Dissertação

Mestrado em Engenharia Informática – Computação Móvel

Arquitetura de Segurança do IPL

Adaíl Domingues da Silva de Oliveira

Leiria, Setembro de 2011

Dissertação

Mestrado em Engenharia Informática – Computação Móvel

Arquitetura de Segurança do IPL

Adaíl Domingues da Silva de Oliveira

Dissertação de Mestrado realizada sob a orientação do Professor Doutor Carlos Manuel da Silva Rabadão, Professor Adjunto do Departamento de Engenharia Informática do Instituto Politécnico de Leiria.

Leiria, Setembro de 2011

À Luciana e Matilde

Esta página foi intencionalmente deixada em branco

Agradecimentos

O presente trabalho só foi possível de concretizar com o apoio de diversas pessoas. Para todas elas e de um modo genérico quero aqui expressar os meus sinceros agradecimentos.

Pelo papel fundamental que tiveram não poderia deixar de agradecer particularmente a algumas pessoas, cuja influência foi determinante para o concluir deste trabalho.

Ao Professor Doutor Carlos Rabadão, por ter aceite o desafio de transformar um problema do dia-a-dia num caso de estudo. Pela sua enorme disponibilidade, incentivo, apoio e orientação que se revelaram determinantes na concretização e sucesso do trabalho.

Ao meu saudoso amigo e colega Carlos Canudo que me marcou imenso e me fez crescer com os seus ensinamentos, teimosias e profissionalismo.

Aos elementos da minha equipa de trabalho (UARS) dos Serviços Informáticos do Instituto Politécnico de Leiria e aos meus colegas de gabinete, pela motivação e disposição que me transmitiram ao longo dos tempos.

Aos meus pais por me permitirem chegar aqui, pelos valores que me transmitem, pela sua presença e apoio constante.

Por último, mas não menos importantes, um agradecimento profundo à minha esposa Luciana e filha Matilde, pelo carinho, apoio, incentivo e encorajamento constantes ao longo de todo o tempo que lhes privei.

Esta página foi intencionalmente deixada em branco

Nota Prévia

A presente dissertação foi realizada na Unidade de Administração de Redes e Segurança dos Serviços Informáticos do Instituto Politécnico de Leiria, tendo como base a atividade "Plataforma de Monitorização e Segurança" no âmbito da operação "IPL e-Rede", candidatada aos Sistemas de Apoios à Modernização Administrativa.

Neste trabalho existem questões que não foram aprofundadas devido à sensibilidade da informação envolvida e necessidade de sigilo.

Esta página foi intencionalmente deixada em branco

O viajante sente no Castelo de Marialva uma grande responsabilidade. Por um minuto, e tão intensamente que chegou a tornar-se insuportável, viu-se como ponto mediano entre o que passou e o que virá. Experimente quem o lê ver-se assim, e venha depois dizer como se sentiu.

José Saramago

Esta página foi intencionalmente deixada em branco

Resumo

O massivo desenvolvimento tecnológico contemporâneo destituiu concepções tradicionais, valores e formas de vida, originando um novo paradigma caracterizado pela globalização da atividade humana suportada por uma sociedade em rede.

O homem através da enorme capacidade de adaptação, que é observável ao longo da história encara estas alterações de forma passiva, rendendo-se perante os benefícios da evolução tecnológica, tornando-se rapidamente dependente desta nova forma de vida. O que inicialmente poderá ser considerado como excentricidade, rapidamente deixa de o ser e introduz-se no quotidiano com naturalidade.

Esta sociedade contemporânea caracterizada de civilização tecnológica onde o homem persegue os avanços tecnológicos sempre com maior ousadia, encontra-se suportada fundamentalmente na Internet.

Nas últimas décadas, mercê do crescimento exponencial da Internet e da massificação do seu uso, surgiram diversas ameaças de segurança. Tais ameaças devem-se, na maioria dos casos, à ausência de mecanismos de segurança adequados, deficiência de políticas de segurança, massificação do uso de terminais móveis, mobilidade e ingenuidade dos utilizadores.

O uso de terminais móveis fez com que os sistemas deixassem de estar confinados aos limites físicos dos edifícios sendo responsável pela mudança do perímetro de segurança das organizações. O perímetro de segurança deixou de ser algo bem definido e identificado e passou a ser constituído por todos os tipos de dispositivos que pertençam à rede da organização.

Com o surgir das aplicações viradas para a Internet surgiu também uma nova geração de ameaças de segurança. Estas aplicações, denominadas de aplicações *Web 2.0,* possuem a particularidade de facilmente contornarem os mecanismos e políticas de segurança existentes. Atualmente, a maioria das aplicações deste tipo já estão "infiltradas" dentro das organizações, sendo responsáveis pela perda de produtividade, consumo excessivo de largura de banda e risco de perda de dados.

Perante este cenário, é importante que na definição e desenho de arquiteturas de segurança duma organização sejam tidos em conta todos os desafios de segurança e ameaças que atualmente as organizações se encontram expostas, sejam diretamente ou indiretamente.

Neste trabalho será proposta uma nova arquitetura e mecanismos de segurança que permitam acompanhar as necessidades resultantes da centralização ocorrida em 2007 do Instituto Politécnico de Leiria, tendo sempre como missão a salvaguarda do negócio do IPL e a sua proteção das ameaças atuais.

Palavras-chave: Rede, Arquiteturas de Segurança, Aplicações *Web 2.0*

Abstract

The excessive development of technology deposed modern traditional concepts, values and ways of life, creating a new paradigm characterized by the globalization of human activity supported by a network society.

Man has an enormous capacity of adapting, this has been observed throughout history, humans view changes passively and surrender to the benefits of technological changes and quickly become dependent on this new way of life. What initially might seem eccentric quickly ceases and gets introduced into a daily routine with ease.

Our modern society characterized as a modern technological civilization in which man pursues technological advances, is supported primarily by the Internet.

In recent decades, thanks to the exponential growth of the Internet and its use, several security threats have emerged. Such threats are due to absence of adequate security mechanisms, deficiency of security policies, an excessive use of mobile terminals, mobility and the ingenuity of users.

The use of mobile devices have caused the system to no longer be confined to the physical boundaries of buildings which are responsible for changing the security perimeter of the organizations. The security perimeter is no longer well defined, therefore began to consist of all types of devices that belong to the organization network.

With the emerging of applications facing the Internet a new generation of security threats arose. These applications called Web 2.0 have the particularity of the mechanisms and easily circumvent existing security policies. Currently, most applications of this type are already "infiltrated" within their organization, causing loss of productivity, excessive consumption of bandwidth and the risk of data loss.

