra encerrado ou suspenso.
- Desligar os PCs da lista ativa.
- Entrar na administração da aplicação.
- Alterar a senha de administração embutida.
- Definir a conta de serviço do domínio.
- Definir a conta local de serviço.
- Adicionar conta aos administradores.
- Remover conta dos administradores.
- Adicionar conta aos utilizadores.
- Remover conta aos utilizadores.

- Definir o endereço de rede a utilizar.
- Definir controlos de endereços e programas.
- Definir controlos de dispositivos.
- Definir controlos de contas de avaliação.
- Configurar o bloqueio de computadores.
- Executar o bloqueio dos computadores.
- Executar o desbloqueio dos computadores.
- Verificar estado de um computador.
- Visualizar os registos do sistema.
- Exportar os registos do sistema.

A Figura 27 representa o esboço da janela principal da aplicação «PC Border» identificando a sua constituição. É a partir desta janela que todas as ações e configurações serão executadas. A disposição dos componentes constituintes da aplicação será de tal forma a transmitir intuição acerca do funcionamento da própria aplicação.

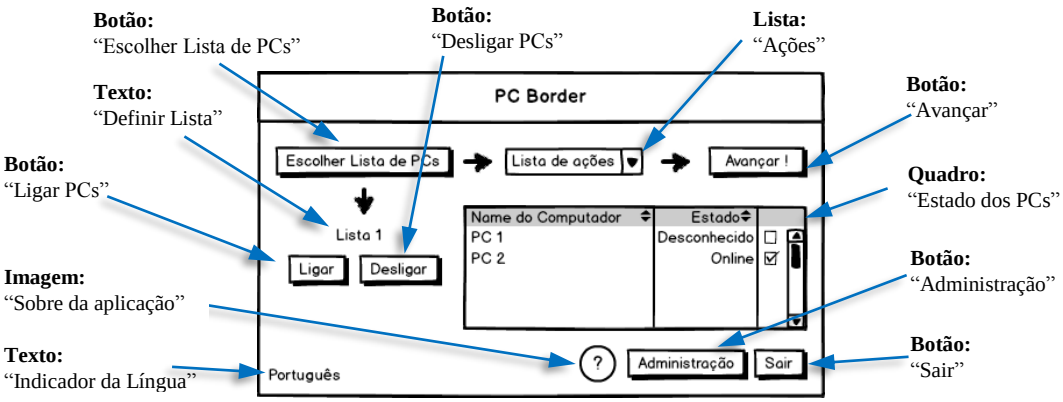

Figura 27 – Esboço da janela principal da aplicação «PC Border»

3.4.1 Escolher a língua da Interface

A Figura 28 representa o esboço da janela «Selecionar Língua». Uma vez alterada a língua de apresentação, todas as janelas passarão a utilizar esta nova língua. O sistema guardará esta configuração de forma que seja mantida da próxima vez que a aplicação for utilizada.

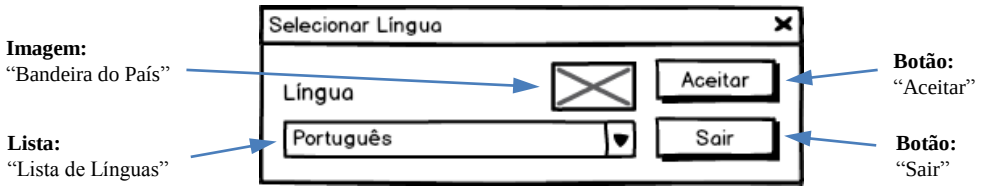

Figura 28 – Esboço da janela «Selecionar Língua»

Caminho principal:

1- O utilizador carrega no texto indicativo da língua atual presente na janela principal.
2- O sistema carrega a lista de línguas e apresenta a janela «Selecionar Língua».
3- O utilizador seleciona uma das línguas presentes na «Lista de Línguas».
4- O sistema altera a língua da janela «Selecionar Línguas» para a língua escolhida.
5- O utilizador aceita a língua selecionada carregando em «Aceitar».
6- O sistema guarda a língua selecionada, fecha a janela «Selecionar Língua», volta para e altera a língua da janela principal e passa a apresentar as novas janelas na língua selecionada.

Caminho alternativo:

3.1- O utilizador mantém a língua.
3.1.1- O utilizador carrega em «Aceitar».
3.1.2- O sistema continua no ponto 6.
3.2- O utilizador cancela a operação.
3.2.1- O utilizador carrega em «Sair».
3.2.2- O sistema fecha a janela «Selecionar Língua» e volta para a janela principal.
5.1- O utilizador cancela a operação – continua em 3.2.1.

3.4.2 Carregar uma lista de PCs

A Figura 29 retrata o esboço da janela «Gerir lista de PCs». É nesta janela que serão feitas todas as configurações relativas às listas de PCs. Uma lista de PCs é uma agregação de computadores afetos a avaliações que serão utilizados numa determinada avaliação. Pode ou não ser coincidente com as máquinas existentes numa sala de aulas.

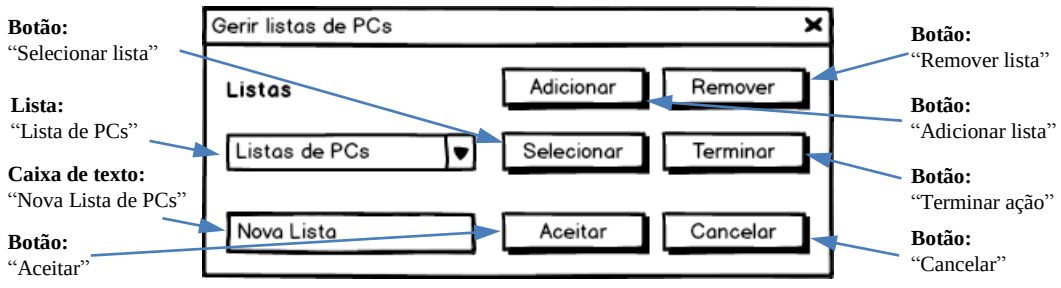

Figura 29 – Esboço da janela «Gerir lista de PCs»

Caminho principal:

1- O utilizador carrega no botão «Escolher lista de PCs» presente na janela principal.
2- O sistema carrega as listas de PCs e apresenta a janela «Gerir listas de PCs» e ativa os botões «Editar» e «Remover» caso a lista não esteja vazia.
3- O utilizador escolhe uma das listas disponíveis na lista «Listas de PCs».
4- O utilizador carrega em «Selecionar» na janela «Gerir listas de PCs».
5- O sistema guarda a informação da lista selecionada, fecha a janela «Gerir listas de PCs», volta para a janela principal, apresenta os botões de «Ligar» e «Desligar» dos PCs, apresenta o nome dos PCs da lista no quadro «Estado dos PCs», inicia o processo de contacto com os PCs e vai atualizando-o à medida que vai obtendo resposta.

Caminho alternativo:

3.1- O utilizador cancela a operação.
3.1.1- O utilizador carrega em «Terminar» na janela «Gerir listas de PCs».
3.1.2- O sistema fecha a janela «Gerir listas de PCs», volta para a janela principal e termina as tarefas relativas à lista anteriormente ativa.
3.2- O utilizador adiciona uma nova lista – *Caso de uso «Criar lista de PCs»*.
4.1- O utilizador remove a lista selecionada – *Caso de uso «Eliminar lista de PCs»*.

3.4.3 Criar lista de PCs

Caminho principal:

1- O utilizador carrega no botão «Adicionar» na janela «Gerir listas de PCs».
2- O sistema estende a janela «Gerir listas de PCs» apresentando a caixa de texto «Nova lista de PCs» e os botões «Aceitar» e «Cancelar» e desativa o botão «Adicionar».
3- O utilizador define o nome da nova lista.
4- O sistema valida o nome ativando o botão «Aceitar» caso o nome não seja nulo.
5- O utilizador aceita o nome para a nova lista carregando em «Aceitar».
6- O sistema cria uma lista nova no ficheiro de registo, coloca a seleção na lista acabada de criar, ativa o botão «Adicionar» e encolhe a janela «Gerir listas de PCs» ao seu tamanho original desativando a caixa de texto «Nova lista» e os botões «Aceitar» e «Terminar».

Caminho alternativo:

3.1- O utilizador cancela a operação.

3.1.1- O utilizador carrega no botão «Cancelar».

3.1.2- O sistema ativa o botão «Adicionar» e encolhe a janela «Gerir listas de PCs» ao seu tamanho original.

3.2- O utilizador termina a operação.

3.2.1- O utilizador carrega no botão «Terminar».

3.2.2- O sistema fecha a janela «Gerir listas de PCs», volta para a janela principal e termina as tarefas relativas à lista anteriormente ativa.

3.3- O utilizador remove a lista selecionada – *Caso de uso «Eliminar lista de PCs»*.

6.1- Ocorre um erro ao criar a lista.

6.1.1- O sistema apresenta uma mensagem indicando que ocorreu um erro.

6.1.2- O utilizador carrega em «OK».

6.1.3- O sistema fecha a mensagem e continua no ponto 3.

3.4.4 Eliminar lista de PCs

Caminho principal:

1. O utilizador escolhe a lista da lista «Listas de PCs» na janela «Gerir listas de PCs» e carrega no botão «Remover».
2. O sistema apresenta uma caixa de diálogo questionando o utilizador se pretende mesmo eliminar a lista selecionada.
3. O utilizador confirma carregando em «Sim».
4. O sistema fecha a caixa de diálogo, remove a lista do ficheiro de registos e volta para a janela «Gerir listas de PCs».

Caminho alternativo:

3.1- O utilizador cancela a operação

3.1.1- O utilizador aborta a operação carregando em «Não»

3.1.2- O sistema fecha a caixa de diálogo e volta para a janela «Gerir listas de PCs».

3.4.5 Adicionar PCs a uma lista

A Figura 30 retrata o esboço da janela «Gerir Computadores». É nesta janela que serão feitas todas as configurações dos PCs afetos às listas de PCs. Sempre que se adicionar um PC a uma

lista terá de se identificar qual as credenciais que serão usadas cada vez que a aplicação necessitar comunicar com a esse PC.

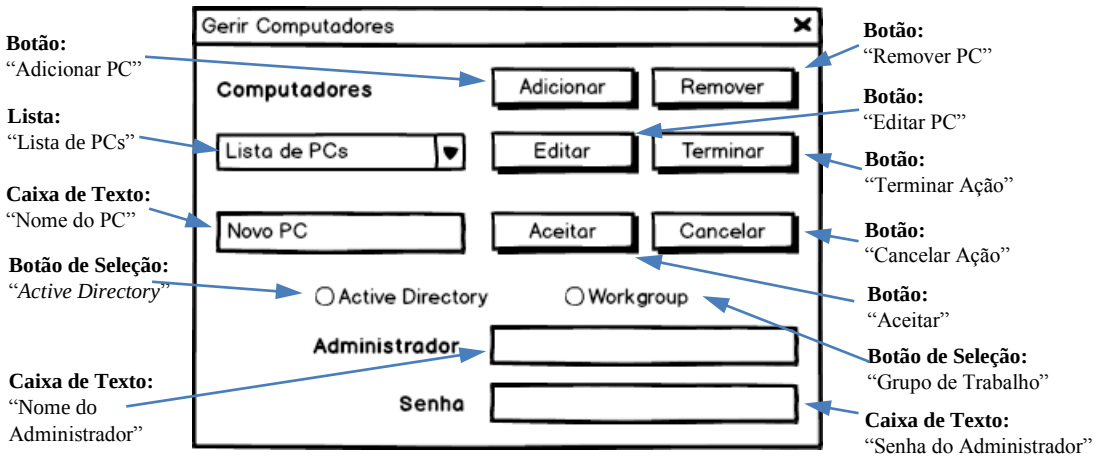

Figura 30 – Esboço da Janela «Gerir Computadores»

Caminho principal:

1. O utilizador carrega no texto indicativo da lista ativa designado de «Definir Lista» que se encontra visível na janela principal da aplicação após o utilizador ter carregado uma lista de PCs.
2. O sistema carrega a lista de PCs, apresenta a janela «Gerir Computadores» e ativa os botões «Editar PC» e «Remover PC» caso a lista não esteja vazia.
3. O utilizador carrega no botão «Adicionar PC».
4. O sistema expande a janela «Gerir Computadores» apresentando a caixa de texto «Nome do PC», os botões «Aceitar» e «Cancelar», os botões de seleção «*Active Directory*» e «Grupo de Trabalho», as caixas de texto «Nome do Administrador» e «Senha do Administrador» e desativa o botão «Adicionar PC».
5. O utilizador introduz o nome do computador a adicionar na caixa de texto «Nome do PC» e carrega no botão de seleção «*Active Directory*».
6. O sistema ativa o botão «Aceitar».
7. O utilizador carrega no botão «Aceitar».
8. O sistema acrescenta o nome do computador à lista de computadores ativa, cifra os dados guardando-os em ficheiro e comprime a janela «Gerir Computadores» ao seu tamanho original.
9. O utilizador carrega em «Terminar Ação».

Caminho alternativo:

3.1- O utilizador termina a operação.

3.1.1- O utilizador carrega no botão «Terminar Ação».

3.1.2- O sistema fecha a janela «Gerir Computadores» e volta à janela principal da aplicação.

5.1- O utilizador cancela a operação.

5.1.1- O utilizador carrega no botão «Cancelar».

5.1.2- O sistema reduz o tamanho da janela «Gerir Computadores» ao tamanho original.

5.2- O utilizador define que o computador é membro de um Grupo de Trabalho.

5.2.1- O utilizador carrega no botão de seleção «Grupo de Trabalho».

5.2.2- O sistema ativa as caixas de texto «Nome do Administrador» e «Senha do Administrador».

5.2.3- O utilizador preenche os dados da credencial de administrador local.

5.2.4- O sistema valida que as caixas de texto «Nome do PC», «Nome do Administrador» e «Senha do Administrador» e ativa o botão «Aceitar» - Continua em 7.

3.4.6 Remover PCs de uma lista

Caminho principal:

1. O utilizador carrega no texto indicativo da lista ativa designado de «Definir Lista» que se encontra visível na janela principal da aplicação após o utilizador ter carregado uma lista de PCs.
2. O sistema carrega a lista de PCs, apresenta a janela «Gerir Computadores» e ativa os botões «Editar PC» e «Remover PC» caso a lista não esteja vazia.
3. O utilizador seleciona da lista «Lista de PCs» o computador que pretende retirar.
4. O utilizador carrega em «Remover PC».
5. O sistema apresenta uma caixa de diálogo questionando o utilizador se pretende mesmo retirar o computador da lista.
6. O utilizador carrega em «Sim».
7. O sistema fecha a caixa de diálogo, remove o computador da lista, cifra os dados, atualiza o ficheiro de dados, verifica se a lista está vazia e caso afirmativo, desativa os botões «Remover PC» e «Editar PC».
8. O utilizador carrega em «Terminar Ação».

9. O sistema fecha a janela «Gerir Computadores», volta para a janela principal da aplicação, termina as ações dos PCs removidos e esconde o quadro «Estado dos PCs» caso a lista ativa esteja vazia.

Caminho alternativo:

3.1- O utilizador termina a operação.

3.1.1- O utilizador carrega no botão «Terminar Ação».

3.1.2- O sistema fecha a janela «Gerir Computadores» e volta à janela principal da aplicação.

4.1- O utilizador edita as configurações do PC – *Caso de uso «Editar definições de PC»*.

4.2- O utilizador adiciona um PC – *Caso de uso «Adicionar PCs a uma lista»*.

4.3- O utilizador termina a operação – Continua em 3.1.1.

6.1- O utilizador desiste de remover o computador.

6.1.1- O utilizador carrega em «Não».

6.1.2- O sistema fecha a caixa de diálogo – Continua em 3.

3.4.7 Editar definições de PC

Caminho principal:

1. O utilizador seleciona da lista «Lista de PCs» o computador que pretende editar na janela «Gerir Computadores».
2. O utilizador carrega no botão «Editar PC».
3. O sistema estende a janela «Gerir Computadores» apresentando os botões «Aceitar» e «Cancelar», os botões de seleção «*Active Directory*» e «Grupo de Trabalho» selecionados conforme registado no ficheiro de dados, apresenta as caixas de texto «Nome do Administrador» e «Senha do Administrador» igualmente preenchidas se for o caso e desativa o botão «Adicionar PC».
4. O utilizador seleciona o botão de seleção "*Active Directory*".
5. O sistema ativa o botão «Aceitar».
6. O utilizador carrega em «Aceitar».
7. O sistema atualiza as configurações, cifra os dados, guarda no ficheiro de dados e reduz a janela «Gerir Computadores» ao tamanho original.
8. O utilizador carrega em «Terminar».

9. O sistema fecha a janela «Gerir Computadores» e reinicia as tarefas de comunicação com o computador.

Caminho alternativo:

2.1- O utilizador termina a operação.

2.1.1- O utilizador carrega no botão «Terminar Ação».

2.1.2- O sistema fecha a janela «Gerir Computadores» e volta à janela principal da aplicação.

2.2- O utilizador remove o computador – *Caso de uso «Remover PCs de uma lista»*.

2.3- O utilizador adiciona um computador – *Caso de uso «Adicionar PCs a uma lista»*.

3.4.8 Ligar os PCs da lista ativa

Caminho principal:

1. O utilizador carrega no botão «Ligar PCs» na janela principal da aplicação.
2. O sistema envia um «Pacote mágico» pela rede para cada um dos computadores da lista ativa.

3.4.9 Desligar PCs da lista ativa

Caminho principal:

1. O utilizador carrega no botão «Desligar PCs» na janela principal da aplicação.
2. O sistema envia um comando ao sistema operativo dos computadores da lista ativa a indicá-los a encerrar.

3.4.10 Entrar na administração da aplicação

Através da «Janela de Administração», esboçada pela Figura 31, um administrador poderá definir as contas de utilizadores (docentes), de administradores e as contas de serviço associadas ao domínio e à máquina local. Um docente poderá definir os parâmetros de controlo da aplicação.

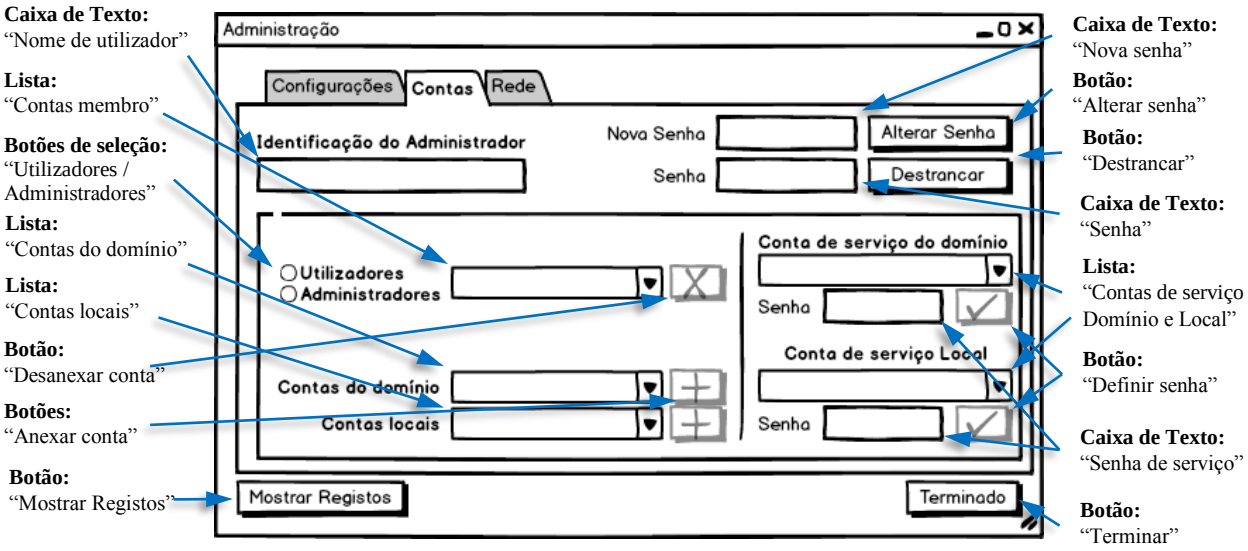

Figura 31 – Esboço da janela «Administração – Contas»

Caminho principal:

1. O utilizador carrega no botão «Administração» na janela principal da aplicação.
2. O sistema abre a janela «Administração».
3. O utilizador seleciona o separador «Contas».
4. O sistema verifica se o utilizador não é membro do grupo de administradores.
5. O utilizador introduz as suas credenciais nas caixas de texto «Nome de utilizador» e «Senha».
6. O sistema identifica o nome de utilizador, verifica se a senha não é nula e ativa o botão «Destrancar».
7. O utilizador carrega no botão «Destrancar».
8. O sistema valida as credenciais e ativa os restantes controlos da janela.

Caminho alternativo:

3.1- O utilizador termina a operação.

3.1.1- O utilizador carrega no botão «Terminar».

3.1.2- O sistema fecha a janela «Administração» e volta para a janela principal da aplicação.

3.2- O utilizador visualiza os registos – *Caso de uso «Visualizar os registos do sistema»*.