Given this scenario, it is important that the definition and design of security architectures of an organization are taken into account, all the security challenges and threats that organizations are currently exposed, whether directly or indirectly

In this study a new architecture and security mechanism to monitor the needs, resulting from the centralization occurred in 2007 is proposed from the Polytechnic Institute of Leiria with the mission to safeguard the IPL business and protection of its current threats.

Key-Words: *Network, Security Architecture, Web 2.0 Applications*

Esta página foi intencionalmente deixada em branco

Índice

Agradecimentos iii
Nota Prévia v
Resumo ix
Abstract xi
Índice xiii
Lista de Figuras xix
Lista de Tabelas xxi
Lista de Acrónimos xxiii
1 - Introdução 1
1.1 - Motivação e Objetivos 2
1.2 - Metodologia de Investigação 2
1.3 - Principais Contribuições 3
1.4 - Estrutura de Dissertação 4
2 - Conceitos e Princípios de Segurança 5
2.1 - A tríade CIA 5
2.1.1 - Confidencialidade 6
2.1.2 - Integridade 7
2.1.3 - Disponibilidade 7
2.2 - Pessoas, Processos e Tecnologia 8
2.3 - Políticas, Normas, Orientações e Procedimentos 9
2.3.1 - Políticas 10
2.3.2 - Normas 11
2.3.3 - Orientações/Guia de Boas Práticas 11
2.3.4 - Procedimentos 12

2.4 - Segurança de Redes 12
2.4.1 - Desenho de Redes e Segurança 15
2.4.2 - História da Segurança de Redes 16
2.5 - Ameaças, Vulnerabilidades e Riscos 17
2.5.1 - Ameaças 18
2.5.2 - Vulnerabilidades 18
2.5.3 - Relação entre Ameaças e Vulnerabilidades 19
2.5.4 - Risco 20
2.6 - Atacantes, Ataques e Motivações 20
2.6.1 - Atacantes e Suas Motivações 21
2.6.2 - Ataques 23
2.6.3 - Fases de um ataque 25
2.7 - Modelo de Segurança em camadas 29
2.7.1 - Camada Física 30
2.7.2 - Camada VLAN 31
2.7.3 - Camada ACL 31
2.7.4 - Camada *Software* 32
2.7.5 - Camada Utilizador 33
2.7.6 - Camada Administrativa 33
2.7.7 - Camada Departamento TI 34
2.7.8 - Relação entre o modelo NSM e o modelo OSI 34
2.7.9 - Implementação do Modelo NSM 36
2.8 - Perímetro de Segurança 38
2.8.1 - O que é um Perímetro 38
2.8.2 - Evolução do Perímetro de Segurança 39
2.8.3 - Definir o Perímetro 41
2.8.4 - Zonas de Rede 42

2.8.5 - Segurança do Perímetro 45
2.8.6 - Considerações 46
3 - Boas Práticas no Desenho de Arquiteturas de Segurança 49
3.1 - Gestão de Risco 49
3.1.1 - Gestão de Risco Reactivamente ou Proativamente 50
3.1.2 - Avaliação de Riscos 52
3.1.3 - Mitigação de Riscos 65
3.1.4 - Avaliação 66
3.2 - Cisco SAFE: Arquitetura de Referência de Segurança 67
3.2.1 - Cisco Security Control Framework (SCF) 69
3.2.2 - Arquitetura de Segurança SAFE 70
3.2.3 - Princípios da Arquitetura 71
3.3 - Evolução das Aplicações 73
3.3.1 - Classificação 73
3.3.2 - Evasão 74
3.3.3 - Ameaças 76
3.3.4 - Educação vs. Entretenimento 77
3.4 - Desafios de Segurança 2011 79
3.5 - *Firewalls* da Próxima Geração 81
3.5.1 - Identificação de Aplicações 83
3.5.2 - Identificação de Utilizadores 84
3.5.3 - Identificação de Conteúdos 84
3.5.4 - Perda de informação sensível 85
3.5.5 - Controlo de Políticas 86
4 - Avaliação da Arquitetura de Segurança Existente 87
4.1 - Caracterização da Infraestrutura de TI 87
4.1.1 - Ligação Internet 88

4.1.2 - VLANs 89
4.1.3 - Endereçamento 89
4.1.4 - Redes sem fios 90
4.1.5 - Autenticação 91
4.1.6 - Tipos de utilizadores 91
4.1.7 - Acessos remotos 92
4.1.8 - Sistemas operativos 92
4.1.9 - Dispositivos e Mobilidade 92
4.2 - Avaliação da Arquitetura e Mecanismos de Segurança 93
4.2.1 - Avaliação da Arquitetura Existente 94
4.2.2 - Infraestrutura e Controlo de Acessos 96
4.2.3 - Gestão de Segurança 98
4.2.4 - Manutenção dos Níveis de Serviço 99
4.2.5 - Análise de Vulnerabilidades 99
4.3 - Análise de Segurança e Visibilidade de Aplicações 100
4.3.1 - Metodologia de Análise 101
4.3.2 - Riscos Introduzidos por Aplicações de Risco Elevado 103
4.3.3 - Top das Aplicações de Risco em Uso 104
4.3.4 - Características das Aplicações que Determinam Risco 106
4.3.5 - Top das Aplicações que Percorrem a Rede 108
4.3.6 - Aplicações que Utilizam HTTP 110
4.3.7 - Principais Categorias de URLs 111
4.3.8 - Principais Ameaças Presentes na Rede 111
4.3.9 - Utilização de Aplicações por Categoria e Tecnologia 112
4.3.10 - Ameaças Encontradas 113
4.3.11 - Recomendações 114
5 - Proposta de Arquitetura de Segurança 117

5.1 - Arquitetura de Segurança 117
5.1.1 - Zonas de Segurança 119
5.1.2 - Tecnologia 121
5.1.3 - Redundância e Desempenho 122
5.1.4 - Mobilidade 122
5.1.5 - Utilizadores Remotos 123
5.1.6 - Módulos e Proteções 124
5.1.7 - Gestão, Registos e Relatórios 125
5.1.8 - Funcionamento 126
5.2 - Implementação 127
5.2.1 - Implantação de NGFW 127
5.2.2 - Controlo de Utilizadores 128
5.2.3 - Plano de migração 129
6 - Conclusões 133
6.1 - Trabalhos Futuros 134
Bibliografia 135
Anexo A 139
Aplicações de Risco 139
Anexo B 143