4.1- O utilizador é membro do grupo de administradores.

4.1.1- O sistema deteta que o utilizador é membro do grupo de administradores e ativa os restantes controlos da janela.

3.4.11 Alterar a senha de administração embutida

A conta de administração embutida irá salvaguardar o acesso à aplicação na eventualidade da(s) conta(s) de administração definidas terem sido eliminadas.

Caminho principal:

1. O utilizador introduz o texto «Boss» na janela de texto «Nome de utilizador».
2. O sistema apresenta o botão «Alterar senha» e a caixa de texto «Nova senha» na forma desativa.
3. O utilizador introduz a senha na caixa de texto «Senha» e carrega no botão «Destrancar».
4. O sistema valida as credenciais, ativa os restantes controlos da janela e ativa a caixa de texto «Nova senha».
5. O utilizador introduz a nova senha na caixa de texto «Nova senha».
6. O sistema verifica que a senha não é nula e ativa o botão «Alterar senha».
7. O utilizador carrega no botão «Alterar senha».
8. O sistema regista a nova senha e apresenta uma mensagem informando o sucesso da operação.
9. O utilizador carrega em «OK» na mensagem.
10. O sistema fecha a mensagem e volta para a janela «Administração».

Caminho alternativo:

5.1- O utilizador termina a operação.

5.1.1- O utilizador carrega no botão «Terminar».

5.1.2- O sistema fecha a janela «Administração» e volta para a janela principal da aplicação.

3.4.12 Definir a conta de serviço do domínio

A conta de serviço do domínio servirá para estabelecer contacto com as máquinas que sejam membro desse domínio.

Caminho principal:

1. O utilizador entra na janela «Administração».
2. O sistema carrega as contas de domínio existentes na lista «Contas de Serviço do Domínio».

3. O utilizador escolhe uma conta da lista «Contas de Serviço do Domínio» e define a senha respetiva na caixa de texto «Senha de Serviço do Domínio».
4. O sistema verifica que a senha não é nula e ativa o botão «Definir senha».
5. O utilizador carrega no botão «Definir senha».
6. O sistema valida se o utilizador ainda existe, se a senha está correta, regista as credenciais e apresenta uma mensagem de sucesso da operação.
7. O utilizador carrega em «OK».
8. O sistema fecha a mensagem e volta para a janela «Administração».

Caminho alternativo:

6.1- O utilizador enganou-se na senha.

6.1.1 O sistema apresenta uma mensagem informando que a senha está errada.

6.1.2 O utilizador carrega em «OK».

6.1.3 O sistema fecha a mensagem e volta para o ponto 3.

3.4.13 Definir a conta local de serviço

A conta de serviço local servirá para permitir o funcionamento do *software* numa máquina que não pertença a um domínio AD.

Caminho principal:

1. O utilizador entra na janela «Administração».
2. O sistema carrega as contas de domínio existentes na lista «Conta Local de Serviço».
3. O utilizador escolhe uma conta da lista «Conta Local de Serviço» e define a senha respetiva na caixa de texto «Senha Local de Serviço».
4. O sistema verifica que a senha não é nula e ativa o botão «Definir senha».
5. O utilizador carrega no botão «Definir senha».
6. O sistema valida se o utilizador ainda existe, se a senha está correta, regista as credenciais e apresenta uma mensagem de sucesso da operação.
7. O utilizador carrega em «OK».
8. O sistema fecha a mensagem e volta para a janela «Administração».

Caminho alternativo:

6.1- O utilizador enganou-se na senha.

6.1.1 O sistema apresenta uma mensagem informando que a senha está incorreta.

6.1.2 O utilizador carrega em «OK».

6.1.3 O sistema fecha a mensagem e volta para o ponto 3.

3.4.14 Adicionar conta aos administradores

As contas definidas como pertencentes ao grupo de administradores terão a capacidade de adicionar ou remover contas ao grupo de administradores e de utilizadores bem como definir as contas de serviço e ainda os parâmetros de rede.

Caminho principal:

1. O utilizador entra na janela «Administração».
2. O sistema carrega as contas de domínio existentes na lista «Contas do Domínio», as contas locais na lista «Contas Locais» e as contas de utilizadores na lista «Contas membro».
3. O utilizador carrega no botão de seleção «Administradores» e escolhe uma conta da lista «Contas do domínio».
4. O sistema ativa o botão «Anexar conta» respetivo.
5. O utilizador carrega no botão «Anexar conta» respetivo.
6. O sistema regista a conta e inclui-a na lista «Contas membro».

Caminho alternativo:

3.1- O utilizador carrega no botão de seleção «Utilizadores» – *Caso de uso «Adicionar conta aos utilizadores»*.

3.2- O utilizador adiciona uma conta local.

3.2.1- O utilizador escolhe uma conta da lista «Contas locais».

3.2.2- O sistema ativa o botão «Anexar conta» respetivo.

3.2.3- O utilizador carrega no botão «Anexar conta».

3.2.4- O sistema regista a conta e inclui-a na lista «Contas membro».

3.3- O utilizador retira uma conta dos administradores – *Caso de uso «Remover conta dos administradores»*.

3.4.15 Remover conta dos administradores

Caminho principal:

1. O utilizador entra na janela «Administração».

2. O sistema carrega as contas de domínio existentes na lista «Contas do Domínio», as contas locais na lista «Contas Locais» e as contas de utilizadores na lista «Contas membro».
3. O utilizador carrega no botão de seleção «Administradores» e escolhe uma conta da lista «Contas membro».
4. O sistema ativa o botão «Desanexar conta».
5. O utilizador carrega no botão «Desanexar conta».
6. O sistema retira a conta da lista «Contas membro» e guarda as alterações.

Caminho alternativo:

3.1- O utilizador aborta a ação.

3.1.1- O utilizador carrega no botão «Terminar».

3.1.2- O sistema

6.1- Ocorreu um erro.

6.1.1- O sistema apresenta uma mensagem informando o utilizador que ocorreu um erro.

6.1.2- O utilizador carrega em «OK».

6.1.3- O sistema continua no ponto 3.

3.4.16 Adicionar conta aos utilizadores

As contas definidas como utilizadores terão a capacidade de utilizar o *software* para bloquear e desbloquear as máquinas dos formandos.

Caminho principal:

1. O utilizador entra na janela «Administração».
2. O sistema carrega as contas de domínio existentes na lista «Contas do Domínio» e as contas locais na lista «Contas Locais».
3. O utilizador carrega no botão de seleção «Utilizadores» e escolhe uma conta da lista «Contas do domínio».
4. O sistema ativa o botão «Anexar conta» respetivo.
5. O utilizador carrega no botão «Anexar conta» respetivo.
6. O sistema regista a conta e inclui-a na lista «Contas membro».

Caminho alternativo:

3.1- O utilizador carrega no botão de seleção «Administradores» – *Caso de uso «Adicionar conta aos administradores»*.

3.2- O utilizador adiciona uma conta local.

3.2.1- O utilizador escolhe uma conta da lista «Contas locais».

3.2.2- O sistema ativa o botão «Anexar utilizador» respetivo.

3.2.3- O utilizador carrega no botão «Anexar utilizador».

3.2.4- O sistema regista a conta e inclui-a na lista «Contas membro».

3.3- O utilizador retira uma conta dos utilizadores – *Caso de uso «Remover conta dos utilizadores»*.

3.4.17 Remover conta aos utilizadores

Caminho principal:

1. O utilizador entra na janela «Administração».
2. O sistema carrega as contas de domínio existentes na lista «Contas do Domínio», as contas locais na lista «Contas Locais» e as contas de utilizadores na lista «Contas membro».
3. O utilizador carrega no botão de seleção «Utilizadores» e escolhe uma conta da lista «Contas membro».
4. O sistema ativa o botão «Desanexar conta».
5. O utilizador carrega no botão «Desanexar conta».
6. O sistema retira a conta da lista «Contas membro» e guarda as alterações.

Caminho alternativo:

3.1- O utilizador aborta a ação.

3.1.1- O utilizador carrega no botão «Terminar».

3.1.2- O sistema

6.1- Ocorreu um erro.

6.1.1- O sistema apresenta uma mensagem informando o utilizador que ocorreu um erro.

6.1.2- O utilizador carrega em «OK».

6.1.3- O sistema continua no ponto 3.

3.4.18 Definir o endereço de rede a utilizar

A aplicação necessitará de uma forma de receber informação acerca do estado das máquinas que controla. Cada máquina enviará o seu estado e resultado de cada operação para a máquina gestora, sendo para isso necessário estabelecer um ponto de escuta. A Figura 32 representa o

esboço da «Janela de Administração» opção «Rede» onde são definidos o protocolo e a interface de rede que servirá para escutar as referidas respostas.

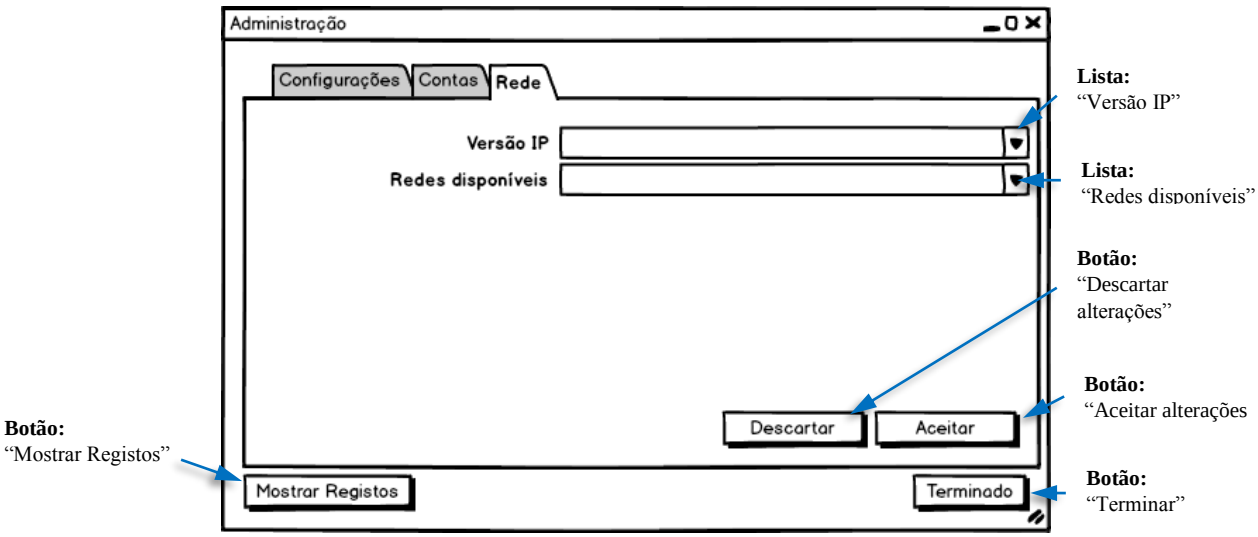

Figura 32 – Esboço da janela «Administração – Rede»

Caminho principal:

1. O utilizador entra na janela «Administração» e escolhe o separador «Rede».
2. O sistema identifica as interfaces operacionais, lista-as na lista «Redes disponíveis» e seleciona a que se encontra definida.
3. O utilizador seleciona a rede que pretende que seja utilizada e carrega em «Aceitar».
4. O sistema guarda a escolha efetuada.

Caminho alternativo:

3.1- O utilizador escolhe o protocolo pretendido.

3.1.1- O utilizador seleciona da lista «Versão IP» o protocolo que pretende utilizar.

3.1.2- O sistema carrega na lista «Redes disponíveis» as interfaces configuradas para operar com o protocolo escolhido e volta para o ponto 3.

3.2- O utilizador aborta a ação.

3.2.1- O utilizador carrega em «Descartar».

3.2.2- O sistema volta a carregar as configurações anteriores.

3.4.19 Definir controlos de endereços e programas

A aplicação basear-se-á em quatro tipos de controlos, sendo estes, os endereços internet, os programas e os dispositivos USB autorizados e ainda as contas de utilizador que serão

autorizadas a iniciar sessão. Para que os formadores possam facilmente associar cada um destes tipos ao item de controlo, o administrador fará a ligação entre um nome amigável ao utilizador e o item correspondente. A Figura 33 retrata o esboço da janela de administração que permitirá associar os endereços de internet. Nesta mesma figura, o caso representado é o da associação entre o nome «Moodle IPL» e o endereço «ead.ipleiria.pt».

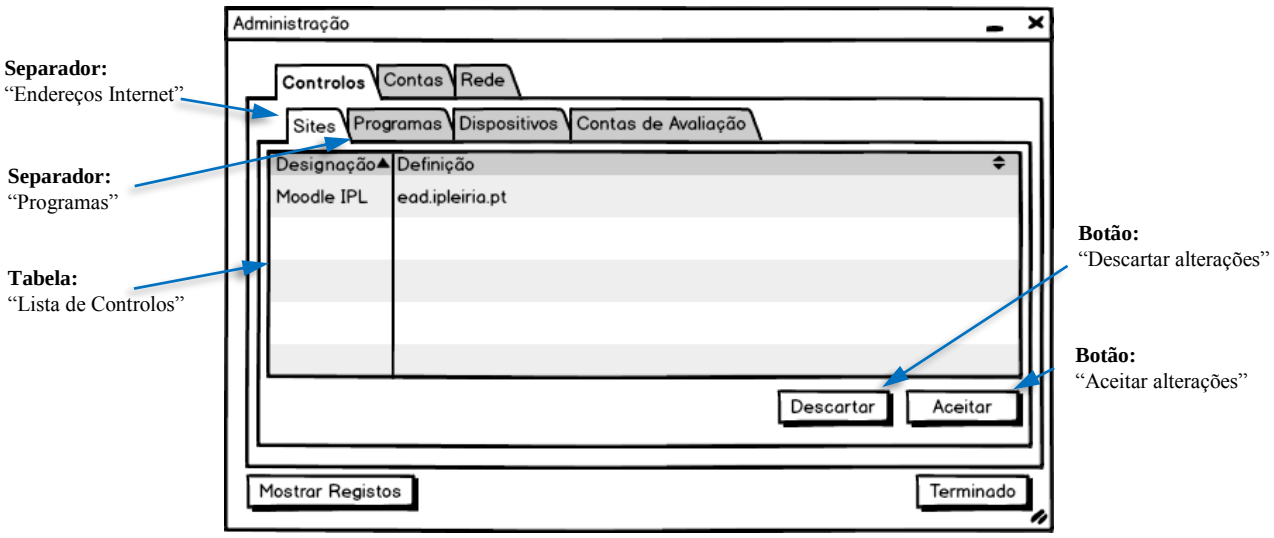

Figura 33 – Esboço da janela «Administração – Sítios Interrnet»

Caminho principal (endereços de rede e programas):

1. O utilizador entra na janela «Administração», escolhe o separador «Controlos» e de seguida o separador «Sites» ou «Programas».
2. O sistema carrega na tabela «Lista de Controlos» as configurações que se encontram guardadas.
3. O utilizador carrega na célula da coluna «Designação» e da linha livre e escreve o nome amigável do controlo que pretende definir.
4. O sistema valida que o nome introduzido não se encontra já utilizado.
5. O utilizador carrega na célula respeitante à coluna «Definição» e introduz a identificação controlo.
6. O sistema valida que o controlo ainda não tinha sido introduzido e ativa o botão «Aceitar alterações».
7. O utilizador carrega no botão «Aceitar alterações».
8. O sistema guarda as configurações.

Caminho alternativo:

3.1- Uma entrada é eliminada.

3.1.1- O utilizador seleciona da tabela «Lista de Controlos», a linha que contém o controlo que pretende eliminar e carrega no botão «eliminar» do teclado.

3.1.2- O sistema retira a linha da tabela «Lista de Controlos» e volta ao ponto 3.

3.2- O utilizador cancela a operação.

3.2.1- O utilizador carrega em «Terminado».

3.2.2- O sistema fecha a janela «Administração» e volta para a janela principal da aplicação.

4.1- O nome introduzido já foi utilizado.

4.1.1- O sistema deteta que o nome introduzido já foi utilizado e desativa o botão «Aceitar alterações».

4.1.2- O utilizador corrige o nome.

4.1.3- O sistema volta ao ponto 4.

6.1- O controlo definido já foi utilizado.

6.1.1- O sistema deteta que o controlo introduzido já foi utilizado e desativa o botão «Aceitar alterações».

6.1.2- O utilizador corrige a identificação do controlo.

6.1.3- O sistema volta ao ponto 6.

7.1- O utilizador descarta as alterações.

7.1.1- O utilizador carrega no botão «Descartar alterações».

7.1.2- O sistema continua no ponto 2.

3.4.20 Definir controlos de dispositivos

A Figura 34 retrata o esboço da janela de administração que permitirá associar os dispositivos USB. Aqui o utilizador poderá definir o seu dispositivo USB no sistema.

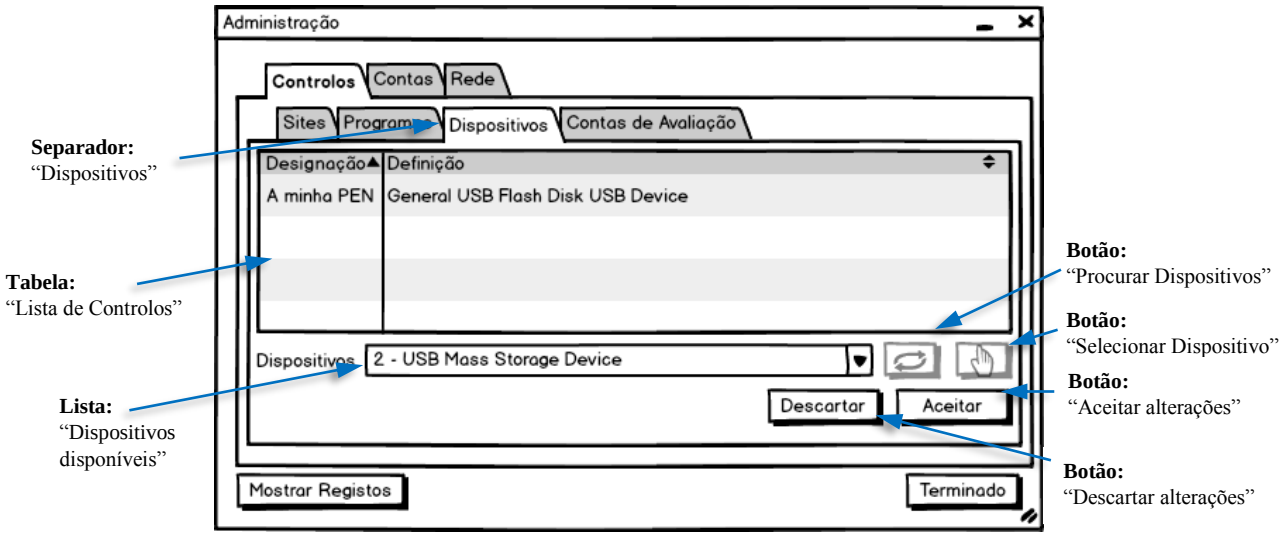

Figura 34 – Esboço da janela «Administração – Dispositivos»

Caminho principal:

1. O utilizador entra na janela «Administração», escolhe o separador «Controlos» e de seguida o separador «Dispositivos».
2. O sistema carrega na tabela «Lista de Controlos» as configurações que se encontram guardadas, recolhe informações sobre os dispositivos USB conhecidos do Sistema Operativo (SO) e apresenta-os na lista «Dispositivos disponíveis».
3. O utilizador carrega na célula da coluna «Designação» da linha livre e escreve o nome amigável do controlo que pretende definir.
4. O sistema valida que o nome introduzido não se encontra já utilizado.
5. O utilizador carrega na célula respeitante à coluna «Definição», seleciona da lista «Dispositivos disponíveis» o dispositivo que pretende adicionar.
6. O sistema valida que o dispositivo ainda não foi adicionado e ativa o botão «Selecionar Dispositivo».
7. O utilizador carrega em «Selecionar Dispositivo».
8. O sistema adiciona o dispositivo na tabela «Lista de Controlos», desativa o botão «Selecionar Dispositivo» e ativa o botão «Aceitar alterações».
9. O utilizador carrega no botão «Aceitar alterações».
10. O sistema guarda as configurações.

Caminho alternativo:

3.1- Um dispositivo é removido.

3.1.1- O utilizador seleciona da tabela «Lista de Controlos», a linha que contém o dispositivo que pretende eliminar e carrega no botão «eliminar» do teclado.

3.1.2- O sistema retira a linha selecionada da tabela «Lista de Controlos» e volta ao ponto 3.

3.2- O utilizador cancela a operação.

3.2.1- O utilizador carrega em «Terminado».

3.2.2- O sistema fecha a janela «Administração» e volta para a janela principal da aplicação.

4.1- O nome introduzido já foi utilizado.

4.1.1- O sistema deteta que o nome introduzido já foi utilizado e desativa o botão «Aceitar alterações».

4.1.2- O utilizador corrige o nome.

4.1.3- O sistema volta ao ponto 4.

5.1- O utilizador introduz um novo dispositivo.

5.1.1- O utilizador após introduzir um novo dispositivo carrega em «Procurar Dispositivos».