Esta página foi intencionalmente deixada em branco

Lista de Figuras

Figura 1 - Desafio da segurança 6

Figura 2 - Relação entre pessoas, processos e tecnologia 8

Figura 3 - Relacionamento dos processos de segurança 10

Figura 4 - Hierarquia dos documentos de segurança 12

Figura 5 - Evolução registada desde 2000 até 2010 no acesso Internet (10) 13

Figura 6 - Tipos de vulnerabilidades 19

Figura 7 - Relação entre ator, motivação e vulnerabilidade 19

Figura 8 - As cinco fases de um ataque 25

Figura 9 - Modelo de Segurança de Redes 29

Figura 10 - Perímetro de segurança 38

Figura 11 - Diferentes Zonas de Segurança 42

Figura 12 - Mobilidade e conectividade de utilizadores 44

Figura 13 - Processo Gestão de Risco 50

Figura 14 - Visão da abordagem proactiva 51

Figura 15 - Processo de Avaliação de Risco 55

Figura 16 – *Security Control Framework* (27) 69

Figura 17 – Ciclo de Vida da SCF 70

Figura 18 – Cisco SAFE (28) 71

Figura 19 – Arquitetura modular da arquitetura SAFE (27) 72

Figura 20 – Aplicações evasivas e suas estratégias (29) 74

Figura 21 – Frequência de detecção das aplicações Google (30) 75

Figura 22 – Consumo de largura de banda em meio académico vs meio não académico (31) 78

Figura 23 – Ligação WWAN de Leiria, Caldas e Peniche 88

Figura 24 – Infraestrutura rede sem fios 91

Figura 25 – Arquitetura de segurança antes da centralização 94
Figura 26 – Arquitetura de análise de risco de aplicações 102
Figura 27 - Top das aplicações de alto risco 103
Figura 28 - Características comportamentais das aplicações de alto risco detectadas 107
Figura 29 - Consumo de sessões em percentagem por tecnologia (aplicações) 113
Figura 30 - Consumo de bytes em percentagem por tecnologia (aplicações) 113
Figura 31 – Arquitetura de segurança proposta 118
Figura 32 – Zonas de segurança 119
Figura 33 – Mecanismos de Proteção 124

Lista de Tabelas

Tabela 1 - Métodos de Ataque e Proteções de Segurança (24) 23
Tabela 2 - Diferentes estados e riscos durante as fases de um ataque 29
Tabela 3 - Comparação das camadas do modelo NSM e modelo OSI invertido 35
Tabela 4 - Relação entre o modelo NSM e modelo OSI invertido 35
Tabela 5 - Mecanismos de implementação do modelo NSM 37
Tabela 6 - Classificação de Classes 43
Tabela 7 – Exemplos de Ativos 52
Tabela 8 – Abordagem Quantitativa vs. Qualitativa 53
Tabela 9 - Diferentes tipos de ameaças 57
Tabela 10 - Ameaças Humanas: Fontes de Ameaças, Motivações e Ações 57
Tabela 11 - Relação Vulnerabilidade / Ameaças 58
Tabela 12 - Exemplos de Vulnerabilidades 59
Tabela 13 - Definição de Probabilidade 61
Tabela 14 - Magnitude da definição do impacto 62
Tabela 15 - Matriz Nível de Risco 63
Tabela 16 - Níveis de Risco e Ações a Tomar 63
Tabela 17 – Exemplos de Controlos 64
Tabela 18 – Categorias com mais consumo de largura de banda (31) 78
Tabela 19 – Principais elementos de uma arquitetura de segurança 93
Tabela 20 – Categorias e subcategorias de classificação de aplicações 102
Tabela 21 - Aplicações descobertas com risco elevado 5 104
Tabela 22 - Aplicações descobertas com risco elevado 4 105
Tabela 23 - Top de aplicações que consumem largura de banda 108
Tabela 24 - Subcategorias de todas as aplicações encontradas 109
Tabela 25 - Top de aplicações HTTP identificadas 110

Tabela 26 - Top categorias de URL visitadas 111

Tabela 27 - Principais ameaças identificadas, ordenadas pelo número de incidentes 112

Lista de Acrónimos

AP	*Access Point*
CIA	*Confidentiality, Integrity and Availability*
CERT	*Computer Emergency Response Team*
DLP	*Data Loss Prevention*
DMZ	*Demilitarized Zone*
DNS	*Domain Name Service*
DoS	*Denial of Service*
ITSEC	*Information Technology Security Evaluation Criteria*
IPL	Instituto Politécnico de Leiria
IEEE	Institute of Electrical and Electronics Engineers
ISSO	*International Standard Organization*
MIT	*Massachusetts Institute of Technology (MIT)*
NGFW	*Next Generation Firewall*
NSM	*Network Security Model*
NIST	*Nation Institute of Standards and Technology*
NOC	*Network Operation Center*
IPL	Instituto Politécnico de Leiria
ISSO	*International Standard Organization*
OSI	*Open Systems Interconnection*
P2P	*Pear to Pear*
QoS	*Quality of Service*
ROSI	*Return On Security Investment*
SANS	*SysAdmin, Audit, Network, Security*
SCF	*Security Control Framework*
SCP	*Secure Copy*
SLE	*Single Loss Expectancy*
SSID	*Service Set Identifier*

SSL	*Secure Sockets Layer*
UARS	Unidade de Administração de Redes e Sistemas
URL	*Uniform Resource Locator*
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
VLAN	*Virtual Local Area Network*
VoIP	*Voice over IP*
VPN	*Virtual Private Network*
VRF	*Virtual Rounting and Forwarding*
VTP	*VLAN Trunking Protocol*
WAN	*Wide Area Network*
WWW	*World Wide Web*

1 - Introdução

As preocupações com a segurança dos Sistemas de Informação cresceram exponencialmente nas últimas décadas como resultado da dependência das sociedades na era digital. Com aposta das organizações nos mercados e tecnologias emergentes, surgem riscos acrescidos para estas, aumentando a dificuldade no assegurar dos pilares confidencialidade, integridade e disponibilidade da informação.

Apesar dos significativos investimentos em segurança, as organizações continuam a ser alvo de ameaças que por vezes possuem consequências graves. Simultaneamente, os tempos de crise obrigam à apresentação de melhores resultados com a diminuição dos recursos. Noutras palavras o acréscimo da eficácia da segurança é necessária se não imprescindível, enquanto o aumento da eficiência e flexibilidade também se tornou um objetivo primordial.