5.1.2- O sistema recolhe informações sobre os dispositivos USB conhecidos do SO e apresenta-os na lista «Dispositivos disponíveis» e continua no ponto 5.

6.1- O controlo definido já foi utilizado.

6.1.1- O sistema deteta que o controlo introduzido já foi utilizado e desativa o botão «Aceitar alterações».

6.1.2- O utilizador corrige a identificação do controlo.

6.1.3- O sistema volta ao ponto 6.

9.1- O utilizador descarta as alterações.

9.1.1- O utilizador carrega no botão «Descartar alterações».

9.1.2- O sistema continua no ponto 2.

3.4.21 Definir controlos de contas de avaliação

A Figura 35 retrata o esboço da janela de administração que permite associar as contas a utilizar nas avaliações. Quando ativado este controlo, apenas as contas definidas poderão iniciar sessão com sucesso. Este controlo fará também parte do funcionamento do bloqueio «Programas» bem como do bloqueio «Copiar e Colar».

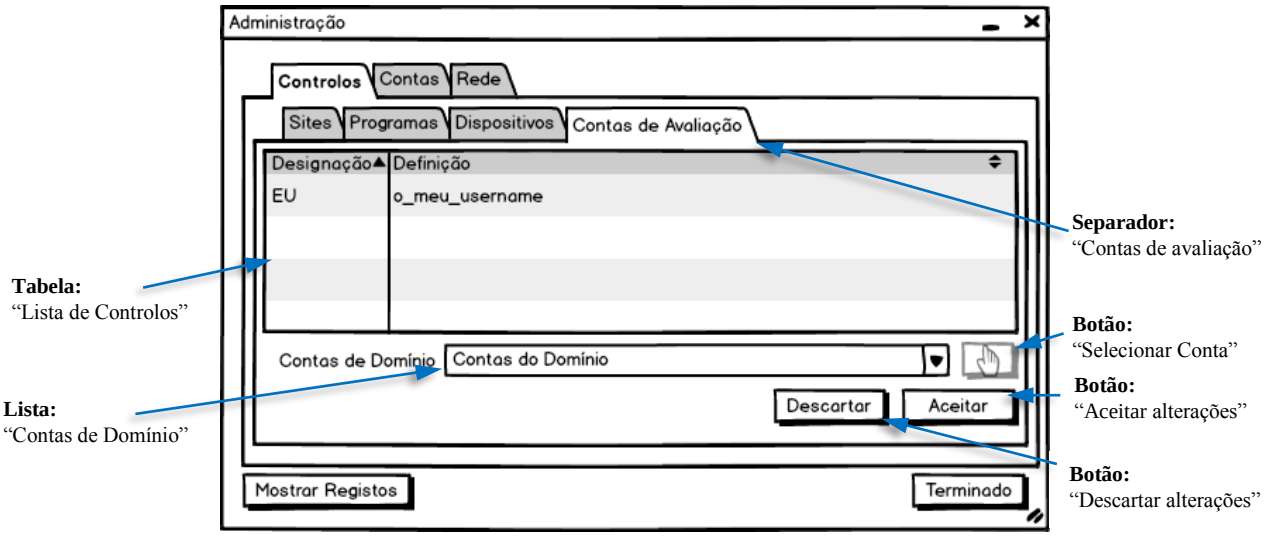

Figura 35 – Esboço da janela «Administração – Contas de avaliação»

Caminho principal:

1. O utilizador entra na janela «Administração», escolhe o separador «Controlos» e de seguida o separador «Contas de Avaliação».
2. O sistema carrega na tabela «Lista de Controlos» as configurações que se encontram guardadas, recolhe informações sobre as contas de Domínio presentes na OU onde a máquina se encontra inserida e apresenta-as na lista «Contas de Domínio».
3. O utilizador carrega na célula da coluna «Designação» da linha livre e escreve o nome amigável do controlo que pretende definir.
4. O sistema valida que o nome introduzido não se encontra já utilizado.
5. O utilizador carrega na célula respeitante à coluna «Definição», seleciona da lista «Contas de Domínio» ou define manualmente a conta que pretende adicionar.
6. O sistema valida que a conta ainda não foi adicionada e ativa o botão «Selecionar Conta».
7. O utilizador carrega em «Selecionar Conta».
8. O sistema adiciona a conta na tabela «Lista de Controlos», desativa o botão «Selecionar Conta» e ativa o botão «Aceitar alterações».
9. O utilizador carrega no botão «Aceitar alterações».
10. O sistema guarda as configurações.

Caminho alternativo:

3.1- Uma conta é removida.

3.1.1- O utilizador seleciona da tabela «Lista de Controlos», a linha que contém a conta que pretende eliminar e carrega no botão «eliminar» do teclado.

3.1.2- O sistema retira a linha selecionada da tabela «Lista de Controlos» e volta ao ponto 3.

3.2- O utilizador cancela a operação.

3.2.1- O utilizador carrega em «Terminado».

3.2.2- O sistema fecha a janela «Administração» e volta para a janela principal da aplicação.

4.1- O nome introduzido já foi utilizado.

4.1.1- O sistema deteta que o nome introduzido já foi utilizado e desativa o botão «Aceitar alterações».

4.1.2- O utilizador corrige o nome.

4.1.3- O sistema volta ao ponto 4.

6.1- O controlo definido já foi utilizado.

6.1.1- O sistema deteta que o controlo introduzido já foi utilizado e desativa o botão «Aceitar alterações».

6.1.2- O utilizador corrige a identificação do controlo.

6.1.3- O sistema volta ao ponto 6.

9.1- O utilizador descarta as alterações.

9.1.1- O utilizador carrega no botão «Descartar alterações».

9.1.2- O sistema continua no ponto 2.

10.1- Ocorreu um erro ao guardas as configurações.

10.1.1- O sistema apresenta uma mensagem de erro indicando ao utilizador que ocorreu um erro.

10.1.2- O utilizador carrega em «OK».

10.1.3- O sistema volta ao ponto 3.

3.4.22 Configurar o bloqueio de computadores

A Figura 36 retrata o esboço da janela «Configurações», o local onde se configura quais os controlos que vão produzir efeito no ato do bloqueio. Nesta janela podem ser identificados cinco tipos de controlos, são eles: os Sites autorizados; os Programas autorizados; os dispositivos USB autorizados; as Contas de Utilizador autorizadas e o controlo da utilização da Área de transferência. Os primeiros quatro tipos possuem configuração granular, ou seja, permite escolher qual ou quais os controlos desse tipo a surtir efeito.

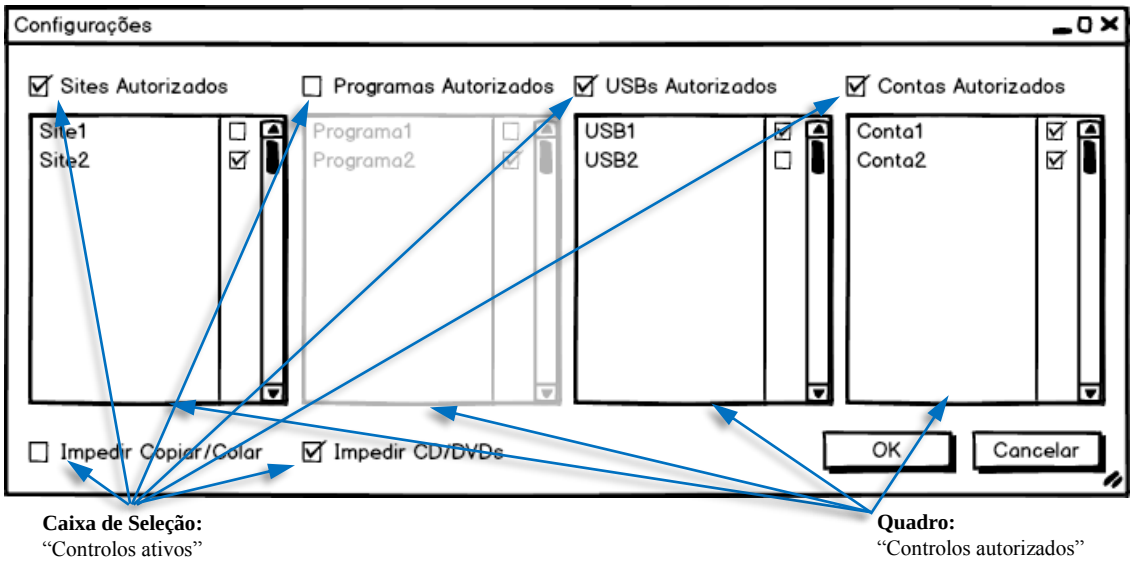

Figura 36 – Esboço da janela «Configurações»

Caminho principal:

1. Após selecionar a lista de PCs nos quais pretende aplicar a restrição, o utilizador seleciona «Configurar» na lista «Ações» presente na janela principal da aplicação identificada pela Figura 27 e de seguida carrega no botão «Avançar».
2. O sistema abre a janela «Configurações» e carrega as configurações existentes para a lista de PCs em causa.
3. O utilizador define quais os controlos que pretende aplicar aos PCs da lista.
4. O sistema valida que o(s) controlo(s) selecionado(s) não requer(em) a definição de «Contas Autorizadas».
5. O utilizador carrega em «OK».
6. O sistema guarda as configurações de bloqueio da lista de PCs selecionada, fecha a janela «Configurações» e volta para a janela principal da aplicação.

Caminho alternativo:

3.1- O utilizador cancela a ação.

3.1.1- O utilizador seleciona «Cancelar».

3.1.2- O sistema fecha a janela «Configurações» e volta para a janela principal da aplicação.

4.1- Os controlos selecionados exigem definir contas de utilização.

4.1.1- O sistema coloca o visto na caixa de texto «Contas autorizadas» e apresenta o quadro de definição de controlos de contas autorizadas.

4.1.2- O utilizador confirma as contas que vão ser utilizadas e carrega em «OK».

4.1.3- O sistema continua no ponto 6.

6.1- Ocorreu um erro ao guardas as configurações.

6.1.1- O sistema apresenta uma mensagem de erro indicando ao utilizador que ocorreu um erro.

6.1.2- O utilizador carrega em «OK».

6.1.3- O sistema volta ao ponto 3.

3.4.23 Executar o bloqueio de computadores

Caminho principal:

1. Após selecionar a lista de PCs nos quais pretende aplicar a restrição, o utilizador seleciona «Bloquear» na lista «Ações» presente na janela principal da aplicação identificada pela Figura 27 e de seguida carrega no botão «Avançar».
2. O sistema verifica se já obteve resposta de todos os PCs da lista e ativa o botão «Avançar».
3. O utilizador carrega em «Avançar».
4. O sistema envia os comandos necessários aos PCs identificados na lista e atualiza o estado do «Quadro de PCs» à medida que as respostas vão chegando.

3.4.24 Executar o desbloqueio de computadores

Caminho principal:

1. Após selecionar a lista de PCs nos quais pretende aplicar a restrição, o utilizador seleciona «Desbloquear» na lista «Ações» presente na janela principal da aplicação identificada pela Figura 27 e de seguida carrega no botão «Avançar».
2. O sistema verifica se já obteve resposta de todos os PCs da lista e ativa o botão «Avançar».
3. O utilizador carrega em «Avançar».
4. O sistema envia os comandos necessários aos PCs identificados na lista e atualiza o estado do «Quadro de PCs» à medida que as respostas vão chegando.

3.4.25 Verificar estado de um computador

A Figura 37 retrata o esboço da janela «Detalhes do Estado do PC», o local onde o utilizador pode verificar quais os controlos ativos num determinado PC.

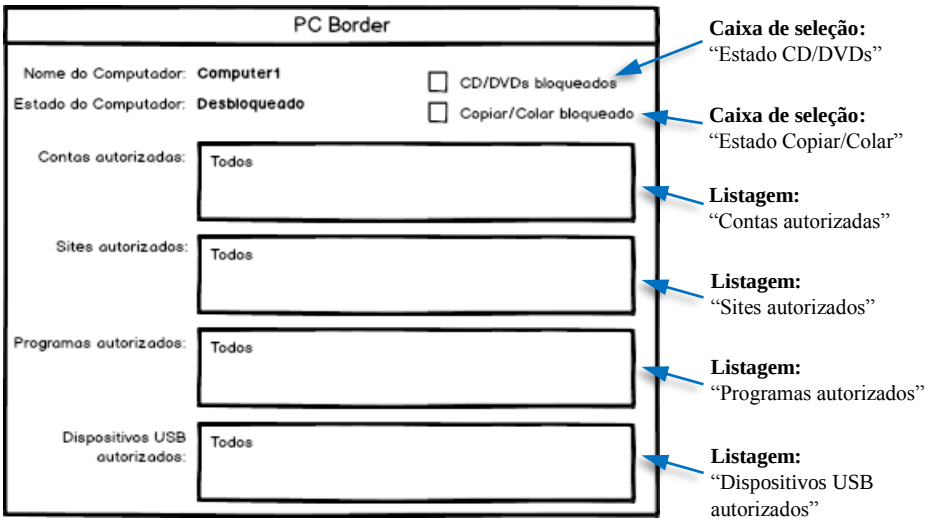

Figura 37 – Esboço da janela «Detalhes do estado do PC»

Caminho principal:

1. O utilizador faz duplo-clique na linha do «Quadro de PCs» que contém o PC que deseja analisar.
2. O sistema abre uma janela «Detalhes do Estado do PC» e apresenta o seu estado.
3. O utilizador fecha a janela carregando na tecla «Escape» do teclado enquanto tem a janela em foco ou fazendo novo duplo-clique na linha correspondente do «Quadro de PCs».
4. O sistema fecha a janela «Detalhes do Estado do PC» correspondente.

3.4.26 Visualizar os registos do sistema

A Figura 38 Figura 37retrata o esboço da janela «Visualizador de Registos», local onde qualquer utilizador pode visualizar as ações cometidas na utilização do *software*. Um administrador tem ainda a capacidade de limpar todos os registos.

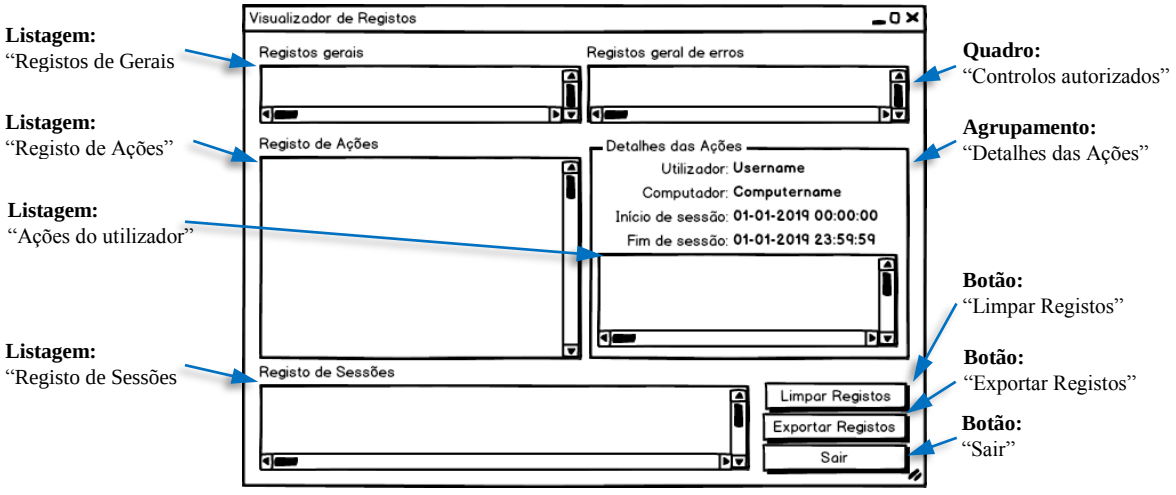

Figura 38 – Esboço da janela «Visualizador de Registos»

Caminho principal:

1. O utilizador carrega em «Mostrar Registo» na janela «Administração» (Figura 31).
2. O sistema mostra a janela «Visualizador de Registos», valida qual o papel do utilizador e ativa o botão «Limpar Registos» caso tenha o papel de administrador.
3. O utilizador seleciona um registo da listagem «Registo de Ações» fazendo duplo-clique.
4. O sistema apresenta o agrupamento «Detalhes das Ações» carregando-lhe os detalhes das ações efetuadas pelo utilizador da sessão do registo.

Caminho alternativo:

3.1- O utilizador cancela a ação.

3.1.1- O utilizador carrega no botão «Sair».

3.1.2- O sistema fecha a janela «Visualizador de Registos» e volta para a janela «Administração».

3.2- O utilizador elimina os registos.

3.2.1- O utilizador carrega no botão «Limpar Registos».

3.2.2- O sistema elimina todos os registos à exceção dos registos da sessão do utilizador.

3.3- O utilizador exporta os registos – *Caso de uso «Exportar os registos do sistema»*.

3.4.27 Exportar os registos do sistema

Caminho principal:

1. O utilizador carrega em «Exportar Registos» na janela «Visualizador de Registos».
2. O sistema abre uma janela de abertura de ficheiro.
3. O utilizador define o nome do ficheiro e carrega em «Abrir».
4. O sistema adiciona a extensão «csv» ao nome, fecha a janela de abertura de ficheiro, faz uma cópia de segurança caso o ficheiro selecionado já exista apagando uma possível cópia já existente, exporta os registos em formato «csv» para o ficheiro indicado e apresenta uma mensagem indicando o sucesso da operação.

Caminho alternativo:

3.1- O utilizador cancela a ação.

3.1.1- O utilizador carrega em «Cancelar» na janela de abertura de ficheiro.

3.1.2- O sistema fecha a janela de abertura de ficheiro e volta para a janela «Visualizador de Registos».

Capítulo 4 - A aplicação «PC Border»

A aplicação a desenvolver, de certa forma, servirá de fronteira a um PC, controlando a entrada e saída de informação. Dado que a palavra inglesa «Border» significa «Fronteira» na língua portuguesa, a aplicação foi denominada de «PC Border», ou seja, a fronteira do computador.
Neste capítulo são descritos os passos e as técnicas utilizadas na conceção da referida aplicação.

4.1 Arquitetura

O objetivo é a criação de uma aplicação com interface gráfica para ambiente Microsoft Windows. A aplicação deve implementar as funcionalidades propostas e ser simples de utilizar e intuitiva. Para tal, foi optado pela utilização da *framework* .NET com a linguagem de programação C#. A utilização do *Integrated Development Environment* (IDE) da Microsoft designado de «Visual Studio» e da referida *framework*, permite conceber uma aplicação cuja interação é familiar à grande maioria das pessoas.

Presentemente, os sistemas operativos Windows XP, Vista, Windows 8 e as primeiras versões do Windows 10 já ultrapassaram o período de suporte[22] dado pelo fabricante. Embora o Windows 7 permaneça com suporte previsto apenas até o início de 2020, segundo as estatísticas[23,24], o número de sistemas com o Windows 7 ainda corresponde a cerca de metade do número de sistemas com o Windows 10. Posto isto e visando a possibilidade de a aplicação ser utilizada por outras instituições, o *software* terá de funcionar com pelo menos o Windows 7, tanto em arquitetura de 32 como de 64-bit.

A aplicação deve funcionar com máquinas munidas de sistema operativo (SO) integrados num domínio de AD, bem como, com máquinas configuradas em «Grupo de Trabalho», tal como representado na Figura 39.

[22] https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet
[23] https://www.w3schools.com/browsers/browsers_os.asp
[24] http://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide

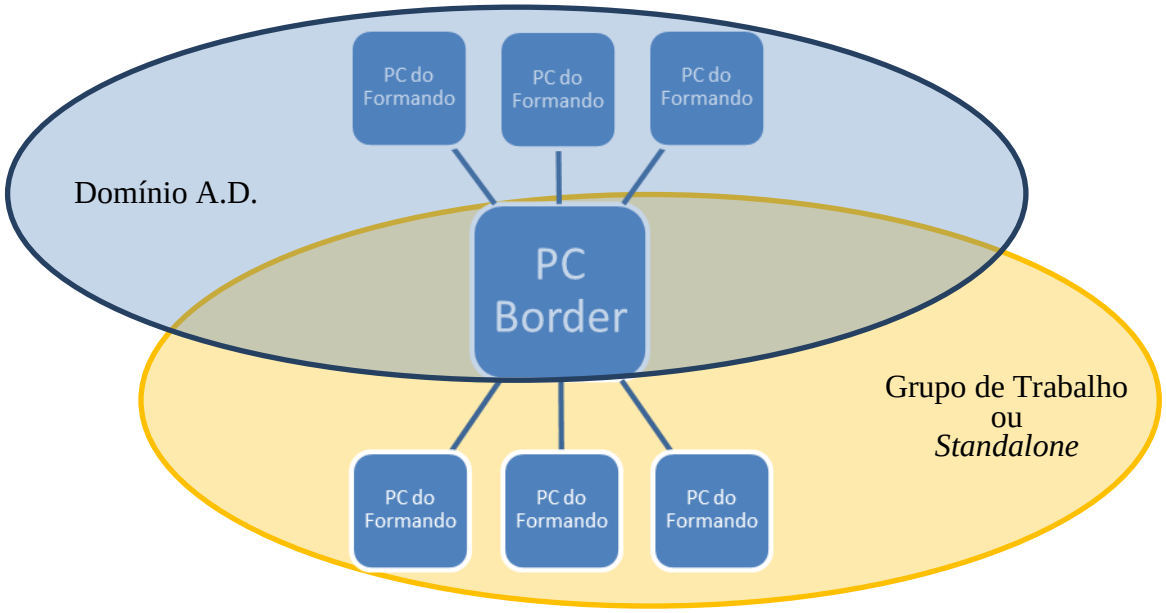

Figura 39 – Esquema representativo da conectividade PC Border – Máquinas cliente

Quanto à topologia de rede, não existem requisitos. As máquinas envolvidas podem pertencer à mesma rede ou a segmentos de rede diferentes desde que operem o protocolo TCP/IP e que seja garantido o correto roteamento de tráfego entre elas, tal como representado na Figura 40.