A segurança é mais do que um simples produto ou tecnologia que qualquer um pode adquirir como supressor de sintomas. É um processo contínuo e amplo, com implicações em todas as áreas e atores que compõem as organizações. Caracterizado por se encontrar em permanente evolução, mutação e transformação, o processo de segurança obriga a um esforço redobrado por parte de todos os intervenientes das organizações, sendo que, o seu sucesso só é exequível se aos novos desafios que surgem com a evolução histórica, for dada como resposta uma mudança nos hábitos instituídos assim como na infraestrutura de suporte à organização (1).

A proliferação do uso de tecnologias associadas a Web 2.0 fez com que surgissem novas ameaças para o qual os responsáveis pela segurança não se encontram preparados. Um destes fenómenos recentes diz respeito a um conceito chamado de consumerização, que surgiu com a mudança na cultura tecnológica do indivíduo e com a rápida evolução e adopção das tecnologias de computação pessoal, que se encontram acessíveis a qualquer utilizador.

No passado, as tecnologias de ponta existiam apenas no âmbito corporativo, o que caracterizava as empresas por se encontrarem na vanguarda e de serem os grandes centros de introdução de novas tecnologias. Atualmente, estas novas tecnologias surgem primeiro nos equipamentos voltados para os consumidores, sendo adotadas em larga escala por profissionais e utilizadores de tecnologias emergentes, como ferramentas de uso pessoal.

Esta tendência faz com que os departamentos de TI sejam pressionados pelos utilizadores para que disponibilizem tecnologias em meios corporativos similares às utilizadas em meios pessoais. Por vezes, o utilizador devido à sua insatisfação recorre às novas tecnologias como substituto das tecnologias adoptadas pelos responsáveis das organizações. Esta liberdade de uso cria problemas de segurança potencialmente elevados.

Este trabalho tem como finalidade explorar como os mecanismos e arquiteturas de segurança devem evoluir de forma a responder aos novos desafios de segurança. Especificamente, são analisadas as mudanças ocorridas e quais as alterações necessárias ao nível da segurança da rede e dos dispositivos que a compõem. Todo o trabalho será focado à realidade do Instituto Politécnico de Leiria e suas necessidades.

1.1 - Motivação e Objetivos

Este documento retrata um caso de estudo realizado no âmbito de um projeto real de desenho e implementação de arquitetura de segurança, com intuito de ultrapassar as limitações identificadas na arquitetura atualmente em laboração no IPL. O seu objetivo é o de descrever todo o processo que possibilitou chegar à definição de arquitetura e mecanismos de segurança, assim como a estratégia adotada para sua implementação. Ao longo do documento serão justificadas as opções e caminhos seguidos.

A definição e reestruturação da arquitetura de segurança tem em conta alguns requisitos e lacunas, que não estavam contemplados na anterior arquitetura. Destacando-se:

- Centralização ocorrida no IPL;
- Novos desafios de segurança;
- Necessidades dos atores do IPL;
- Produtividade dos colaboradores;
- Disseminação do perímetro de segurança;
- Redundância e desempenho;
- Gestão unificada de dispositivos de segurança.

A execução deste trabalho deve resultar na definição de uma arquitetura de segurança e num conjunto de mecanismos capazes de combater os desafios e ameaças de segurança existentes nos dias de hoje. A mesma deverá ser caracterizada de redundante, robusta, fácil de gerir e integrável na infraestrutura de autenticação existente. A sua implementação contribuirá ainda para a simplificação do processo de gestão de segurança e responderá às necessidades resultantes do processo de centralização do IPL ocorrido em 2007.

1.2 - Metodologia de Investigação

A metodologia de investigação utilizada para atingir os principais objetivos deste trabalho, inclui várias fases, de alguma forma evidenciadas pela lista de objetivos a atingir.

Numa primeira fase, realizou-se a pesquisa e recolha da literatura referente a desenvolvimentos identificados como relevantes em cada uma das áreas do trabalho. Da análise e estudo da literatura, resultou uma avaliação que se revelou fundamental nas tomadas de decisão e caminho a percorrer na fase de concepção e caracterização da proposta de solução.

Numa segunda fase, foram realizadas reuniões com os elementos da equipa de segurança do IPL, tendo participado também indivíduos da equipa de sistemas e da equipa de

desenvolvimento. O objetivo primordial foi o de recolher requisitos e necessidades ao qual a arquitetura devia responder. Além das reuniões internas, foram também efetuados encontros com empresas portuguesas reconhecidas na área de segurança, com intuito de conhecer as soluções existentes no mercado e receber feedback do esboço do modelo de arquitetura.

Numa terceira fase, foram realizados alguns testes de segurança sobre a arquitetura em laboração, com o objetivo de conhecer os riscos e problemas de segurança ao qual o IPL se encontra exposto. Nos testes realizados, elaborou-se uma análise detalhada de visibilidade das aplicações que circulam na rede do IPL. Além dos testes de segurança, foram também testadas algumas soluções de *Next Generation Firewall* existentes no mercado.

Numa quarta fase, tendo por base o conhecimento científico adquirido e os testes realizados na fase anterior, foi concebida e caracterizada uma proposta de arquitetura e mecanismos de segurança para dar reposta às necessidades e aos problemas identificados.

Por fim, na última fase foi elaborado um plano de migração para a implementação da nova arquitetura. O plano foi definido com o objetivo de reduzir ao mínimo a indisponibilidade de serviço, assim como o impacto na arquitetura que serve de suporte ao negócio do IPL.

1.3 - Principais Contribuições

O desafio de proteger nos dias de hoje é diferente do passado, a evolução tecnológica, a mudança de mentalidades e atitudes, fez com que surgissem novos desafios de segurança que se encontram referenciados neste trabalho. Muitos dos problemas identificados, são uma presença constante nas organizações e no dia-a-dia dos utilizadores, sem que exista a sensibilização para os mesmos.

A análise de risco e visibilidade de aplicações resultante deste trabalho, realizada num meio académico caracterizado pela sua dimensão, permite perceber o uso dado às redes académicas e os riscos resultantes da sua utilização.

A análise, descrição e implementação dos NGFW na segurança das organizações, revela-se também uma contribuição importante devido ao pouco conhecimento deste tipo de mecanismos.

Outra das contribuições importantes, senão a mais importante, diz respeito à definição de arquiteturas de segurança em meios académicos. A arquitetura proposta que teve como suporte as recomendações da arquitetura SAFE da cisco, poderá servir de base para o desenho de futuras arquiteturas de segurança em meios similares ao do estudo deste trabalho.