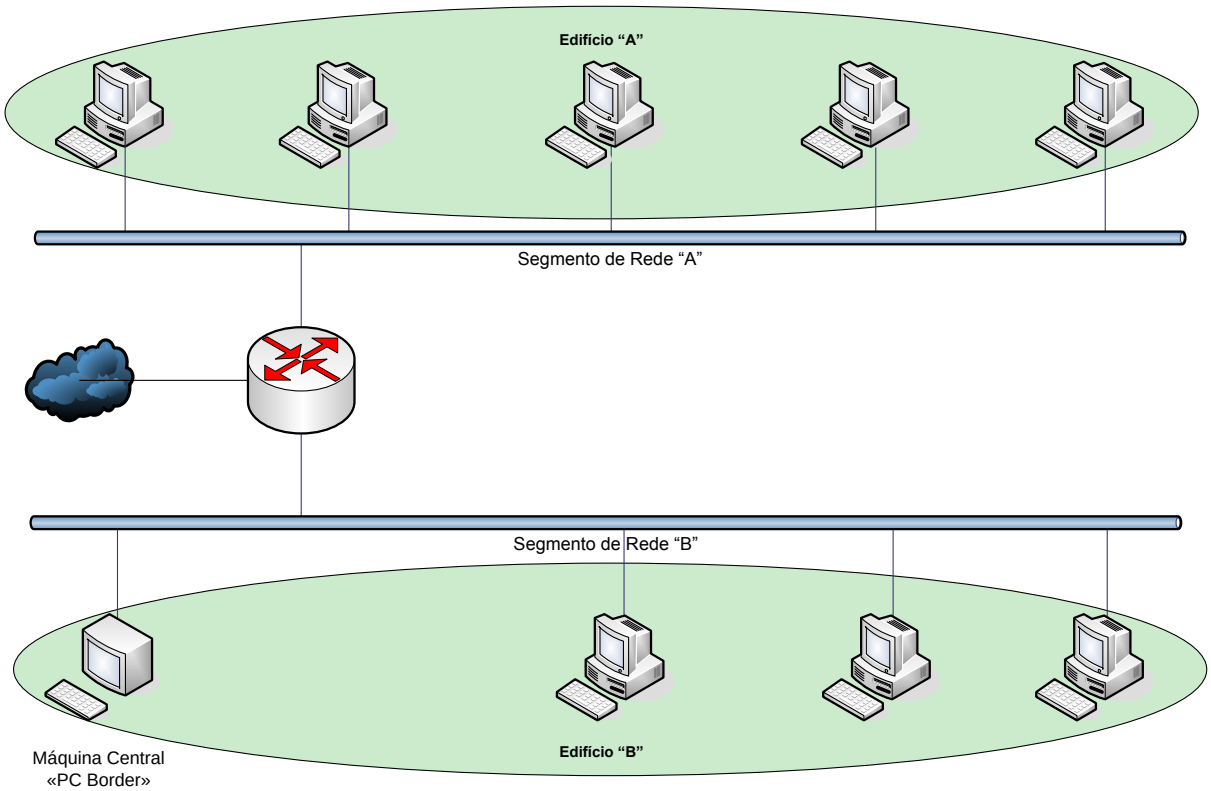

Figura 40 – Diagrama representativo da topologia de rede

A implementação de uma forma centralizada de configuração das máquinas que serão afetas às avaliações, implica a existência de um meio de comunicação entre estas máquinas cliente e a máquina central, onde é executado o «PC Border». A comunicação entre estas máquinas é efetuada através da própria rede, dispensando a implementação de novo hardware ou infraestrutura e seus custos associados. No caso sobre o qual este trabalho recai, a máquina central é um PC que se encontra ao dispor exclusivo do formador e presente na mesma rede física que os PCs dos formandos.

4.2 Idealização e princípios de funcionamento

Qualquer software deve ser apresentado na língua que o utilizador mais prefere, como tal, a forma de conseguir alterar a língua de apresentação, deve ser evidente, estando presente na janela principal da aplicação. As exigências neste aspeto foram de disponibilizar a interface em português, inglês e francês, sendo que a solicitação do idioma francês se deve à existência de docentes a lecionar esta língua e que virão a utilizar o *software*.

O aspeto visual das aplicações é de grande importância, especialmente em aplicações de *desktop*. Deste modo, a aplicação PC Border recorre, na medida do possível, ao uso de imagens e gama de contraste de cores que sejam perfeitamente percetíveis e agradáveis à visão, não esquecendo ainda que cerca de 8% dos homens e 0,5% das mulheres[25] apresentam alguma limitação na perceção de certas cores, vulgarmente designado por daltonismo.

A razão para criação do *software* «PC Border» é permitir o controlo da circulação de informação, de forma fácil e rápida, em determinadas máquinas. Decidiu-se que esta aplicação apenas dará ordens às máquinas a bloquear, não fazendo em si parte do processo de bloqueio. Não será uma aplicação do tipo editor de texto ou jogo, onde a sua execução é previsível durar algum tempo. Após as restrições aplicadas nas máquinas, a aplicação poderá ser encerrada, pois essas restrições permanecerão ativas mesmo sem haver contacto com a aplicação. O facto de não tomar papel ativo no bloqueio das máquinas torna o funcionamento autónomo e permite que sejam poupados recursos, tanto de rede, como das próprias máquinas. Se a aplicação for mantida em execução, irá enviando *echo-requests* de três em três minutos para determinar se as máquinas continuam contactáveis. Ao fim de cada 10 minutos ou logo após ter sido

[25] http://www.colourblindawareness.org/colour-blindness/

restabelecido contacto com alguma das máquinas, será enviado um pedido de *status* para que a aplicação continue a par do estado das máquinas.

O princípio de funcionamento da aplicação centra-se na ideia de que as avaliações serão feitas utilizando contas específicas para o efeito e não com as credenciais dos próprios alunos a avaliar. Este princípio é fundamental, pois para executar determinados aspetos do bloqueio, será necessário executar código nas contas e sessões da máquina que se pretende bloquear, bem como, para executar o início automático dessas mesmas sessões, algo que não é possível sem haver posse das credenciais de tais contas. Assim sendo, o administrador terá de identificar essas credenciais e defini-las na aplicação. Para guardar tais credenciais, o *software* irá cifrar as senhas recorrendo a um algoritmo AES[20] (*Advanced Encryption Standard*) e registá-las em zona própria da configuração existente em memória. Essa configuração será, também, posteriormente cifrada com algoritmo próprio idealizado para essa tarefa e escrita em ficheiro próprio, o que faz com que as senhas sejam duplamente cifradas. Este ficheiro estará localizado na máquina onde a aplicação está a correr, permitindo a sua reutilização a qualquer altura no futuro sem exigir configurações prévias.

A aplicação terá dois papéis perfeitamente distintos, o primeiro sendo o de operação[26] e o segundo o de configuração[27]. A configuração estará a cargo de um ou mais técnicos de informática que serão os administradores da aplicação. Os docentes serão as pessoas responsáveis por operar a aplicação e terão, também, a capacidade para adicionar os seus próprios equipamentos USB à configuração presente na lista[28] de equipamentos autorizados, bem como, outras pequenas configurações. A aplicação deverá permitir selecionar/agrupar um conjunto de máquinas para que possam todas receber a mesma configuração de bloqueio, por exemplo, caso se pretenda configurar uniformemente os PCs de uma mesma sala de aulas. A criação de um agrupamento poderá ser feita pelo administrador de sistema ou pelo próprio operador. O operador começará por selecionar a «Sala» que pretende controlar. Para facilitar o definir da correlação entre máquinas e salas, o sistema terá de ser capaz de determinar quais as máquinas inseridas na mesma «OU» do domínio, onde eventualmente o PC central possa estar inserido, e apresentá-las numa lista para que o utilizador possa selecionar.

[26] Papel o qual permite a um utilizador operar a aplicação no sentido de executar a tarefa para a qual foi concebida.
[27] Papel o qual permite a um utilizador fazer todas as configurações prévias para uma simples utilização do operador.
[28] Lista de dispositivos USB cuja utilização é autorizada e que se encontra registada no ficheiro de configuração.

Os formadores que irão utilizar a aplicação não terão necessariamente de ter conhecimentos de informática, muito menos das Tecnologias de Informação. Será requerido ao administrador a pré-configuração de todos os parâmetros necessários para tornar a aplicação simples de utilizar pelos docentes. Em primeiro lugar, caberá exclusivamente ao administrador definir quem são os utilizadores da aplicação, quer sejam docentes ou outros administradores. Em segundo lugar, o administrador terá de definir qual a interface de rede e o protocolo de comunicação que a aplicação vai utilizar para receber comunicações dos clientes. Posto estes factos, a aplicação deverá incluir estas configurações no ficheiro de registo. No arranque, a aplicação necessitará comparar o utilizador da sessão executante com a lista dos utilizadores autorizados identificando o seu papel. Caso o utilizador não esteja definido e se for administrador da máquina, a aplicação terá de apresentar uma janela dando a possibilidade ao utilizador de se adicionar mediante a apresentação das credenciais da conta de administração embutida[29]. Observando a Tabela 3, é possível identificar quais as permissões que os papéis terão na aplicação. Normalmente um administrador não teria permissões para bloquear ou desbloquear os PCs, pois essa tarefa é dos formadores. Foi decidido atribuir-lhes esta capacidade para que possam diagnosticar alguma anomalia que ocorra na aplicação, sem que necessitem da intervenção de terceiros ou que sejam atribuídos ambos os papéis ao mesmo utilizador.

Tabela 3 – Permissões dos papéis de utilizador

	PAPÉIS	
TAREFAS	Administrador	Formador
Definir língua de apresentação	**X**	**X**
Gerir contas de Administrador	**X**	
Gerir contas de Formador	**X**	
Definir contas de serviço	**X**	
Definir protocolo de rede	**X**	
Visualizar registos	**X**	**X**
Gerir sites autorizados	**X**	**X**
Gerir programas autorizados	**X**	**X**
Gerir dispositivos autorizados	**X**	**X**
Gerir contas de avaliação	**X**	**X**
Gerir listas de PCs (salas)	**X**	**X**
Gerir PCs das listas de PCs	**X**	**X**
Configurar[30], bloquear e desbloquear PCs	**X**	**X**
Eliminar os registos da aplicação	**X**	

[29] A conta de administração embutida, é uma salvaguarda ao acesso à aplicação caso tenham sido eliminados todos os administradores.
[30] Selecionar o(s) tipo(s) de bloqueio que a aplicação vai forçar.

Os parâmetros de bloqueio que serão configuráveis são os sítios de internet ou intranet, os programas, os dispositivos USB e as contas de avaliação. Estas requerem que haja uma forma mais amigável de associação, pois o memorizar de determinado endereço eletrónico ou número de série de dispositivo USB não é nada funcional, assim, torna-se necessário implementar uma forma de fazer correlação entre o item afeto ao bloqueio e um nome facilmente percetível pelos utilizadores. A definição das contas de avaliação não pode passar só por atribuir um nome amigável, mas também por especificar a senha as elas associada. Antes de proceder ao bloqueio de determinado(s) computador(es), serão selecionados os itens de bloqueio através do seu nome amigável. Nessa altura será possível selecionar outros dois itens que não são objeto de configuração, pois trata-se da inibição da «Área de transferência» e da possibilidade de ejeção dos leitores de CD, DVD ou Blu-ray que não tem parâmetros configuráveis.

O bloqueio das máquinas dos formandos será feito através da rede, utilizando-a para lhes enviar os binários que posteriormente vão executar. Neste processo, terão de seguir também as credencias necessárias à execução dos binários na máquina de destino. Apenas um só ficheiro será enviado para execução, o qual pode vir a produzir, na máquina de destino, outros executáveis para que seja efetuado o bloqueio desejado. O ficheiro enviado para execução poderá ser designado de «Agente» e será este que irá afetar as máquinas, configurando-as para o bloqueio. Sempre que a natureza do bloqueio exigir a definição de permissões de execução a programas (aplicações instaladas na máquina remota), este agente irá produzir um novo binário e executá-lo com as credenciais indicadas para a tarefa. Se a natureza do bloqueio implicar a inibição dos dispositivos USB ou da «Área de transferência», o agente produzirá um outro binário que permanecerá em execução enquanto o bloqueio estiver efetivo. A razão da permanência da execução nestes dois casos é para, no primeiro, averiguar quais os dispositivos conectados para posterior inibição e, no segundo caso, para colocar um texto sugestivo do bloqueio na zona da memória pertencente ao utilizador, que está afeta ao «copiar» e «colar».

4.3 Desenvolvimento e Mecanismos de Controlo

Antes de proceder ao isolamento e bloqueio dos clientes, é necessário recolher informações acerca das suas configurações para posteriormente poder repô-los no seu estado original. A consola da Microsoft designada de «WMIC - *Windows Management Instrumentation Console*»

permite recolher essas informações[31]. Entre outras, é essencialmente necessário saber qual a «rota por omissão» (*default gateway*) de cada um dos clientes. À exceção de máquinas ou equipamentos específicos, presentemente são raras as redes informáticas locais (LAN) que não usam um servidor *Dynamic Host Configuration Protocol* (DHCP) para atribuir endereços IP. Este servidor pode ser integrado[32] com os servidores de resolução de nomes (DNS). A

Figura 41 – Problemas com a resolução de nomes

Figura 41 permite provar, que nas instalações da instituição a qual deu origem ao presente trabalho, em algumas ocasiões, como por exemplo, na ligação a ambiente de trabalho remoto, já se tinha constatado que ocasionalmente a resolução de nomes das máquinas remotas não devolve o endereço IP correto. Um simples *ping* a uma máquina na rede informa-nos que o IP respetivo termina em 19, no entanto, questionada a máquina com o IP terminado em 17, verifica-se que esta é a máquina que se pretende contactar. Devido à capacidade administrativa limitada, forçada pelas credenciais disponíveis, não foi possível determinar adequadamente a razão deste acontecimento.

Com a consola WMIC é possível certificar se a máquina contactada é de facto a máquina que se pretende contactar, pois o nome dessa máquina pode ser um dos valores devolvidos pelo cliente, evitando assim, que se proceda à configuração de uma máquina errada. A consola WMIC pode funcionar em modo interativo com a consola do sistema, o que faz com que aceite chamadas proferidas por *scripts* ou outras aplicações. É possível ainda com esta consola, utilizar credenciais diferentes para aceder a outras máquinas. Esta consola, chamada com os parâmetros «/NODE:"*máquina remota*"», «/USER:*utilizador*» e «/PASSWORD:*senha*», tal como mostra a Figura 42, consegue obter parte da informação necessária para se poder garantir colocar um cliente no seu estado original. Nesse exemplo, a máquina alvo é uma máquina com sistema

[31] https://blogs.technet.microsoft.com/askperf/2012/02/17/useful-wmic-queries/
[32] https://social.technet.microsoft.com/wiki/contents/articles/51810.windows-server-integration-between-dns-and-dhcp.aspx

operativo (SO) *Windows XP* que tem credenciais de administração diferentes das da máquina que está a fazer o pedido. Nestes sistemas é necessário, alterar o registo «forceguest» dentro da chave «HKLM\SYSTEM\CurrentControlSet\Control\Lsa» de «1» para «0»[33]. A aplicação concebida está destinada a operar em SO *Windows 7* e posterior, portanto, não vai ser necessário definir este registo.

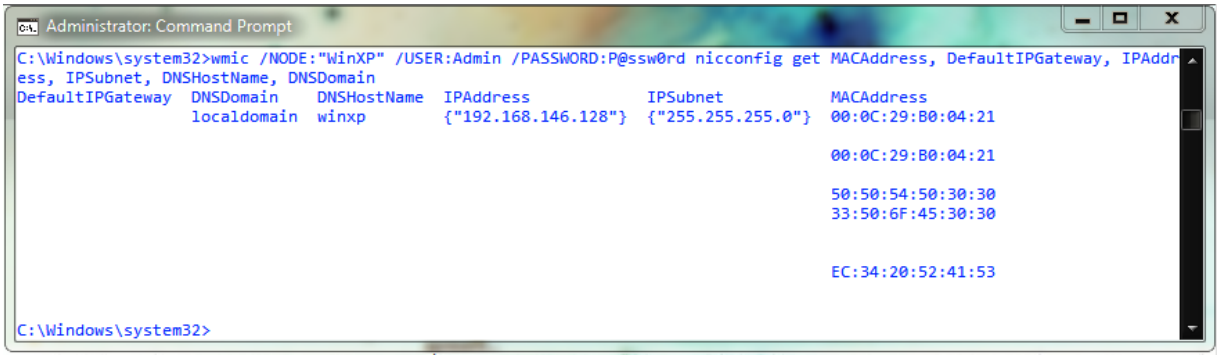

Figura 42 – Exemplo de utilização da consola WMIC

Existindo um meio de comunicação, torna-se necessário definir a forma de comunicação entre a máquina central e as máquinas cliente. Para conseguir este feito, tendo em conta que estes clientes poderão não partilhar as credenciais da máquina central e o facto de ser necessário iniciar e executar código nos clientes, foi decidido que a utilização da ferramenta «PsExec» da Sysinternals, identificada em 2.6, seria a mais adequada. A referida ferramenta, que o autor garante que funciona com os SOs Windows Vista e posterior[34] e que através de experiências efetuadas, também é capaz de operar corretamente com o SO Windows XP, até permite executar código numa sessão de utilizador específica no destino. No entanto, existem determinadas restrições que dificultam a sua utilização. A *firewall* da máquina remota é um aspeto problemático para o sucesso da ação, pois se esta estiver ativa, a ferramenta não consegue cumprir a sua função independentemente das credenciais utilizadas. A utilização desta ferramenta é bastante simples e versátil, no entanto, após experiências efetuadas, verificou-se que, em alguns casos, a ferramenta terminava devolvendo a informação de que não foi possível iniciar o serviço «PCEXESVC» no cliente, e, em outros casos, que houve dificuldades em estabelecer o contacto com a máquina alvo, tal como relatado na Tabela 4.

[33] https://support.solarwinds.com/Success_Center/Patch_Manager/Knowledgebase_Articles/How_to_enable_WMI_connections_to_Windows_XP_clients_installed_in_a_Workgroup

[34] https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

Tabela 4 – Relação de privilégio/sucesso da ferramenta «PsExec»

Máquina executante do psExec / Previlégios da conta executante	Membro de domínio A.D.		*Standalone*	
	Destino membro do domínio A.D.	Destino *Standalone*	Destino membro do domínio A.D.	Destino *Standalone*
Com previlégios de administração	Sucesso	Falha (acesso)	Sucesso	Falha (acesso)
Sem previlégios de administração	Falha (serviço)	Falha (acesso)	Sucesso	Falha (acesso)

Observando a tabela anterior, consegue-se distinguir três tipos de resultados. O primeiro é o de sucesso, os restantes dois manifestam-se nas situações onde ocorre uma falha. Estes dois problemas identificados são quando a máquina remota nega o funcionamento da ferramenta, quer na execução do serviço, quer no acesso mesmo quando são fornecidas credenciais com privilégios de administração. A Figura 43 mostra um caso onde a execução do serviço no cliente é negada.

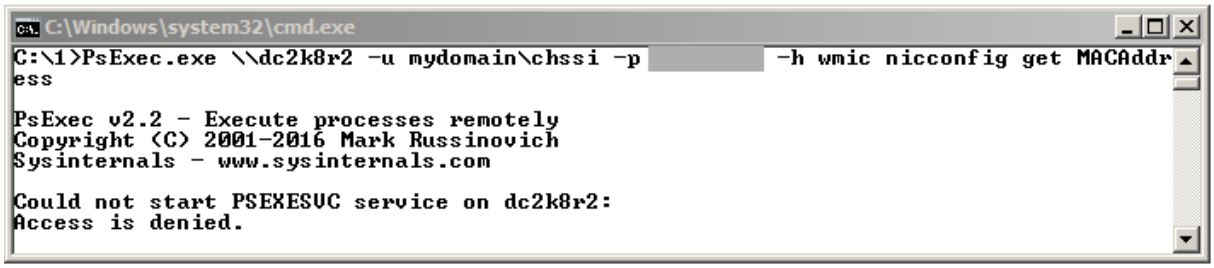

Figura 43 – Falha na execução do serviço da ferramenta «PsExec»

A solução para este caso é muito simples, passa apenas por executar o comando no modo privilegiado, o que no exemplo apresentado pela Figura 44, traduz-se na execução «como administrador» da consola.

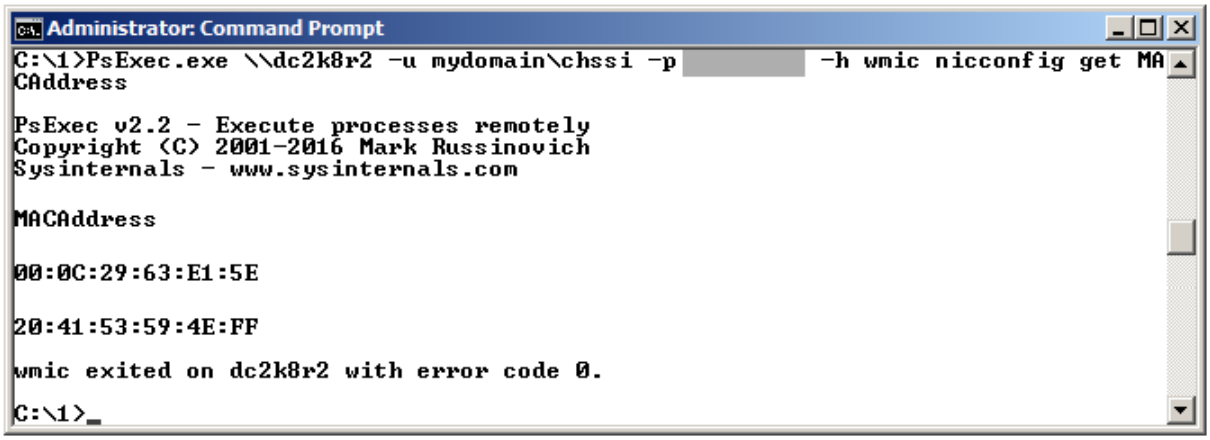

Figura 44 – Sucesso na obtenção de resultados com a ferramenta «PsExec»

A Figura 45 apresenta um caso onde o acesso é negado mesmo sendo o comando executado localmente com credenciais administrativas e forçada a utilização de credenciais do mesmo tipo do lado do cliente. Quando o parâmetro «-h» é definido na linha de comandos, instrói a ferramenta a executar a tarefa no cliente em modo privilegiado. A solução para estes casos, passa por acrescentar uma entrada no registo do sistema.

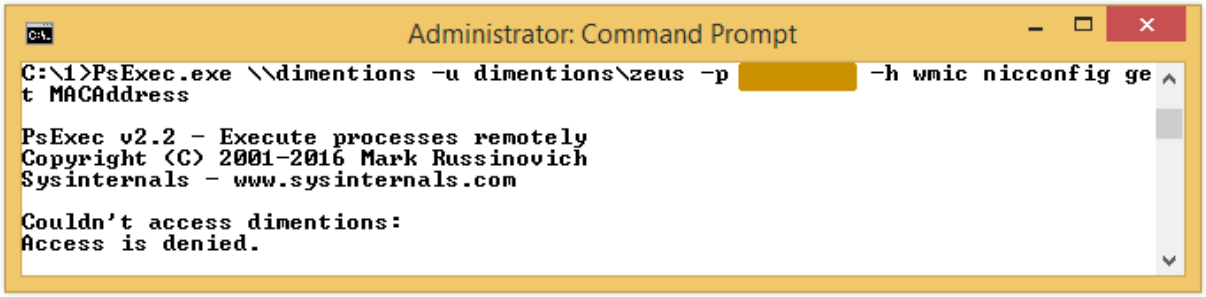

Figura 45 – Negação de acesso à ferramenta «PsExec» pelo cliente

O registo «LocalAccountTokenFilterPolicy» do tipo *DWORD* definido com o valor «1»[35] na chave «HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System» permite que seja gerado um *token* de acesso com privilégio elevado. Este registo não está criado por omissão e terá de ser criado manualmente no cliente. Esta alteração produz efeito imediato, não sendo necessário reiniciar o sistema.

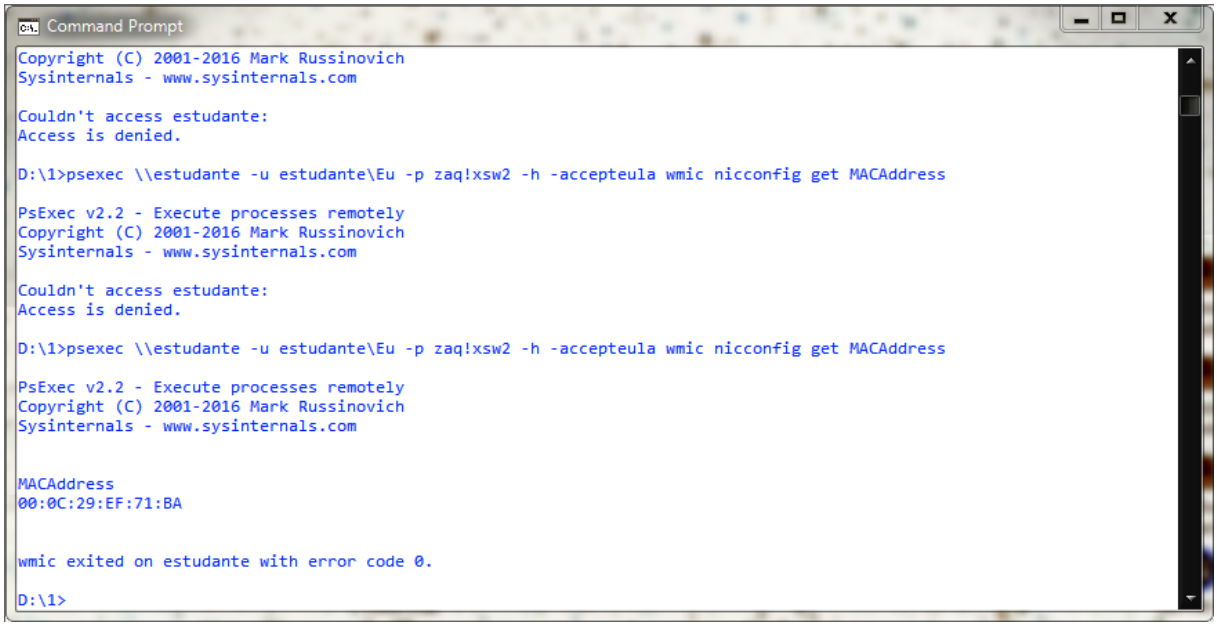

Figura 46 – Resultado da execução da ferramenta «PsExec» após modificação do registo

[35] https://support.microsoft.com/en-us/help/947232/error-message-when-you-try-to-access-an-administrative-share-on-a-wind

Observando a Figura 46, que ilustra os resultados antes e após a configuração deste registo, consegue-se constatar que esta configuração efetivamente produz resultado mesmo que a conta utilizada localmente não seja de administração. Esta ferramenta existe em duas arquiteturas, a de 32 e de 64-bit. Enquanto que a de 64-bit só funciona em sistemas de 64-bit, a de 32-bit funciona em ambos.

Ao ter em conta que é necessário efetuar algumas alterações ao sistema operativo dos clientes e tendo presente o facto que um dos objetivos é a simplicidade de utilização, torna-se necessário guardar em disco local as credenciais com os privilégios necessários para executar as ditas alterações. Guardar as credenciais em disco local, é justificado ao mesmo tempo pela permanente disponibilidade das mesmas e pelo facto de não carecer de custos, mas por outro lado, torna-se numa situação que exige cuidados acrescidos. Estas credenciais têm de ser adequadamente protegidas para que não possam ser obtidas por terceiros, mas de forma a manter a capacidade de retenção das senhas utilizadas. O recurso a *hash* para guardar estas senhas, neste caso, não é funcional, uma vez que as ferramentas utilizadas só aceitam as senhas *em claro*. Assim, é necessário utilizar um algoritmo de cifragem robusto o suficiente para proteger adequadamente tais credenciais. O algoritmo que se adapta melhor a esta tarefa tem como base de funcionamento a utilização de uma chave simétrica. O algoritmo AES[20] de 256-bit é a escolha adequada visto que só é necessário cifrar as senhas das contas registadas. A aplicação tem também de guardar as configurações das máquinas e da própria aplicação, embora já não contendo dados sensíveis, é sempre boa prática não guardar nada *em claro*. Observando outro dos requisitos, que dita que a aplicação deve ser o menos pesada possível e tendo em conta que um algoritmo de cifragem é exigente para com o processador, será idealizado um algoritmo próprio para esta ação descartando o facto de ser desaconselhado.

Segundo os requisitos estabelecidos, a aplicação tem de conseguir restringir a sua utilização a docentes ou administradores, o que obriga a identificação prévia dos utilizadores na aplicação. No sentido de facilitar a vida ao administrador da aplicação na identificação dos docentes, o *software* será capaz de enumerar e apresentar as contas de utilizador existentes no sistema. Num computador a executar um sistema operativo Microsoft Windows, a classe *WMI* designada de «Win32_Account»[36] possui informação acerca de contas de utilizador e de grupo. Quatro das propriedades desta classe são «LocalAccount», «SID», «SIDType» e «Status». A primeira

[36] https://docs.microsoft.com/en-us/windows/desktop/cimwin32prov/win32-account

contém o valor «True» ou «False» caso se trate respetivamente de uma conta local ou de domínio. A propriedade «SID» contém a sequência de carateres que identificam inequivocamente a conta. Desta sequência consegue-se saber, entre outras informações, se se trata de uma conta de utilizador ou de grupo. A propriedade «SIDType» contém um caractere numérico que identifica o tipo do objeto, tal como relata a Tabela 5.

Tabela 5 – Relação dos código do «SIDType»

SIDTYPE	1	2	3	4	5	6	7	8	9
DESIGNAÇÃO	*User*	*Group*	*Domain*	*Alias*	*WellKnownGroup*	*DeletedAccount*	*Invalid*	*Unknown*	*Computer*

Por último, a propriedade «Status» contém texto que traduz o estado da conta. O texto «OK» significa que a conta está em condições de utilização e «Degraded» significa que não está, como por exemplo, se estiver desativada.

4.3.1 Área de transferência

Existem duas formas óbvias de restringir a utilização da «Área de transferência», uma passa por impedir que se coloque ou retire de lá informação, a outra passa por inutilizar a informação que lá se encontra. Foram efetuadas algumas tentativas de inibição de utilização da «Área de transferência» pelo método de impedir a colocação e extração de informação. Estas tentativas provaram ser ineficazes. Olhando ao método de inutilização da informação e tendo em conta que a «Área de transferência» não é partilhada de sessão para sessão, é fácil compreender que este método requer que seja executado código na sessão de utilizador que se pretende afetar. Assim, um simples pedaço de código que temporariamente vá limpando esta zona de memória, consegue ser bastante eficaz mesmo sem consumir recursos significativos da máquina. Ao colocar código a correr na sessão do utilizador alvo do bloqueio, suscita um problema pois este pode terminar a tarefa e assim recuperar o acesso à memória. Sempre que se pretende então isolar a «Área de transferência» desta forma, torna-se necessário impedir que o utilizador tenha acesso ao «Gestor de Tarefas» ou a outro utilitário capaz de terminar processos no sistema. A escolha foi feita optando por esta segunda forma, por ser eficaz e até permitir dar a conhecer ao utilizador que a sua «Área de transferência» foi bloqueada, isto é, colocando de texto informativo do facto, nessa zona da memória. Esta escolha obriga à identificação das sessões ativas na máquina a bloquear, o que é possível graças ao comando «`quser`» presente nos sistemas operativos da Microsoft. Observando a Figura 47, pode ver-se que, no exemplo apresentado, existem três sessões iniciadas estando uma delas ativa na consola e as restantes a

correr em segundo plano. Pode também ser observado o número de identificação dessas sessões. Este número é necessário para que conjugado com o parâmetro «-i» dos comandos enviados à ferramenta «PsExec», se consiga executar o código pretendido nessa sessão.

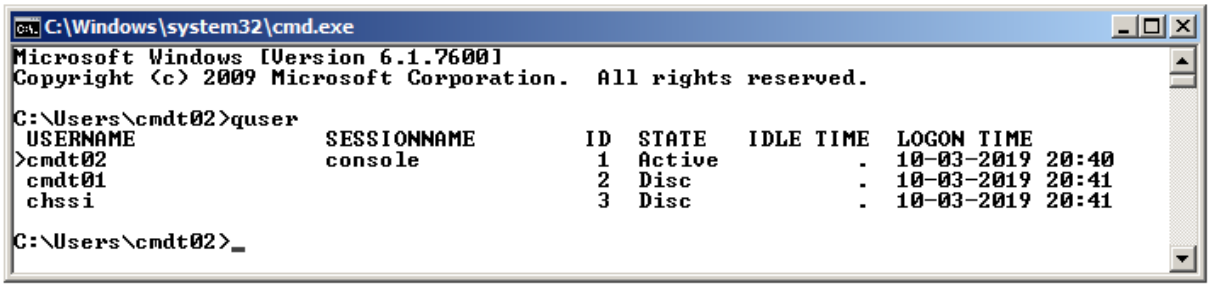

Figura 47 – Resultado da execução do comando «quser»

4.3.2 Dispositivos externos de armazenamento de dados

O sistema operativo (SO) Windows traz incluído no «*Registry*» uma chave que mediante o seu valor impede a iniciação de dispositivos de armazenamento de dados de ligação USB. Esta forma é muito rudimentar pois contempla as seguintes fragilidades:

a) Apenas impede que o equipamento seja inicializado – equipamentos já inicializados continuam a funcionar;
b) Não permite inibir equipamentos seletos;
c) Ao introduzir um equipamento que ainda não esteja instalado no sistema, o SO desativa automaticamente esta forma de inibição e todos os dispositivos daí em diante passam imediatamente a funcionar.

A solução mais robusta e eficaz é, sem sombra de dúvida, a utilização do utilitário «USBDeview» da «Nirsoft». Para funcionamento da aplicação «PC Border», esta é a solução que foi adotada na inibição de utilização deste tipo de dispositivos.

4.3.3 Unidades de discos óticos (CD, DVD e Blu-Ray)

Nos Sistemas Operativos Windows, as unidades de discos óticos utilizam uma letra ou mapeamento para uma pasta localizada em disco formatado em NTFS (*New Technology File System*) para mapear o seu acesso, tal como nas unidades de disco rígido ou de armazenamento externo. Uma forma de impedir a utilização deste tipo de unidades, passa por retirar-lhes a letra de acesso. Se a letra de acesso for desmapeada, o utilizador deixa de ter um caminho para chegar aos ficheiros localizados num destes dispositivo apenas se não houver um mapeamento para

pasta NTFS. A capacidade existente de impedir a ejeção de discos óticos[37] apresenta-se como uma alternativa viável e versátil, pois permite que possam ser utilizados discos com conteúdo necessário aos testes enquanto impede a utilização deste meio com outro conteúdo. Alguns dos testes que irão usufruir da utilização da aplicação «PC Border» são de língua estrangeira, onde a interpretação auditiva é um fator de avaliação. Ao garantir que os discos óticos contendo o conteúdo de audição não podem ser removidos do leitor, alivia de certa forma a preocupação dos responsáveis pela vigilância dos testes e permite cumprir dois objetivos com uma só ação.

4.3.4 Programas

A inibição ou definição de programas passa por manipular as configurações existentes no «*Registry*» do Windows. Só uma conta com privilégios suficientes pode efetuar alterações deste tipo. Visto ser necessário efetuar alterações desta natureza utilizando as contas de avaliação, é necessário atribuir temporariamente as permissões necessárias a essas contas. As contas de serviço definidas na configuração da aplicação são usadas para este fim. É com as contas de serviço que se torna possível atribuir permissões às contas de avaliação, permitindo-lhes manipular as configurações necessárias no «*Registry*». Esta ação é exigida sempre que seja utilizada a opção de bloqueio de programas, bem como, quando se pretende bloquear a «Área de transferência» que por sua vez necessita impedir a execução do «Gestor de tarefas».

4.3.5 Contas e *autologon*

Nas avaliações, as contas a utilizar têm de estar identificadas, não só para que se possa executar operações relacionadas com a execução de programas, como também para definir quais as contas de utilizador que terão capacidade de iniciar sessão na máquina. A aplicação irá criar um ficheiro *batch* que correrá aquando o início de sessão. O código presente neste ficheiro irá ordenar o término imediato da sessão, caso a conta utilizada não seja uma das que estão autorizadas. O sistema operativo Microsoft Windows possui a capacidade de executar o início de sessão automático[38], ou seja, sem intervenção humana, mesmo que a conta a iniciar tenha uma senha associada. Para que isto aconteça, basta definir alguns valores no «Registry». Dentro da chave «HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon», cinco são os valores que necessitam ser configurados, sendo eles, «DefaultDomainName»,

[37] https://msdn.microsoft.com/en-us/library/windows/desktop/aa364575(v=vs.85).aspx
[38] https://docs.microsoft.com/en-us/windows-hardware/customize/desktop/unattend/microsoft-windows-shell-setup-autologon

«DefaultUsername», «DefaultPassword», «AutoLogonCount» e «AutoAdminLogon». A Tabela 6 indica qual o tipo de valor, a informação que pode conter e qual a função de cada valor.

Tabela 6 – Valores para definição de «Autologon»

NOME DO VALOR	TIPO DE VALOR	VALOR POSSÍVEL	DESIGNAÇÃO
AUTOADMINLOGON	Texto	0 – Inativo 1 – Ativo	Define se o início automático de sessão está ativo ou não
AUTOLOGONCOUNT	DWORD	Número inteiro >= 0	Define o número restante de inícios automáticos a que o sistema vai executar
DEFAULTDOMAINNAME	Texto	FQDN	Define o nome do domínio da conta a iniciar
DEFAULTUSERNAME	Texto	Texto alfanumérico	Define a conta a iniciar
DEFAULTPASSWORD	Texto	Qualquer	Define a senha da conta a iniciar

4.3.6 Controlo dos acessos à rede

Restringir os acessos de rede ao meio exterior é uma tarefa que tem de ser atacada em duas frentes. É necessário impedir o tráfego destinado à *default gateway* (GW) e o tráfego destinado à mesma rede. Impedir que o tráfego que normalmente é enviado para a GW é fácil, bastando para isso remover a «rota por omissão». Quando se trata de restringir o acesso a determinado destino dentro da mesma rede, o processo complica um pouco, pois este tráfego é encaminhado diretamente pela 2ª camada do protocolo TCP/IP. Neste caso, para impedir o acesso a qualquer destino, é necessário manipular o sistema de forma a que ele não questione a rede acerca da localização desse destino. Se a informação acerca de um destino já se encontrar na tabela de endereços do sistema, esta será aproveitada. Ao definir no sistema informação errada relativa aos destinos, consegue fazer-se com que o tráfego não seja encaminhado para o destino pretendido. Esta forma de atacar o problema não é totalmente segura, pois se houver um destino exterior que inicie comunicação com a máquina adulterada, esta vai corrigir a informação errónea existente e a máquina passa a poder comunicar com esse destino. Esta foi a solução encontrada para não necessitar interagir com a *firewall* do próprio sistema. Após a máquina estar isolada, é adicionada a informação correta acerca dos destinos autorizados, ou seja, os MAC-Address são corretamente definidos para os destinos que se encontram na mesma rede e, é adicionada à tabela de encaminhamento, uma rota estática com indicação da GW por cada destino permitido.

A Tabela 7 apresenta uma síntese de todos os valores e chaves do registo que estão sujeitos a intervenções pela aplicação, pois são essenciais para obter sucesso no seu funcionamento.

Tabela 7 – Identificação dos valores de registo sujeitos a alteração

CHAVE DE REGISTO	VALOR	PROPÓSITO
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	AutoAdminLogon	Indicar se o início de sessão automático está ativo
	AutoLogonCount	Definir o número de inícios de sessão automáticos restantes
	DefaultDomainName	Definir o nome do domínio da conta a utilizar
	DefaultUserName	Definir o nome de utilizador da conta a utilizar
	DefaultPassword	Definir a senha da conta a utilizar
HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\System	LocalAccountToken FilterPolicy	Permitir que seja gerado um *token* de acesso com privilégio elevado
HKCU\Software\Microsoft\Windows\ CurrentVersion\Policies\Explorer	DisallowRun	Indicar ao sistema que existem aplicações que não estão autorizadas a executar
	RestrictRun	Indicar ao sistema que existem aplicações que estão autorizadas a executar
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun	1, 2, …, n	Identificar as aplicações impedidas de executar
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun	1, 2, …, n	Identificar as aplicações autorizadas a executar

4.4 Obstáculos encontrados

Na elaboração da aplicação «PC Border», vários testes tiveram de ser efetuados e obstáculos ultrapassados. A inibição do funcionamento dos equipamentos USB passou inicialmente por implementar a negação de acesso aos ficheiros responsáveis pelo seu correto funcionamento manipulando, para tal, as permissões NTFS. Se as permissões de leitura forem negadas à conta do utilizador e à conta do sistema, este fica incapaz de saber como comunicar com o equipamento, efetivando assim o bloqueio. Esta opção, no entanto, provou apresentar quatro problemas, que são:

a) Não funciona em sistemas cuja formatação do disco de sistema não seja NTFS;
b) Não permite o bloqueio seletivo dos equipamentos;
c) Pelo menos o Sistema Operativo Windows 10, não permite que sejam alteradas as permissões dos ficheiros inclusos nas pastas «Windows\System32» e «Windows\inf», quer através de linha de comandos, quer através de procedimentos implementados pela *framework* Microsoft .net. Este facto impede a manipulação desejada das permissões dos ficheiros «usbstor.*»;
d) Um equipamento já conectado continua em funcionamento.