1.4 - Estrutura de Dissertação

Esta dissertação está estruturada em cinco capítulos, que refletem o trabalho desenvolvido para atingir os objetivos anteriormente apresentados.

No presente capítulo são apresentadas as motivações desta tese e definidos os principais objetivos do trabalho. É ainda descrita a estrutura da dissertação e como esta se encontra organizada com objetivo de transmitir uma visão global deste documento.

No Capítulo 2, é efectuado o levantamento do estado do conhecimento científico na área da segurança, sendo identificados os principais conceitos, modelos e tendências. Posteriormente, no Capitulo 3, são referidas as boas práticas e os desafios na definição de arquiteturas de segurança.

O caso de estudo assim como a análise da arquitetura e os mecanismos de segurança do IPL, são caracterizados no Capitulo 4, sendo também apresentado o modelo de arquitetura de segurança.

No Capitulo 5 é analisada e avaliada a arquitetura, mais concretamente é feita a validação das suas funcionalidades, escalabilidade, desempenho, usabilidade, simplicidade e contribuições ao nível da segurança.

A conclusão da dissertação é efectuada no Capítulo 6, sendo realizado um resumo do trabalho de investigação efectuado concluindo com que extensão foram atingidos os objetivos inicialmente propostos.

2 - Conceitos e Princípios de Segurança

Ao longo da História e acompanhando o processo evolutivo humano, a informação ocupou um papel importante, tendo sido rotulada de fundamental nas últimas décadas. A evolução registada nas TIC foi um dos factores que mais contribuiu para a atribuição deste rótulo, mercê de ter revolucionado a forma de aquisição, trato e partilha da informação.

A informação é decisiva no sucesso das organizações (2), em especial nas que apostam em mercados instáveis e bastante concorridos, sendo fundamental na descoberta e introdução de novas tecnologias.

O aumento da interação social, a evolução do comércio baseado em trocas para um ambiente sustentado e virado exclusivamente para a geração de lucro, fez com que a obtenção de informação para sustentar estas mudanças se tornasse uma obsessão, existindo a preocupação de garantir que a informação do negócio da organização se mantenha segura.

Identificar como tiveram início as primeiras preocupações de segurança relativamente à informação, é algo difícil de referenciar, mas desde sempre existiu a preocupação de garantir a privacidade de alguma informação, particularmente quando esta era considerada importante. Sempre se ouviu dizer "o segredo é a alma do negócio".

2.1 - A tríade CIA

Ao longo de 20 anos, a segurança de informação, sistemas ou computadores tem como pilares os conceitos de confidencialidade, integridade e disponibilidade (3), sendo considerados de fundamentais no processo de segurança. A interpretação destes elementos, denominados de tríade CIA (*Confidentiality, Integry and Availability*) varia em função do meio onde são aplicados.

Estes conceitos representam também as principais propriedades, que, atualmente orientam a análise, planeamento e implementação da segurança para um determinado grupo de informações que se pretende proteger. O desafio no processo de segurança passa por tentar conseguir encontrar o equilíbrio entre os três elementos (4).

Figura 1 - Desafio da segurança

Alguns autores defendem outro tipo de modelos com diferentes particularidades e elementos na abordagem da segurança. Um desses exemplos é o modelo definido por *Parker* constituído por seis atributos (5):

1. Disponibilidade (usabilidade da informação);
2. Utilidade (interesse da informação);
3. Integridade (legibilidade e qualidade);
4. Autenticidade (validade e conformidade);
5. Confidencialidade (observação);
6. Posse (deter e controlar).

De acordo com a ISO/IEC 17799 (6) a segurança da informação deve ser caracterizada tendo em conta a tríade CIA, não esquecendo que o principal objetivo da segurança de informação é proteger a informação de ameaças e vulnerabilidades, minimizando os danos causados por incidentes de segurança e maximizando o retorno dos investimentos da organização.

2.1.1 - Confidencialidade

O conceito confidencialidade diz respeito ao sigilo da informação e à forma de como a proteger. O seu objetivo é garantir, que, unicamente sujeitos autorizados tenham acesso à mesma, independentemente de pertencerem ou não à organização. Este conceito aplica-se em qualquer tipo/formato de informação.

Numa organização, a confidencialidade é um dos conceitos mais importantes a ter em conta, devendo-se identificar toda a informação confidencial e não confidencial. Ao ser comprometida a confidencialidade, muitas vezes compromete-se também a imagem da instituição perante terceiros.

No contexto de rede, o conceito confidencialidade significa garantir que a informação permutada nas comunicações não deve ser visualizada por indivíduos ou mecanismos não autorizados. Aqui, a confidencialidade pode-se repartir entre a confidencialidade de tráfego e de conteúdos. O primeiro tipo permite ocultar os interlocutores constantes na interação; já o segundo esconde os dados trocados entre eles.

Algumas das técnicas usadas com objetivo de garantir a confidencialidade, são:

- Mecanismos de controlo de acesso: Previnem que sujeitos não autorizados acedam aos sistemas;
- Controlos de segurança de sistema de ficheiros: Previnem que sujeitos autorizados a utilizar um sistema excedam os seus direitos e tenham acesso a informações confidenciais ao qual não devem ter acesso;
- Criptografia: Pode ser usada para encriptar os conteúdos de ficheiros sensíveis e ao mesmo tempo protegê-los de olhares atrevidos inclusivamente nos casos em que os mecanismos de controlos de acesso e segurança falham.

2.1.2 - Integridade

A integridade consiste em proteger a informação contra a modificação, sem que o seu proprietário o permita. Além dos dados, deve-se garantir a integridade da origem da informação. Um sistema para ser considerado seguro deve assegurar a integridade da informação.

Exemplo: Imaginemos que um jornal publica uma notícia vinda de uma fonte de informação dentro do governo, mas que a atribui a outra fonte erradamente. Apesar da informação publicada se encontrar correta, a informação deixa de ter integridade por não corresponder à verdadeira fonte.

A proteção da integridade deve ser considerada nas mais variadas formas e formatos, seja de informação armazenada em discos, cópias de segurança ou quaisquer outros formatos.

Nos sistemas financeiros, a integridade é um dos factores de maior importância, pois as transferências bancárias e de títulos têm de garantir a integridade das mesmas, garantindo também que aos dados das transações nada seja acrescentado, retirado ou modificado.

2.1.3 - Disponibilidade

Nos tempos que correm, a informação é um pilar essencial para o desenvolvimento das organizações sendo o seu acesso algo imprescindível. O conceito disponibilidade consiste em garantir que a informação, assim como todos os serviços associados, estejam acessíveis aos utilizadores autorizados. Um sistema indisponível poderá significar perdas de tal forma elevadas como as causadas pela eliminação da informação do sistema.