Outra dificuldade enfrentada foi a que surgiu durante a tentativa de impedimento de utilização da «Área de transferência». Inicialmente, o método adotado foi de impedir todas as formas de aceder a esta zona de memória, desabilitando, entre outras, a conjugação das teclas «CTRL + C» e «CTRL + V» e impedindo o acesso a estas opções nos menus do sistema e das aplicações. A realidade, no entanto, é que não é possível prever todas as aplicações com capacidade de acesso à «Área de transferência», logo este método seria ineficaz. O melhor procedimento passa, assim, por inutilizar quaisquer dados encontrados nesta parte da memória, o que obriga a uma permanente consulta e alteração do que se lá possa encontrar. Esta opção exige a criação de uma aplicação dedicada para o efeito capaz de permanecer em execução apenas enquanto o bloqueio estiver em efeito e, visto a «Área de transferência» ser individual e intransmissível, tem de ser executada no perfil de cada utilizador a bloquear.

A ferramenta «PsExec» embora sendo um poderoso apetrecho dos administradores de sistemas, não conjuga bem com a classe «Process» da API (*Application Programming Interface*) «System.Diagnostics». Quando chamada por esta classe, só é possível aproveitar praticamente uma linha do *output* produzido pela tarefa executada e redirecionada para a referida classe. Foi possível dar volta a esta situação, certificando que todo o *output* da tarefa executada seja concatenado com caracteres delimitadores de forma a que constitua uma só linha de saída.

A aplicação foi testada numa infraestrutura onde a sua dimensão justifica a utilização de mais de 50 controladores de domínio e um número equivalente de servidores de DNS. Devido à extensão da AD, a aplicação perdia desempenho ao executar tarefas específicas relacionadas com a obtenção e tratamento de contas de utilizador e grupos de segurança, enquanto fazia *queries* WMI. Foi possível observar que esta operação demorava cerca de 11 minutos ao ser executada num PC com processador intel dual-core@3.0GHz e 8GB de RAM. O código foi refeito de forma a utilizar os identificadores de segurança *Windows SID* para obter o resultado pretendido. Após esta alteração de código, o processo passou a demorar 20 segundos em média.

4.4.1 Acesso à Internet

A utilização de servidores de proxy para aceder a determinados endereços na *web*, causa um transtorno significativo, na medida em que todos os pedidos de acesso à internet têm como alvo o este servidor. Quem efetivamente estabelece contacto com o destino é o servidor de proxy, que posteriormente devolve o tráfego ao cliente. O cliente nem necessita saber qual o IP do site a contactar. Nesta situação, embora os pedidos com destino na intranet não sejam afetados,

torna-se impossível restringir o acesso a um número finito de destinos na internet, sendo que, ou são todos permitidos ou todos negados. Existem pelo menos três formas de resolver esta situação, no entanto, cada uma tem as suas imposições:

a) Instalação de um *router* adicional. – Esta opção exige a instalação de um equipamento extra, o qual terá de ter acesso à mesma rede externa que o servidor *proxy* tem. Esta solução permite à aplicação «PC Border» controlar os destinos diretamente pelo IP de destino, no entanto, abre portas à utilização indevida e incontrolada da internet por parte de terceiros que conheçam este router, bem como, a todos os aspetos de segurança que causa;
b) Instalação de um servidor *proxy* adicional. – Esta opção também exige mais um equipamento e acesso à rede externa que tem acesso direto à internet. Esta solução tem um ponto a favor e outro contra. Com esta solução, que não é controlada pelos administradores centrais, é possível garantir que a utilização da internet está limitada a um grupo definido de endereços. Por outro lado, não permite à aplicação definir seletivamente quais os endereços predefinidos que estarão acessíveis, voltado à situação de se ter acesso a todos ou a nenhum;
c) Interação com a *firewall* do sistema operativo. – Esta opção implica a alteração das políticas de segurança estabelecidas pela instituição. Além de estar sujeito à autorização para implementação, pode não ser concebível pois a *firewall* dos PCs já está a ser controlada pelo antivírus. A implementação desta opção pode acarretar outras consequências na eventualidade de um destes PCs ser infetado por algum tipo de *malware*, pois a responsabilidade pela infeção pode ser posta em causa especialmente se houver custos associados.

A primeira opção aparenta ser a mais viável para incluir na próxima versão do «PC Border» desde que, seja possível garantir que todos os PCs sujeitos à manipulação por parte desta aplicação estejam, ligados a segmentos de rede exclusivos e que sejam definidas listas de controlo de acessos a estes segmentos (ACL) no router em questão.

4.4.2 Limitações do sistema

Durante a construção da aplicação, foram sentidas algumas dificuldades na implementação dos objetivos. A primeira limitação do sistema a contornar, prende-se com a execução de tarefas utilizando credenciais diferentes das do utilizador que está a correr a aplicação. Sendo

necessário que estas tarefas corram independentemente dos privilégios constantes da conta do utilizador, a API (*Application Programming Interface*) «System.Diagnostics» da *framework* .NET, que inclui uma classe designada de «Process»[39], permite esse feito. Esta classe contém alguns parâmetros de configuração, sendo que os fundamentais são:

- **WindowStyle** – define como a janela da tarefa a executar é apresentada. As opções são «Maximized», «Normal», «Minimized» e «Hidden». Esta última é especialmente útil, pois permite abstrair o utilizador das tarefas que a aplicação tem de executar. Para que funcione, é, no entanto, necessário que o parâmetro «UseShellExecute» [40] esteja definido como «Verdadeiro».
- **CreateNoWindow** – define se a tarefa a executar é executada sem janela nova para a conter[41]. A sua atividade está limitada ao parâmetro «UseShellExecute» estar definido como «Falso» e aos parâmetros «UserName» e «Password» serem nulos.
- **RedirectStandardOutput** – faz com que o *output* da tarefa executada seja encaminhado para a aplicação de modo a permitir o seu processamento. Os testes efetuados revelaram que, quando a tarefa a executar é a ferramenta «PsExec», existe um número limitado de linhas de texto que que são redirecionadas para a aplicação.
- **UserName** – define o nome de utilizador das credenciais que se pretende utilizar.
- **Domain** – define o nome do domínio de *Active Directory* ou da máquina local referente às credenciais a utilizar.
- **Password** – É um parâmetro do tipo «SecureString» onde é definido de forma segura a senha das credenciais a utilizar.
- **WorkingDirectory** – permite definir qual a pasta de trabalho da tarefa a criar. Se não for definido, o sistema usa a pasta «%SYSTEMROOT%\system32» cujo acesso depende dos privilégios atribuídos à conta de quem está a utilizar a aplicação. Este parâmetro funciona em conjunto com o «UseShellExecute» que tem de ser definido como «Falso»[42] para que possa ser utilizado.

Visto que, em alguns casos, o parâmetro «WorkingDirectory» necessita ser definido, o que obriga que o «UseShellExecute» seja configurado como «Falso». Tal impede a ação do

[39] https://docs.microsoft.com/en-us/dotnet/api/system.diagnostics.process?view=netframework-4.5
[40] https://docs.microsoft.com/en-us/dotnet/api/system.diagnostics.processstartinfo.useshellexecute?view=netframework-4.5
[41] https://docs.microsoft.com/en-us/dotnet/api/system.diagnostics.processstartinfo.createnowindow?view=netframework-4.5
[42] https://docs.microsoft.com/en-us/dotnet/api/system.diagnostics.processstartinfo.workingdirectory?view=netframework-4.5

parâmetro «WindowStyle», o que pode vir a tornar visível a janela da tarefa a executar. Visto ainda que a utilização do parâmetro «CreateNoWindow» requer que não sejam definidas credenciais, faz com que a API seja incapaz de abstrair o utilizador das tarefas executadas em segundo plano, as quais são necessárias ao funcionamento da aplicação.

A *framework* .NET já vem pré-instalada[43] nos sistemas operativos (SO) da Microsoft. Cada lançamento de SO pode incluir uma versão diferente desta *framework*. A maior diferença nota-se quando se compara o Windows 7 e o Windows 8, o que constitui outra limitação do sistema. O primeiro inclui a versão 3.5.1 que, por sua vez, contempla as versões 2.0, 3.0 e 3.5 da *framework*. Existe a versão 4.5[44] para este SO, mas terá de ser instalada manualmente. Em contrapartida, o Windows 8 traz pré-instalada apenas a versão 4.5 que não inclui nenhuma das versões anteriores, embora seja possível adicioná-las posteriormente. Qualquer aplicação a conceber depende de uma versão específica para funcionar, e visto que as versões 2.0, 3.0 e 3.5 apenas estão pré-instaladas no Windows 7, bem como, a versão 4.5 apenas no Windows 8 e posterior, não existe uma versão .NET comum a todos os SO sobre os quais a aplicação tem de funcionar. Posto este dilema, optou-se por orientar a aplicação para a versão 2.0 da *framework* para SO inferiores ou iguais ao Windows 7, e para a versão 4.5 para SO iguais ou superiores ao Windows 8. A Figura 48 mostra-nos o resultado da tentativa de remotamente ordenar a execução do agente numa máquina com SO Windows 10 caso a aplicação apenas tivesse como alvo a versão 2.0 da *framework*.

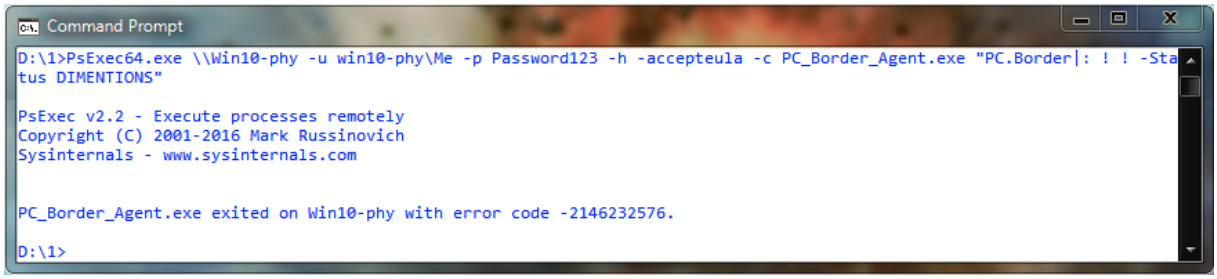

Figura 48 – Conflito de versão .NET *framework*

A Figura 49 exibe o resultado de manualmente executar o agente na máquina destino nas mesmas condições – O sistema deteta que a aplicação (agente) requer a versão 2.0 da *framework* .NET e oferece-se para a instalar.

[43] https://blogs.msdn.microsoft.com/astebner/2007/03/14/mailbag-what-version-of-the-net-framework-is-included-in-what-version-of-the-os/
[44] https://www.microsoft.com/en-us/download/details.aspx?id=30653

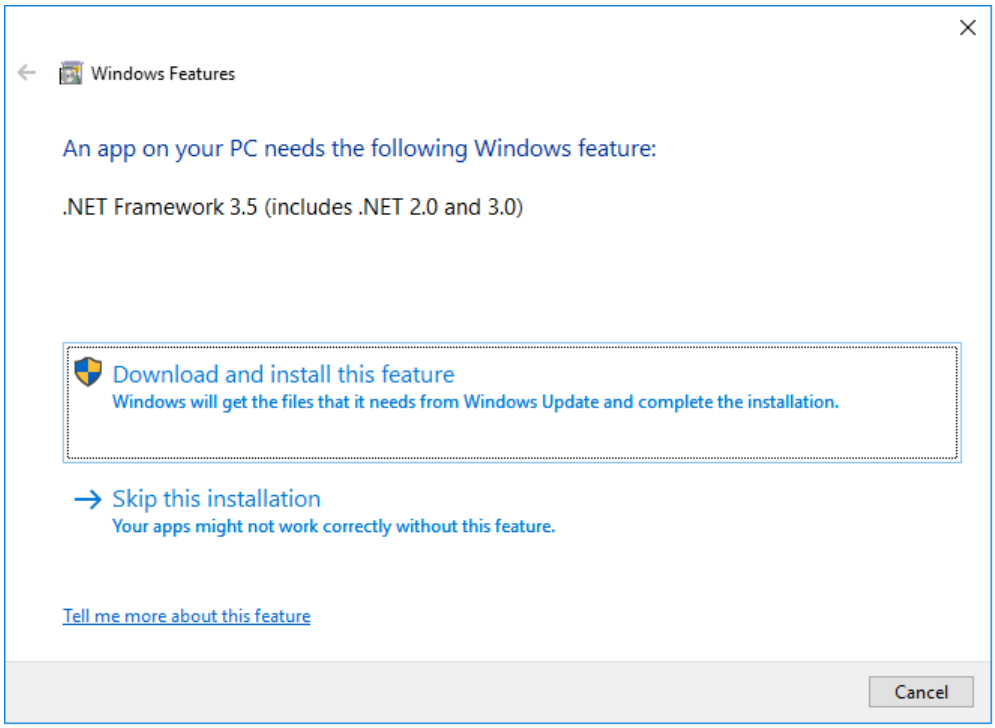

Figura 49 – Caixa de diálogo após conflito de versão .NET *framework*

Este método automático de instalação da referida *framework*, requer uma ligação à internet, tal como, o método manual via assistente identificado pela Figura 50.

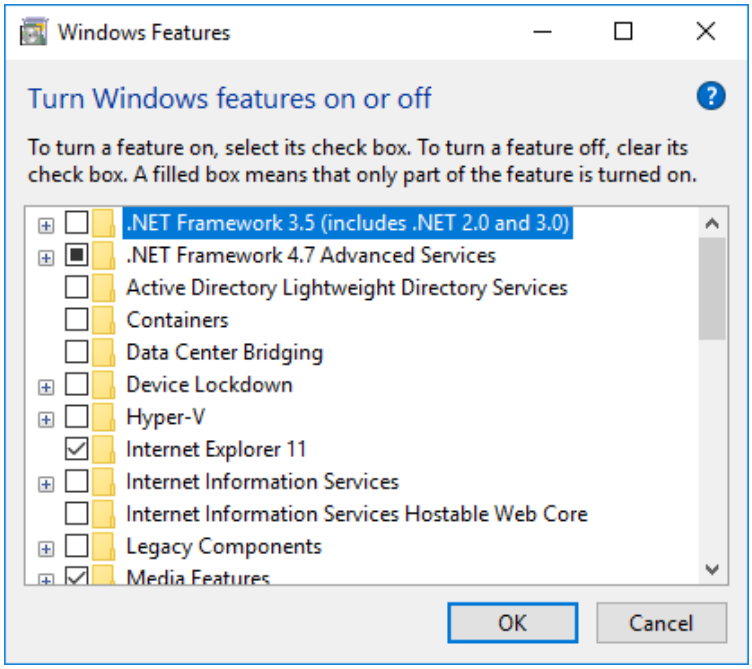

Figura 50 – Método manual de instalação da framework .NET 4.5 em Windows 10

Esta *framework* pode ser instalada manualmente através de linha de comandos redigida numa consola de Administração com o comando «`Dism /online /enable-feature /featurename:NetFx3`

`/All /Source:F:\sources\sxs /LimitAccess`» onde «F:» indica a unidade onde se encontra o DVD ou PEN USB com a instalação do sistema operativo.

A utilização da *framework* versão 4.5, apresenta-nos outro problema que se manifesta nos SO de 64-bit. Ao aceder à *registry* de um sistema destes em modo de 32-bit, os valores acedidos pertencem à secção «Wow6432Node» que não surtem o resultado pretendido. Para resolver esta situação, é necessário certificar que as opções de compilação no IDE incluem «Qualquer CPU» como plataforma de destino e que não está selecionado a opção «Preferir 32-bit» para que a aplicação corra no modo de 64-bit onde possível.

4.5 Produto final

Um objetivo imposto é que a aplicação possa ser executada em qualquer dos sistemas operativos suportados, sem configurações ou adaptações específicas para o permitir. Assim, a aplicação é apenas constituída por um só ficheiro – o próprio executável.

No final, a aplicação ganhou forma. A Figura 51 apresenta a janela principal da aplicação com uma lista de PCs ativa, a qual é designada de «GrupoTrabalho». A esta lista pertencem 3 PCs (clientes) com os nomes «Win10», «winxp» e «Win8». Durante o seu desenvolvimento, surgiu a necessidade de efetuar algumas alterações em relação aos esboços traçados e identificados nos Casos de Uso (*Use Cases*). Estas alterações, maioritariamente implementadas na janela principal da aplicação, são de natureza puramente cosmética e com objetivo de melhorar o aspeto visual da mesma.

Figura 51 – Janela príncipal da aplicação «PC Border»

4.5.1 Pré-requisitos de *software*

Os pré-requisitos ao funcionamento do *software* são dois. O primeiro é que os sistemas operativos das máquinas do formador e dos formandos (clientes) sejam suportados tal como mencionado na alínea g) dos *Requisitos de Utilizador*. O segundo é que a *framework* .NET esteja instalada nessas máquinas. As máquinas cliente apenas necessitam da versão 2.0 caso operem o Windows 7 ou da versão 4.5, caso estejam munidas de sistema operativo Windows 8 ou posterior. A máquina do formador onde a aplicação vai correr, independentemente da versão do seu sistema operativo, necessita da versão 4.5. Esta exigência deve-se ao facto de as versões anteriores não permitirem operar com ficheiros comprimidos (ZIP).

4.5.2 Composição da aplicação

Não contando com os pré-requisitos, o executável da aplicação possui todo o conteúdo necessário para que possa funcionar e cumprir a sua missão. No seu funcionamento e à medida que é necessário, a aplicação extrai os binários essenciais ao cumprimento da tarefa em execução. Um dos binários incluídos na aplicação é o «Agente». Devido ao facto deste agente ocupar um pouco mais de 6 MB, surgiu a necessidade de o comprimir. Após compressão, que o reduziu para 10 por cento do seu tamanho original, advém a necessidade de operar com ficheiros comprimidos e por conveniência, a utilização de ficheiros «ZIP». Surgiu a hipótese de o antivírus interferir com o processo de descompressão, algo que não se verificou nem com o «Defender», nem com o «Bitdefender» nem ainda com o «Norton Security». A aplicação no seu total ficou então um pouco aquém de 12 MB.

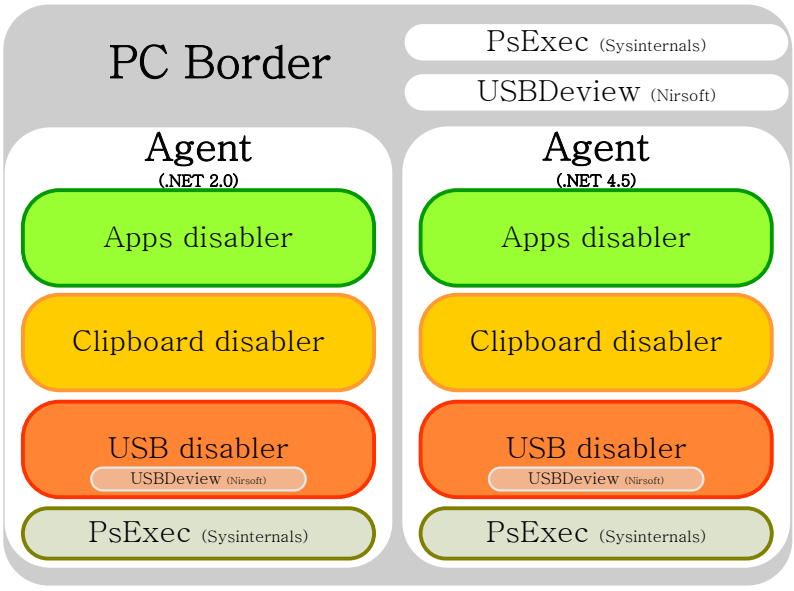

Figura 52 – Representação da constituição da aplicação

Na Figura 52 é possível observar que embutidos na aplicação, estão o «Agente», a ferramenta «PsExec» e o utilitário «USBDeview». O agente por si contém três binários que têm tarefas específicas ao bloqueio dos clientes, e ainda, uma cópia da ferramenta «PsExec». É possível observar também que um dos binários existentes no referido agente, e que está designado por «USB disabler», contém ainda uma outra cópia do utilitário «USBDeview».

4.5.3 Funcionamento

Para além dos seus constituintes, descritos no ponto anterior, o executável da aplicação integra todo o interface gráfico para a necessária interação com o utilizador (docente ou administrador).

O utilitário «USBDeview» que está incluído na base da aplicação, é apenas extraído e utilizado caso o utilizador selecione o separador «Dispositivos» presente na configuração dos itens de bloqueio. A configuração dos itens de bloqueio é persistente, não sendo necessária esta ação cada vez que se pretender utilizar a aplicação. O utilitário extraído é necessário para que se possa adicionar dispositivos «USB» à lista dos equipamentos conhecidos. A passagem de informação do utilitário para a aplicação é feita por meio de um ficheiro «XML» que lista todos os dispositivos USB presentes no sistema. Terminada a sua utilização, o utilitário e o ficheiro por ele produzido são de imediato eliminados do sistema.

A ferramenta «PsExec» é extraída e utilizada sempre que a aplicação necessite comunicar com as máquinas cliente.

A extração, descompressão e execução do «Agente» são efetuadas sempre que a aplicação necessite determinar o estado dos clientes ou que seja ordenada a execução de uma ação de bloqueio. A criação de um agente que funciona desta forma vem ao encontro de um dos requisitos que dita que não deve existir código em execução permanente nos sistemas.

Na parte superior da Figura 53, está representado o funcionamento entre a aplicação e os clientes. A parte inferior da mesma figura representa o funcionamento do agente no cliente.

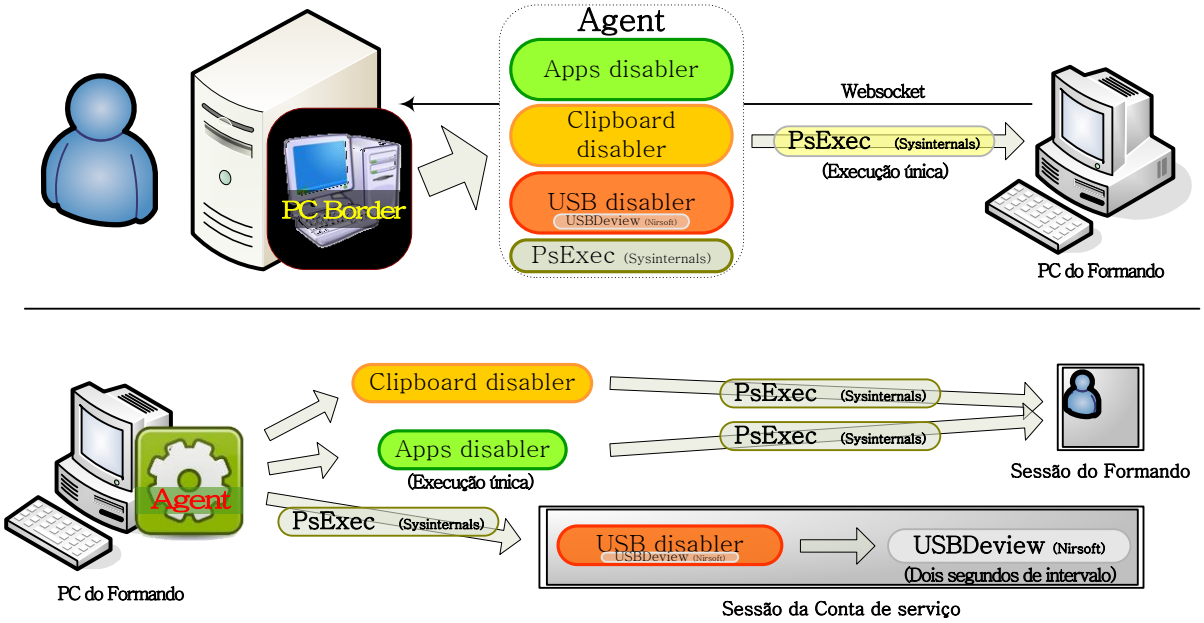

Figura 53 – Diagrama de funcionamento dos constituintes da aplicação

Do lado do cliente, o agente extrai e executa a ferramenta «PsExec» sempre que seja necessário agir sobre a «Área de transferência», autorizar ou negar o funcionamento de aplicações e na definição de dispositivos USB.

O componente do agente designado de «Clipboard disabler» é lançado pela ferramenta «PsExec» pois necessita ser executado na sessão do utilizador (conta de avaliação) e de forma independente do agente. Permanecerá em execução enquanto o bloqueio estiver ativo.

O componente designado de «Apps disabler» funciona alterando, no registo do sistema, valores específicos da conta do utilizador com sessão iniciada. É lançado também pelo «PsExec» para que possa ser executado na sessão indicada. Ao contrário do componente anterior, este é apenas executado uma vez por cada ordem invocada.

O último componente do agente designado de «USB disabler» é também lançado pelo «PsExec» pois tem de operar independentemente do agente. Operando na conta de serviço, este componente permanece em execução enquanto o bloqueio vigorar. Funciona lançando o utilitário «USBDeview» de dois em dois segundos para garantir que qualquer dispositivo de armazenamento USB, que não esteja na lista de equipamentos autorizados, não possa ser acedido.

É tarefa do próprio agente a inibição das unidades de discos óticos, a definição das contas de avaliação autorizadas, bem como, dos acessos via rede.

A extração imediatamente antes da utilização de qualquer um dos executáveis e a sua eliminação logo após ter terminada a sua ação permite reduzir os riscos nefastos de correr binários não desejados, fruto de uma possível ação mal-intencionada de terceiros.

A primeira ação, logo após ter sido selecionado uma sala (lista de PCs), é a de contactar as máquinas (clientes) nela definidas, questionando-as acerca do seu estado. A aplicação tem a capacidade de estar e manter-se informada acerca do estado dos clientes e, para isso, necessita de implementar uma forma de receber essa informação. A forma mais adequada a essa missão, é a comunicação através de *websockets*. A aplicação está permanentemente à escuta num determinado porto por texto que começa forçosamente por palavras-chave preconcebidas de forma a minimizar possíveis tentativas de ataque ao sistema. Estas palavras têm um outro objetivo que é a de identificação do tipo de mensagem que se segue. O contacto com os clientes é iniciado usando a ferramenta «PsExec» que envia, após ter sido extraído da própria aplicação, um executável designado de «Agente» e o força a correr. Este agente recebe as suas ordens por parâmetros passados diretamente pela ferramenta envolvida e vai analisar o cliente para determinar o seu estado, reportando-o para a aplicação por meio dos *websockets* já referidos. A aplicação ao receber esse reporte, vai registar no ficheiro de registo o valor do MAC-ADDRESS, da *default gateway* e do endereço de *broadcast* do cliente. Do outro lado, o agente vai criar o seu próprio ficheiro onde vai guardar, além dos três valores já referidos, a máscara da rede e detalhes de cada um dois 6 itens de bloqueio, à medida que estes vão sendo ordenados.

As ações seguintes dependem de intervenção humana e das escolhas que faz, de qualquer forma, é o agente o responsável por efetivar tudo quanto são alterações ao sistema, desde que não sejam específicas da conta dos utilizadores. Neste último caso, o agente vai extrair dois binários que vão ser executados nas sessões, as quais são alvo de bloqueio. Um destes binários vai ser responsável por garantir que a «Área de transferência» da sessão onde está a ser executado permanece inválida, enquanto o outro garante que só funcionam os dispositivos USB indicados. Enquanto estes binários estiverem em execução, o bloqueio que impõem está ativo. Deste modo, seria fácil voltar a reaver a capacidade inibida pelo bloqueio, bastando para isso que se termine o processo respetivo. Estes processos não poderão ser terminados prematuramente, pois o acesso a programas ou utilitários com capacidade para os terminar foi inibido. A forma com

que estes dois processos podem ser corretamente terminados passa pelo utilização de *websockets* a funcionar num IP da gama de endereços *loopback*, onde o agente tem a missão de enviar o comando adequado para esse efeito.

A ação de bloqueio, dependendo das opções selecionadas, é efetuada em dois tempos. No primeiro tempo, o sistema é forçado a bloquear determinados tipos de ficheiros executáveis, bem como, definir as credenciais da conta de avaliação para permissão de iniciação de sessão e ainda para configuração do «AutoLogon». Após terminarem as tarefas envolvidas no primeiro tempo, o sistema é reinicializado, efetivando parte do bloqueio. Depois da máquina reiniciar e efetuar o início automático de sessão, esta recebe a configuração que não subsiste ao reinício e aplica-a, passando a estar na situação final de «Bloqueada». À medida que o bloqueio se vai efetivando, o agente envia para a aplicação o novo estado da máquina cliente.

4.5.4 Objetivos alcançados

No desenvolvimento do *software*, procurou-se respeitar os requisitos manifestados. Todos foram tidos em consideração e na sua maioria implementados na totalidade. Os *Requisitos do Utilizador* estipulados e apresentados em 3.2.1, foram todos alcançados à exceção da alínea c) , conforme relata a Tabela 8, quando o acesso à internet supõe a utilização de um servidor proxy.

Tabela 8 – Cumprimento dos requisitos do utilizador

DEFINIÇÃO	ESTADO
O *software* deve bloquear todos os acessos a dados de e para os computadores dos formandos a serem avaliados, especialmente na utilização de *pens* USB	Cumprido
O *software* deve bloquear a utilização de aplicações não autorizadas	Cumprido
O *software* deve bloquear a utilização da *web*, à exceção dos sites autorizados	Parcialmente cumprido
O *software* deve estar disponível em português, francês e inglês	Cumprido
O *software* deve ser de utilização simples e intuitiva	Cumprido
O *software* só deve poder ser utilizado pelos docentes	Cumprido
O *software* deve funcionar em sistema operativo Microsoft Windows 7 e posterior	Cumprido

Em seguida apresenta-se a Tabela 9 que indica qual o estado da implementação de cada um dos *Requisitos do Sistema* definidos em 3.2.2. visto estes terem importâncias diferentes para implementação.

Tabela 9 – Cumprimento dos requisitos do sistema

DEFINIÇÃO	IMPORTÂNCIA	ESTADO
O sistema deve ser versátil e adaptável às alterações	Média	Cumprido
O sistema deve conter uma conta de administração incorporada que não seja possível eliminar	Média	Cumprido
O sistema deve permitir alterar a senha da conta de administrador incorporada	Média	Cumprido
Operar em domínio AD Operar em g*rupo de trabalho*	Alta Média	Cumprido Cumprido
Ao iniciar a aplicação, o sistema deve autenticar o utilizador, reconhecendo se é administrador ou docente	Alta	Cumprido
Ao guardar as configurações, o sistema deve cifrar os dados antes de os escrever em ficheiro	Alta	Cumprido
O sistema deve guardar os dados em ficheiro próprio e no mesmo diretório onde se encontra a aplicação	Alta	Cumprido
O sistema deve guardar um registo dos acessos a sessões efetuados na aplicação	Baixa	Cumprido
A componente gráfica deve apresentar uma disposição linear dos componentes de forma a facilitar a perceção de utilização ao docente	Alta	Cumprido
O sistema deve incluir uma forma para facilmente mudar a língua de apresentação	Média	Cumprido
O sistema deve ser capaz de impedir que seja retirada ou introduzida informação no computador do formando quer através da rede, quer através de dispositivos de armazenamento externo, quer ainda através do próprio computador	Alta	Cumprido
O sistema deve bloquear a execução de aplicações não autorizadas	Alta	Cumprido
O sistema deve permitir a configuração de acessos de informação autorizados	Alta	Cumprido
O sistema deve permitir a configuração de equipamentos de armazenamento externo autorizados	Baixa	Cumprido
O sistema deve permitir configurar os diversos tipos de bloqueio	Alta	Cumprido
O sistema deve permitir ao docente escolher quais os tipos de bloqueio que pretende utilizar	Alta	Cumprido
O sistema deve conseguir repor as configurações originais do computador do formando uma vez terminada a ação de bloqueio	Alta	Cumprido
O sistema deve ter a capacidade de funcionar em redes que operam com o protocolo IPv6	Baixa	Em falta
O sistema não deve operar com *daemons*	Média	Cumprido

4.6 Síntese

Neste capítulo foram descritas a arquitetura e funcionamento internos da aplicação «PC Border» e a infraestrutura física para a qual foi concebida para funcionar. Foram, também, descritos os princípios de funcionamento sobre os quais a construção da aplicação assentou e ainda as razões que levaram a tomar determinadas opções no seu desenvolvimento.

Capítulo 5 – Testes efetuados

Este capítulo descreve os testes efetuados após o desenvolvimento da aplicação. Foram executados na infraestrutura de produção para qual a aplicação foi desenvolvida.

5.1 Validação

Assim que a aplicação ganhou forma e passou a incluir todo o código necessário ao bloqueio dos aspetos previstos, a aplicação foi testada em ambiente real, pondo de parte as máquinas virtuais que até então tinham sido usadas como palco para testes. A aplicação foi testada numa sala de aulas constituída por 31 computadores e outra constituída por 25 máquinas onde todas operam o Microsoft Windows 10 versão 1709 membro de uma *Active Directory* (AD).

Todos os testes efetuados até então, com recurso a máquinas virtuais, demonstraram que, quer com o Windows 8, quer com o Windows 10 a correr nos clientes, demoravam bastante tempo a aceitar a conexão vinda da ferramenta «PsExec». Independentemente desta situação ser ou não fruto do facto de todo o ambiente de testes estar contido num só anfitrião, o recurso à utilização de máquinas físicas veio acabar com essa situação, passando a ser praticamente instantânea a referida conexão. A Figura 54 retrata a janela principal da aplicação, com a lista «Sala 300» selecionada, para o primeiro teste efetuado sobre máquinas físicas. Pode ver-se que os 30 computadores da lista já responderam ao pedido de «estado», o primeiro passo do contacto ordenado pelo «PC Border». A coluna designada de «Estado» identifica qual o estado, da configuração e, ainda, de acesso à máquina. A última coluna intitulada de «OK» informa se a máquina está em sintonia com a aplicação.

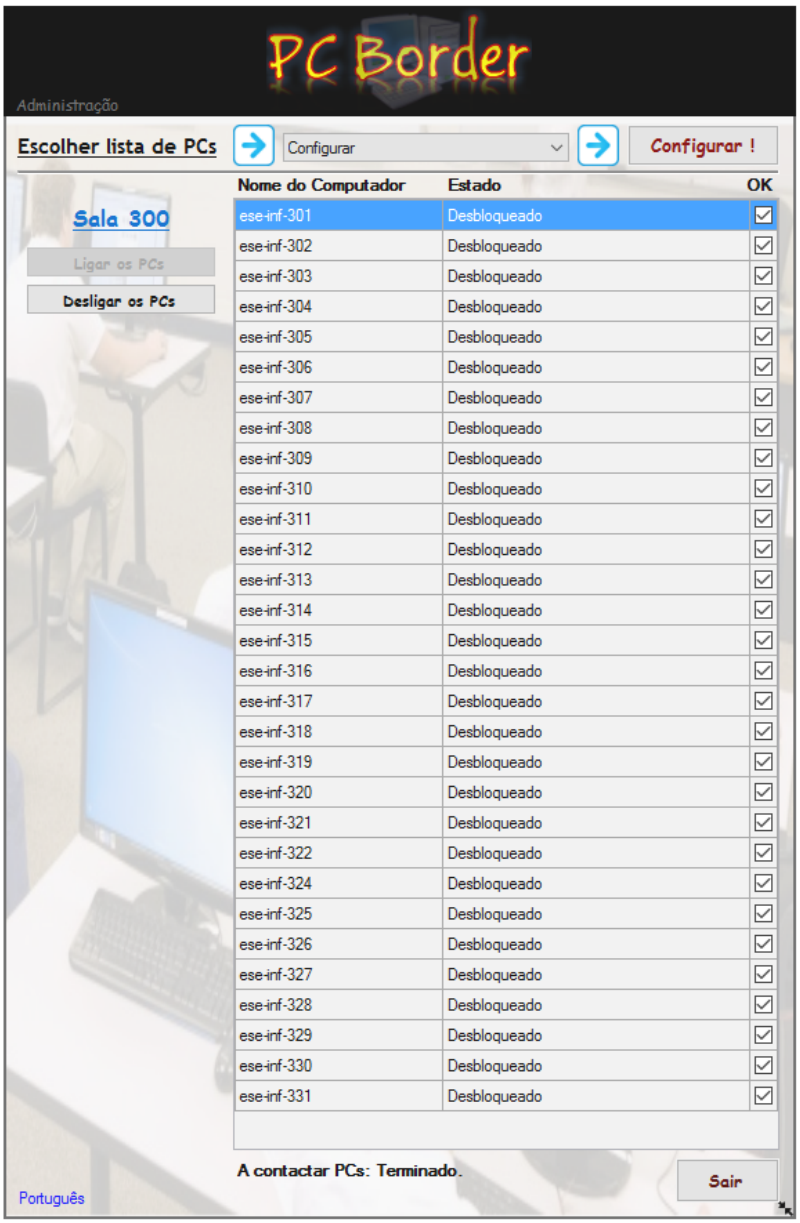

Figura 54 – PC Border - contacto estabelecido

Uma vantagem na utilização de máquinas virtuais é a velocidade com que executam a sua reinicialização. Em contrapartida, o processo de reinicialização nas máquinas físicas utilizadas para este primeiro teste demorou cerca de dois minutos. O primeiro teste constituiu apenas em restringir a inicialização de sessão a uma conta de utilizador e consequente implementação do *autologon*. Sempre que é definido o mecanismo de controlo de utilizadores, a máquina é forçosamente reinicializada para que possa executar o *autologon* iniciando automaticamente a sessão do utilizador definido na consola local da máquina. Esta funcionalidade é bastante útil, pois permite poupar recursos humanos – não é necessário o login presencial máquina a máquina

– na preparação dos PCs com a conta de utilizador indicada para execução dos exames. A Figura 55 destaca o sucesso da ação de bloqueio imposta nas 30 máquinas da lista.

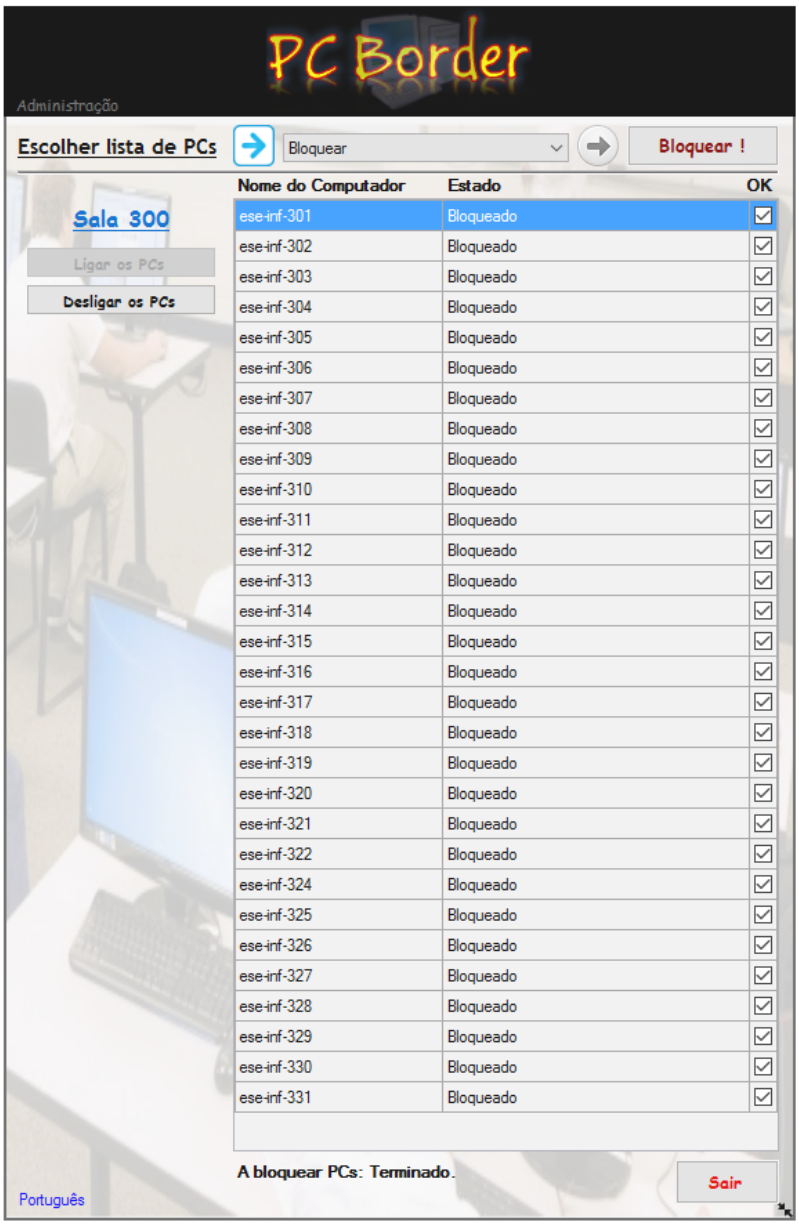

Figura 55 – PC Border - ação de bloqueio

Nesta figura pode ainda ser percetível que foi necessário remover a máquina «ese-inf-323» da lista, pois, problemas imputáveis à resolução de nomes, no sentido que o IP devolvido não corresponde à máquina que se pretende alcançar, impediram o contacto com a máquina pretendida.