Existem vários mecanismos com objetivo de comprometer a disponibilidade da informação, um dos mais utilizados passa pela ocorrência de ataques de negação de serviço, também

conhecidos por DoS (*Denial of Service*), onde são realizadas ações com objetivo de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Este tipo de ataque não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

Para garantir a disponibilidade é necessário que existam mecanismos que permitam proteger o *hardware* e *software*, garantindo que em caso de falha a reposição seja célere.

2.2 - Pessoas, Processos e Tecnologia

A informação faz parte dos ativos essenciais para o negócio das organizações, consequentemente, a sua proteção é uma das grandes preocupações. No mundo atual, caracterizado como global e interligado, a informação encontra-se exposta a um conjunto de ameaças e vulnerabilidades que no passado não existiam (7) sendo recomendado que, independentemente do formato utilizado (papel, correio, electrónico, voz,…), a informação seja sempre protegida (7).

Algumas organizações, tentando garantir a segurança da sua informação, recorrem à utilização de mecanismos físicos (cofres) e/ou digitais (criptografia, autenticação), esquecendo que grande parte das informações confidenciais são indevidamente acedidas ou perdidas através de formatos não controlados, como é o caso do papel ou da voz. A perda de informação confidencial pode representar graves prejuízos financeiros, perda de credibilidade e, em alguns casos, o arruinar do negócio.

Numa perspectiva de continuidade da tríade CIA, a segurança de informação é complementada com uma outra tríade constituída por pessoas, processos e tecnologia (8) vista do prisma de grupo de medidas que comprometem as políticas de segurança. O equilíbrio entre todos os elementos deste conjunto (Figura 2) significa melhores resultados na proteção da informação tornando a segurança mais forte, tendo sempre em mente que *a segurança de um sistema é tão forte quanto o seu elemento mais fraco*.

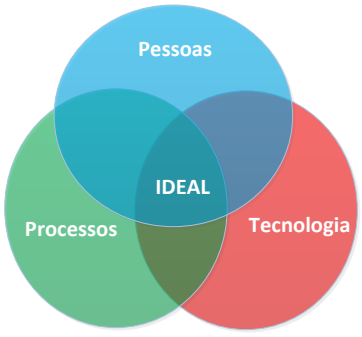

Figura 2 - Relação entre pessoas, processos e tecnologia

O desenho da segurança é algo mais do que a implementação de mecanismos e controlos complexos, com objetivo de facilitar a gestão do dia-a-dia e todos os processos de segurança envolvidos. É olhar para os comportamentos dos utilizadores que lidam com as tecnologias e

perceber que, na maioria das vezes, as pessoas usam os recursos sem estarem alertados e sensibilizados para os problemas de segurança.

Nesta tríade, salta à vista uma fragilidade, as pessoas. O reforço deste elo é extremamente importante no desafio de proteger a informação, não por se considerar o pilar mais importante, mas por ser um ponto de partida essencial para aumentar os níveis de segurança da informação na organização.

A questão que se põe é "Como sensibilizar as pessoas para a importância do seu papel no processo de segurança de informação?"

A resposta a esta questão passa primeiramente por sensibilizar os responsáveis das organizações para a importância deste assunto, apelando à sua participação de forma a reforçar a credibilidade do processo junto dos colaboradores. Os responsáveis detêm também a informação mais relevante e crítica.

Num segundo momento, deve-se promover sessões de segurança com objetivo de consciencializar as pessoas para a importância do seu papel, tornando-as parceiras neste processo. Os princípios e técnicas de *endomarketing*[1] produzem grandes resultados neste tipo de ações (9).

2.3 - Políticas, Normas, Orientações e Procedimentos

Parte da gestão da segurança da informação é determinar como será mantido o processo de segurança na organização. As políticas, normas, orientações e procedimentos permitem ultrapassar este desafio funcionando como mecanismos de controlo, garantindo a consistência e exequibilidade das medidas de segurança, devendo ser aplicados em redor da proteção de informação e dos sistemas que a suportam. Para serem eficazes, devem ser alvo de uma constante análise, monitorização e revisão, garantindo que a sua aplicação está de acordo com os objetivos do negócio e que garantem a segurança da organização (7).

As políticas, normas, orientações e procedimentos (Figura 3) são elementos-chave para garantir que os funcionários e outros saibam as suas responsabilidades e os seus deveres dentro da organização.

[1] Conjunto de ações de marketing institucional dirigida para o público interno.

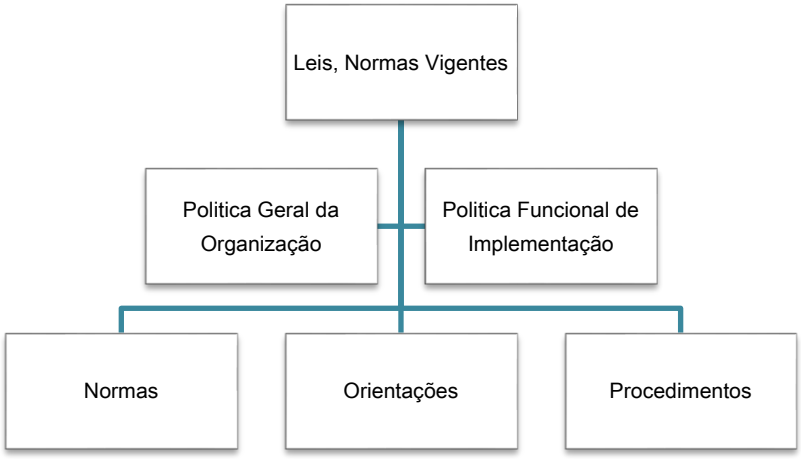

Figura 3 - Relacionamento dos processos de segurança

No processo de definição das políticas de segurança, a administração da organização possui um papel preponderante, definindo quais as políticas a implementar e qual a informação a proteger. Para esta definição, a informação resultante da análise de risco[2], assim como as questões relacionadas com a missão da organização, são fundamentais.

Posterior à definição das políticas, são criadas normas com as regras obrigatórias para as implementar. Algumas destas políticas podem ter várias orientações, que servem como recomendações sobre como executar. Finalmente, os procedimentos consistem em instruções, passo a passo, para ajudar na concretização das diferentes políticas, normas e orientações.

Antes da aprovação de qualquer documento deve existir o cuidado de averiguar se o mesmo está de acordo com as leis/normas vigentes.

De forma resumida, os objetivos de políticas, normas, orientações e procedimentos são:

1. Esclarecer metas e objetivos;
2. Definir funções de responsabilidade e autoridade;
3. Enumerar os direitos e obrigações;
4. Estabelecer as normas;
5. Fornecer informações aos trabalhadores e outros que interagem com a organização;
6. Educar e comunicar.

2.3.1 - Políticas

De todos os documentos da segurança, as políticas pertencem à camada superior. Este documento, oferece uma declaração geral sobre os ativos da organização e qual o nível de proteção que devem ter, sendo constituído por um conjunto reduzido de regras que definem em linhas gerais, o que é considerado pela organização como aceitável ou inaceitável.

[2] Será analisado no capítulo 3.1 -

Quando bem elaborada, a política "responde" às seguintes questões: Quem é o responsável pela segurança? O que se protege? Qual é o nível aceitável de risco? Quais são as medidas a impor aos infractores?

As políticas podem ser vistas como um "plano estratégico" de segurança descrevendo o que deve ser feito mas não indicando como. A decisão de como fazer, é deixada para as normas, recomendações e procedimentos. Uma boa política consegue estabelecer um equilíbrio entre o que é relevante e compreensível. Isto é, se a política for demasiado genérica ninguém vai dar importância ao seu conteúdo porque não se aplica a organização, se a política for muito complexa ninguém a vai ler ou entender.

2.3.2 - Normas

As normas são um documento composto por todas as regras de segurança da organização. Apesar de possuírem um nível de detalhe superior ao encontrado nas políticas, apenas referenciam as tecnologias a usar na organização e a forma segura de como fazer, não chegando ao detalhe de implementação ou operação. Como exemplo, uma norma pode definir como requisito obrigatório que todas as comunicações de correio electrónico da organização funcionem sobre canais seguros, mas nunca indicar qual a marca usada ou modelo para a sua implementação.

O facto de não incluir detalhes de implementação/operação nas normas, faz com que seja conferida alguma intemporalidade ao documento, ficando esse papel para um nível mais baixo da documentação: os procedimentos.

2.3.3 - Orientações/Guia de Boas Práticas

As orientações ou guias das boas práticas são documentos que podem servir de complemento às normas utilizadas. Este tipo de documento pode incluir referência a produtos, configurações ou outros mecanismos com o objetivo de tornar o sistema mais seguro. Existem determinadas áreas onde as recomendações são criadas através de orientações. Por exemplo, numa política, poderá ser necessário realizar uma análise de risco todos os anos. Em vez de ser especificado o procedimento para realizar esta auditoria, poderá ser indicada uma orientação com a metodologia usada para o fazer.

As orientações podem ser vistas como as boas práticas, que não são obrigatórias, mas sim, fortemente recomendadas. Um exemplo de complemento a uma norma utilizada pode passar por uma norma que obrigue a palavra-passe de um utilizador a ser constituída por, pelo menos 8 caracteres. Uma orientação de suporte a esta norma poderá indicar que as boas práticas recomendam que a palavra-passe expire em 30 dias e que possua complexidade elevada.

2.3.4 - Procedimentos

Os procedimentos fazem parte dos documentos de baixo nível (Figura 4) utilizados para descrever detalhadamente como executar as diferentes políticas, normas e orientações definidas na segurança. À medida que se desce na hierarquia dos documentos de segurança, o nível de detalhe vai aumentando, atingindo o máximo nos procedimentos.

Este tipo de documento faz parte da última fase de documentação do processo de segurança, podendo ser utilizado para descrever passo-a-passo: configurações de sistemas, base de dados, *hardware*, *software*, criação de utilizadores, entre outros.

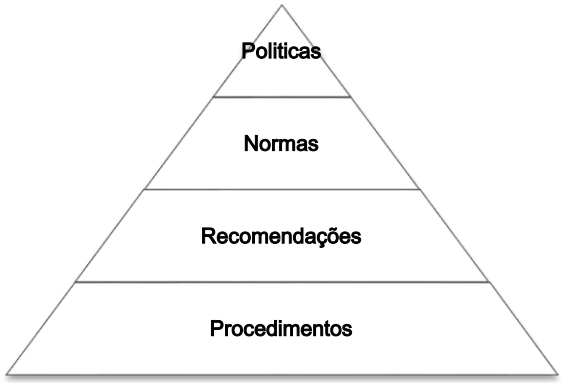

Figura 4 - Hierarquia dos documentos de segurança

Um procedimento pode ser escrito para explicar como instalar o Windows de forma segura, detalhando todos os passos necessários que devem ser tomados para proteger o sistema, de forma a cumprir os requisitos descritos nas políticas, normas e orientações.

2.4 - Segurança de Redes

Durante décadas, a utilização de computadores e sistemas de comunicação esteve apenas confinada em ambientes fechados e controlados a utilizadores com formação especializada (investigadores e universitários). Porém, a evolução registada nos últimos anos permitiu a milhões de pessoas (Figura 5) o acesso a diferentes tecnologias e equipamentos, seja em contexto profissional, pessoal, negócio, entretenimento ou meramente de comunicação.

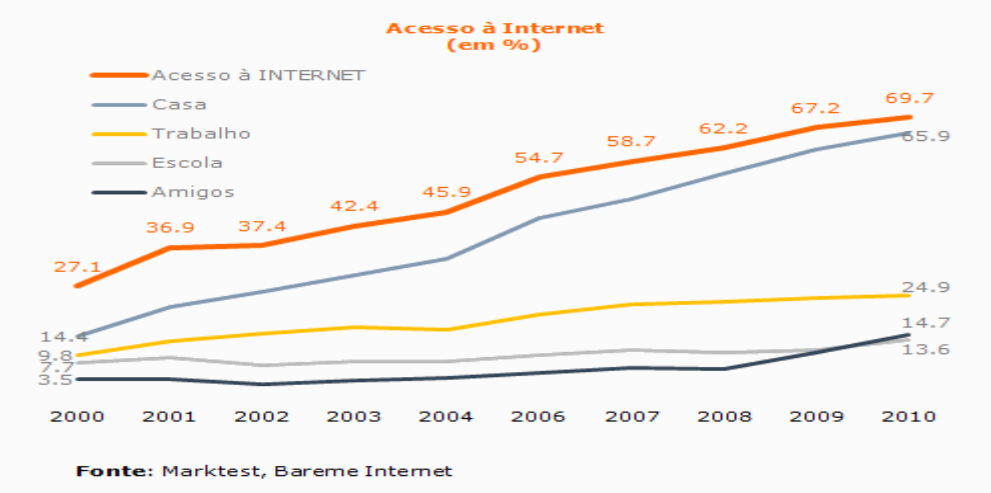

Figura 5 - Evolução registada desde 2000 até 2010 no acesso Internet (10)

Na sociedade atual, as tecnologias atingiram de tal modo o estatuto de essenciais, que é impensável imaginar uma sociedade sem elas. A Internet é um desses casos, onde a sua importância nas comunicações, comércio, ensino e entretenimento é de tal ordem que uma interrupção provocaria custos incalculáveis e provocaria o caos na sociedade em geral.