O segundo teste contemplou todos os tipos de bloqueio configuráveis, no entanto, como algumas das máquinas utilizadas pela instituição que serviu de palco para os testes têm pouco

poder computacional e, especificamente no caso de uma máquina com processador AMD Athlon 64 3200+ e 3GB de RAM a correr o Windows 10 versão 1709, não foi possível à aplicação proceder ao bloqueio de todos controlos definidos, pois a máquina ultrapassou o tempo de espera definido na aplicação para o arranque do sistema. Num tal caso, apenas o bloqueio do utilizador (conta de avaliação) e dos programas autorizados permanecem ativos, tal como se pode observar na Figura 56. Estes dois tipos de bloqueio são os únicos que subsistem após a reinicialização do computador.

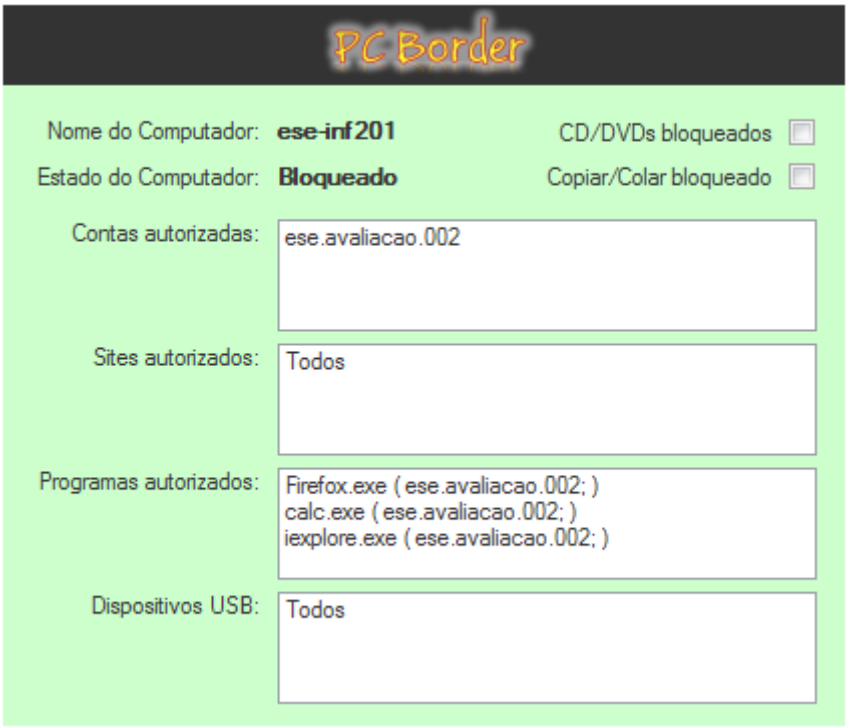

Figura 56 – Detalhes do bloqueio efetivo

Um terceiro teste revelou que a aplicação consegue cumprir a sua missão independentemente da existência do perfil da conta utilizada. Se os tipos de bloqueio configurados exigirem a definição de uma conta de utilizador também vão forçar a inclusão do *autologon* na máquina, logo, esta situação é garantida pelo facto da configuração de bloqueio ser aplicada finda a ação de *autologon*, altura a partir da qual, o perfil já existe.

O teste que se seguiu voltou a contemplar todas opções de bloqueio, desta feita, numa máquina com processador AMD Athlon 64 X2 5200+ e 2GB de RAM configuradas em «dual-channel». Neste teste foi possível comprovar o sucesso em todos os aspetos do bloqueio sem que houvesse constrangimentos devidos à inexistência do perfil, tal como retratado na Figura 57.

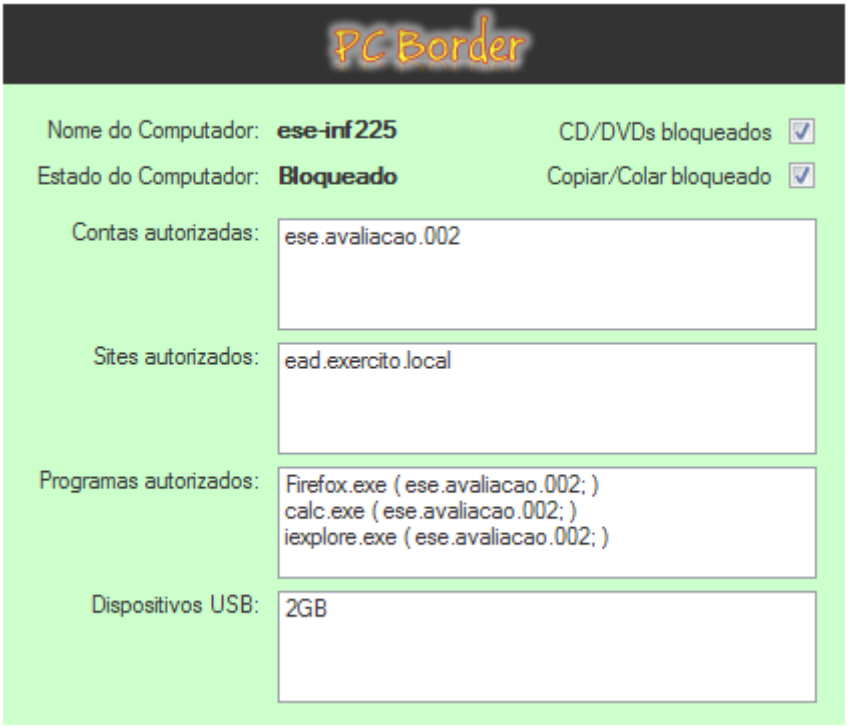

Figura 57 – Confirmação do bloqueio com todas as opções

Na Figura 58 é apresentado um extrato das rotas de encaminhamento de tráfego e da tabela de resolução de endereços logo após o bloqueio da máquina referida anteriormente. Este bloqueio autoriza o acesso, via rede, somente a «ead.exercito.local». Do lado esquerdo da imagem que constitui a figura, está representado parte das rotas de encaminhamento que foram definidas pela aplicação «PC Border». É possível verificar que a rota «0.0.0.0» não está definida. Essa seria a rota que garantiria a entrega de tráfego com destino a redes diferentes, ou seja, a «*Default Gateway*». Está assinalado a vermelho a rota estática que a aplicação definiu, para que o tráfego com destino a «ead.exercito.local» possa seguir, materializando-se assim a forma de acesso aos sites autorizados localizados em redes diferentes. Visto ser necessário manter contacto com os controladores de domínio e com os servidores de DNS, a aplicação definiu ainda as rotas que permitem o acesso a esses servidores, estando também representadas na dita figura embora de forma reduzida. Na realidade, basta estar definido um servidor de cada tipo para que a máquina possa funcionar. Na próxima versão da aplicação será tido em conta a definição de no máximo três servidores de cada para efeitos de redundância. A escolha dos servidores será baseada na distância a que cada um se encontra da máquina a correr a aplicação. Do lado direito da imagem, está representada a primeira parte da tabela de resolução de endereços da máquina. É possível observar que grande parte dos endereços são estáticos pois foram definidos pela aplicação. Estes

endereços são falsos o que permite que a entrega de tráfego para a mesma rede não seja concluída. A figura indica que pelo menos 11 endereços foram definidos dinamicamente, o que implica que a máquina estava em comunicação com outras na mesma rede na altura que o bloqueio foi ordenado. Esta forma de bloquear o tráfego na mesma rede não é eficaz por essa razão.

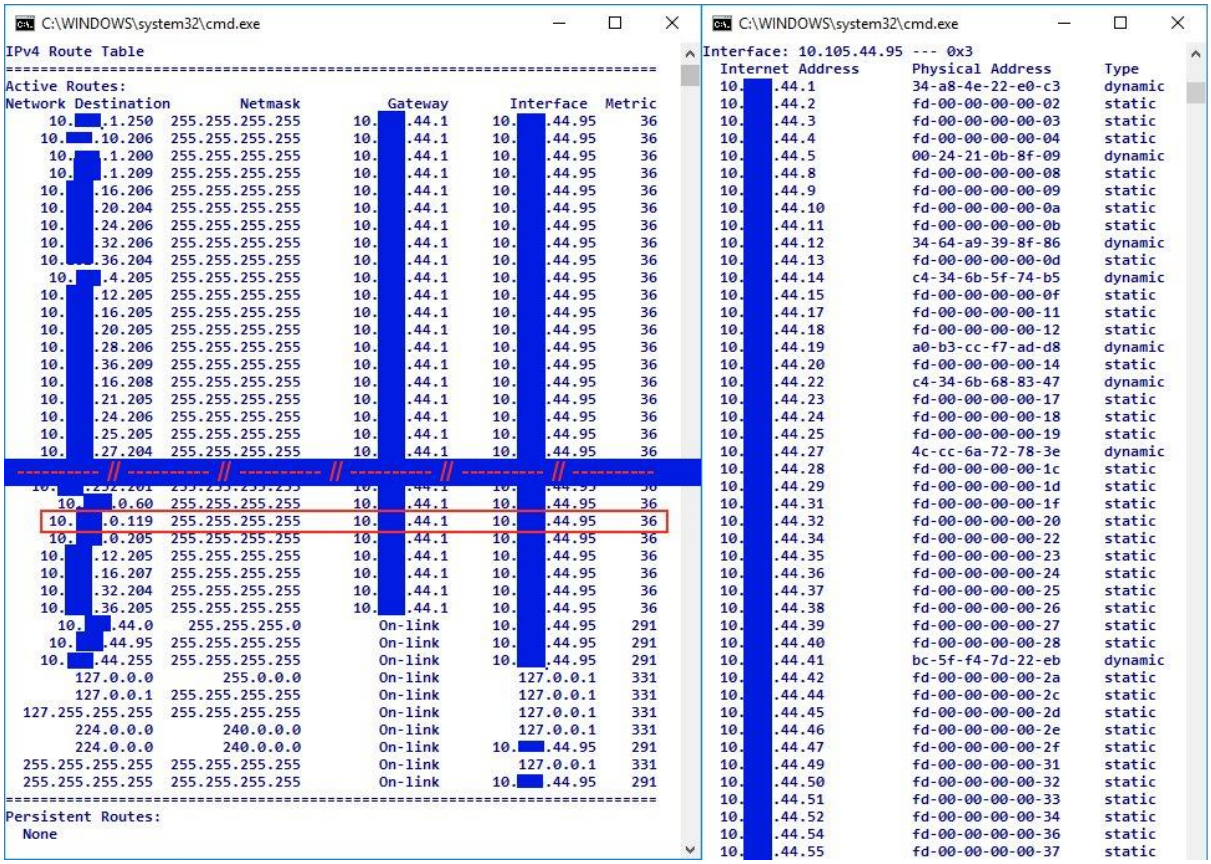

Figura 58 – Restrições impostas à comunicação

Não desconsiderando as observações dos últimos três testes, constatou-se posteriormente que uma máquina com 4 GB de RAM em configuração «dual-channel» e processador dual-core Intel Pentium G630 a 2,7 GHz, operando o sistema operativo Microsoft Windows 10 versão 1809, não conseguiu criar o perfil a tempo de ser aplicada a configuração necessária para a totalidade do bloqueio. Perante esta situação, foi necessário voltar a forçar o bloqueio. Aumentar o tempo de espera da aplicação não é solução, pois provocaria um desperdício de tempo sempre que o perfil da conta utilizada já esteja presente.

Os testes executados em qualquer uma das salas anteriormente referidas, apenas informam sobre os resultados da interação com a versão 1709 do SO Microsoft Windows 10. A versão 1809 do mesmo sistema operativo, que, entretanto, foi lançada, contempla uma nova ferramenta

designada de «Recortar e Desenhar» que vem substituir a atual «Ferramenta de Recorte». Visto esta ferramenta possibilitar a extração e registo de informação presente no ecrã, tal como a sua antecessora, é necessário fazer face a essa situação, incorporando o bloqueio da dita ferramenta na próxima versão do «PC Border». O executável cuja designação é «ScreenSketch.exe» encontra-se numa subpasta dentro da «WindowsApps» tal como identifica a imagem presente na Figura 59.

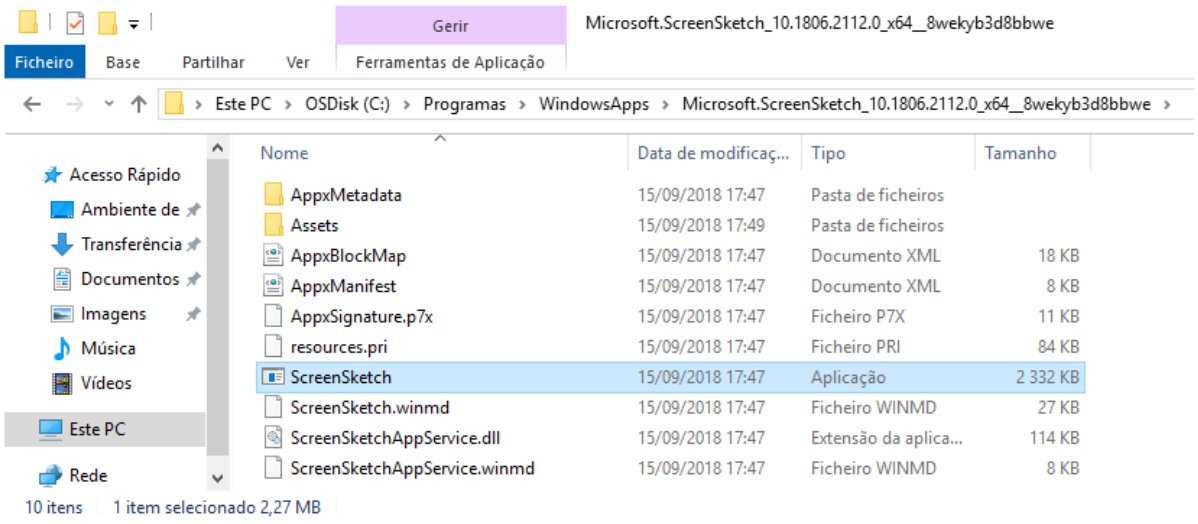

Figura 59 – Localização da ferramenta «Screen Sketch»

5.2 Contributos dos utilizadores

Submetida a aplicação à utilização por parte de docentes da instituição onde foi testada, estes relataram que a forma de a operar foi bastante percetível. Facilmente entenderam o fluxo lógico do «PC Border», dando ênfase ao texto sublinhado que se assemelha com outros sistemas informáticos existentes.

Os docentes inicialmente estranharam o facto da aplicação ter a capacidade de registar as ações que executam, mas, por fim, até concordaram que é uma boa forma que o administrador tem de se aperceber com que facilidade é que os docentes utilizam a aplicação, no sentido de os ajudar na eventualidade de demonstrarem mais dificuldade.

Estes *Beta-testers* também apontaram alguns aspetos negativos, sendo um deles, o facto de a aplicação não ter a capacidade de cancelar uma ação de bloqueio antes de terminar. Um outro aspeto que apontaram foi que não está perfeitamente percetível o que materializa a definição de

novos controlos de programas. Por último, informaram que o facto de a aplicação ter transparência ativa, em determinados fundos de ambiente de trabalho provoca uma sensação «esquisita», o que transtorna a sua utilização.

Capítulo 6 – Conclusão

Este capítulo descreve as conclusões obtidas após a investigação prévia e mediante a construção da aplicação «PC Border» decorridas durante a elaboração do presente trabalho.

6.1 Âmbito Geral

Findo o trabalho de investigação, de desenvolvimento e teste da aplicação «PC Border», pode concluir-se que os sistemas operativos da Microsoft são muito granulares, e que mediante o conhecimento e com mecanismos adequados, é possível executar quase todas as tarefas a que se possa propor. A interação direta com o *kernel*, permite coisas puramente fantásticas, tal como, impedir da abertura mecânica das unidades de discos óticos, mesmo que a ordem de ejeção seja dada pelo botão próprio para o efeito existente na unidade.

O facto de o evitar a execução de código nas máquinas alvo de isolamento ser um requisito, veio tornar a aplicação mais complexa e fazer com que haja mais tráfego a circular na rede. O envio de um agente unicamente no início, logo após seleção de uma sala, iria obrigar a sua permanência em execução durante o período que a sala se mantivesse selecionada, em contrapartida, apenas se notaria um volume de tráfego na rede nos primeiros instantes do funcionamento da aplicação. Sendo que, os restantes contactos seriam estabelecidos por *websockets* a funcionar em ambos os sentidos, garantiria a mesma capacidade operacional em detrimento de alguma capacidade de processamento. Esta será uma solução a propor assim que as máquinas possuam alguma folga de poder computacional de forma a não interferir com a eficácia das mesmas.

6.2 Trabalho futuro

Esta aplicação foi talhada às necessidades específicas relativas ao *hardware* e às políticas de segurança existentes na instituição que manifestou a necessidade. Para trabalho futuro, existe a construção da segunda versão do «PC Border» com princípio de funcionamento baseado em *daemons* e em *websockets*. Desta forma diminuirá o fluxo de tráfego a circular entre a máquina do formador e as dos formandos, bem como permitirá a inclusão de outras funcionalidades que

com a presente versão não é possível. Entre funcionalidades já previstas e outras que certamente surgirão, fala-se nomeadamente na capacidade de cancelar uma operação a meio curso antes de findar, ou mesmo na capacidade de a máquina retomar automaticamente o seu estado de bloqueio após uma interrupção inesperada como a de falha imprevista de energia, e ainda, na capacidade de operar na totalidade independentemente da infraestrutura de TI incluir um servidor *proxy*.

Bibliografia

[1] D. Russell and G. T. Gangemi Sr., *Computer Security Basics - Deborah Russell, Debby Russell, G. T. Gangemi, Sr Gangemi, G. T. Gangemi, Sr. - Google Books*, July 1992. .

[2] A. Guimarães, R. Lins, and R. Oliveira, *Segurança em Redes Privadas Virtuais-VPNs*. Brasport, 2006.

[3] Intel, "Thunderbolt™ Technology," 2012. [Online]. Available: https://www.intel.com/content/dam/doc/technology-brief/thunderbolt-technology-brief.pdf. [Accessed: 21-Oct-2018].

[4] C. R. Meghana, M. Ramya, and D. . (Acharya I. of T. Sakkari, "THUNDERBOLT - LIGHT PEAK," 2011.

[5] L. IntelliAdmin, "USB Disabler Pro | Remote Administration For Windows." [Online]. Available: http://www.intelliadmin.com/index.php/usb-disabler-pro//. [Accessed: 19-May-2018].

[6] SecurityXploded, "Windows USB Blocker Tool : Free Software to Block or Unblock USB on Windows | www.SecurityXploded.com." [Online]. Available: https://securityxploded.com/windows-usb-blocker.php. [Accessed: 21-May-2018].

[7] "NoDrives Manager." [Online]. Available: http://nodrvman.sourceforge.net/. [Accessed: 25-May-2018].

[8] Microsoft, "Prevent users from connecting to a USB storage device." [Online]. Available: https://support.microsoft.com/en-us/help/823732/how-can-i-prevent-users-from-connecting-to-a-usb-storage-device. [Accessed: 25-May-2018].

[9] "View any installed/connected USB device on your system." [Online]. Available: https://www.nirsoft.net/utils/usb_devices_view.html. [Accessed: 01-Oct-2018].

[10] J. Postel, "DoD standard Internet Protocol - IETF," 1980.

[11] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," 1995.

[12] S. E. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," 1998.

[13] S. E. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," 2017.

[14] "5 Tips to Manage Your Windows Clipboard Like a Pro." [Online]. Available: https://www.makeuseof.com/tag/5-tips-manage-windows-clipboard-like-pro/. [Accessed: 27-May-2018].

[15] Ritesh Kawadkar, "Prevent v 1.0 - Restrict Cut Copy Paste Delete in Windows 7/8/10." [Online]. Available: http://madgeektools.blogspot.com/2018/05/prevent-v-10-restrict-cut-copy-paste.html. [Accessed: 04-Oct-2018].

[16] "Key Scan Codes | Microsoft Docs." [Online]. Available: https://docs.microsoft.com/en-

us/previous-versions/visualstudio/visual-studio-6.0/aa299374(v=vs.60). [Accessed: 26-May-2018].

[17] DanRollins, "Keyboard Remapping: CAPSLOCK to Ctrl and Beyond." [Online]. Available: https://www.experts-exchange.com/articles/2155/Keyboard-Remapping-CAPSLOCK-to-Ctrl-and-Beyond.html. [Accessed: 26-May-2018].

[18] "How to Block (or Allow) Certain Applications for Users in Windows." [Online]. Available: https://www.howtogeek.com/howto/8739/restrict-users-to-run-only-specified-programs-in-windows-7/. [Accessed: 29-May-2018].

[19] "Smart Windows App Blocker (Windows) - Download." [Online]. Available: https://smart-windows-app-blocker.en.softonic.com/. [Accessed: 29-May-2018].

[20] J. Daemen and R. V. Rijmen, "The Rijndael Block Cipher."

Glossário

A

ADMINISTRADOR "Utilizador cuja conta contém privilégios superiores na utilização de determinado sistema informático"

C

CLIENTE "Sistema computacional que depende de outro para executar determinada tarefa"

CONTA "Contentor de registo de credenciais de identificação perante um sistema informático"

U

UTILIZADOR "Pessoa ou máquina que utiliza um sistema informático"