Em 2001, apesar da sociedade não ser rotulada de tecnologicamente dependente, como acontece nos dias de hoje, a propagação do *worm Code Red* foi responsável pela infecção de 360.000 servidores, tendo então provocado custos estimados na ordem dos $2.6 mil milhões de dólares e perdas de produtividade incalculáveis (11). Se este incidente tivesse ocorrido na sociedade contemporânea, os custos teriam sido bastante superiores.

A massificação do uso das tecnologias fora de ambientes controlados fez com que aumentassem as preocupações e incidentes de segurança. No passado, os utilizadores deste tipo de sistemas detinham formação especializada para o seu manuseamento, neste momento, a maioria não possui formação, o que faz com que não sejam sensíveis para as limitações dos sistemas e para as questões de segurança inerentes ao manuseamento dos mesmos. Para complicar, existem utilizadores mal-intencionados que tentam aproveitar a falta de conhecimentos, ingenuidade dos utilizadores e limitações dos sistemas, com o propósito de obter ganhos financeiros, entre outros benefícios.

Apesar de existirem grandes preocupações com segurança e de a investigação ter aumentado de forma considerável nesta área, a segurança é um problema de grande dimensão. A complexidade dos sistemas, os utilizadores e dispositivos que os constituem, faz com que o controlo da segurança seja bastante difícil de executar, mesmo para os proprietários dos sistemas.

As dificuldades no controlo e implementação de segurança nos sistemas atuais são espelhadas através das seguintes características:

- **Complexidade** – Na maioria dos casos diz respeito ao *hardware* e *software*. Nos últimos anos, em virtude dos avanços ocorridos no *hardware*, a complexidade aumentou de forma considerável. Os computadores pessoais de hoje são mais poderosos que os supercomputadores de há duas décadas atrás, como consequência, o *software* tornou-se mais complexo, sendo na maioria das vezes constituído por milhões de linhas de código. No desenvolvimento do *software*, por vezes, existe um desfasamento entre as intenções do programador e o comportamento real do programa. Este desfasamento é conhecido por bug, que serve para explorar as vulnerabilidades dos sistemas;

- **Interligação** – A característica de arquitetura distribuída que as redes atuais apresentam, juntamente com a complexidade da computação e os ambientes de comunicação existentes impedem os administradores de ter o controlo total sobre as redes a seu encargo. Os limites existentes nas redes por vezes são muito vagos, o que faz com que os administradores não tenham controlo fora do seu domínio, tornando assim os sistemas em rede, vulneráveis a ataques resultantes da conectividade global. Para os males resultantes da interligação global que a maioria dos sistemas atuais apresentam, o desligar o computador da rede poderá ser a única garantia da inexistência de problemas de segurança.

A segurança da rede pode ser equiparada a um jogo, onde de um lado estão os defensores das redes que utilizam técnicas complexas e mecanismos de defesa e do outro, os atacantes que constantemente atualizam as suas estratégias com objetivo de ultrapassar as diferentes barreiras de segurança implementadas. Enquanto existirem interesses e benefícios por detrás dos ataques, este jogo será jogado.

Devido à complexidade, interligação e sua importância, torna-se difícil arranjar uma única definição para a segurança de rede. Os investigadores que se encontram no foco da segurança da informação, investigando sobre privacidade, referem que a segurança deve incidir sobre algoritmos criptográficos e afins. Já para o investigador com interesse em *hardware*, a segurança deve-se focalizar sobre arquiteturas e computação. Independentemente da especialização, a segurança deve olhar para todas as diferentes áreas, o que exige uma especialização completa.

A segurança é um assunto abrangente onde se incluem diversos problemas. Além de ter como missão garantir que pessoas mal-intencionadas tenham acesso a informação destinadas a outras pessoas, deve também garantir que apenas pessoas autorizadas tenham acesso a serviços remotos. A distinção de mensagens verdadeiras de falsas faz também parte das competências da segurança (12).

2.4.1 - Desenho de Redes e Segurança

O défice de comunicação existente entre os fabricantes de tecnologia de segurança e fabricantes de tecnologias de redes é um dos factores que contribui para que a segurança não seja um processo bem definido.

O desenho de redes é um processo com bastante maturidade que se baseia no modelo OSI que oferece modularidade, flexibilidade e utiliza protocolos padrões. Em oposição, o desenho de segurança de redes é um processo mal desenvolvido, onde não existe metodologia definida para gerir a complexidade dos requisitos de segurança.

Quando se pensa e desenha a segurança de redes, deve-se interiorizar que todos os elementos na rede deverão estar seguros. A segurança não diz apenas respeito à segurança dos computadores, mas também ao canal de comunicação utilizado para transmitir dados entre eles. Este não deverá ser susceptível a ataques por *hackers* podendo estes ter acesso aos dados e alterá-los.

Um plano de segurança de rede deve ser elaborado tendo em conta os seguintes cinco importantes serviços (13):

- **Acesso** – Fornecer ao utilizador autorizado os meios necessários para transmitir e receber dados de e para qualquer rede do qual esteja autorizado a comunicar;
- **Confidencialidade** – Garantir que a informação na rede permanece privada;
- **Autenticação** – Garantir que os utilizadores da rede são os que dizem que são;
- **Integridade** – Garantir que a mensagem que circula na rede não seja alterada;
- **Não-repúdio** - Garantir que o utilizador negue que utilizou a rede.

O desenho de um plano eficaz de segurança deve ter em conta várias questões de segurança, tais como: perceber os potenciais atacantes; o nível de segurança necessário a implementar e os fatores que tornam a rede vulnerável a ataques. Estas informações, são essenciais para determinar qual o nível de segurança que a rede ostenta e em que meio ela atua (13).

A utilização de mecanismos de encriptação, autenticação, detecção de intrusão ou *firewalls,* permite diminuir de forma considerável o nível de vulnerabilidade a que um computador se encontra exposto. Muitas organizações recorrem a combinações de diversas ferramentas com habilidade de implementar alguns desses mecanismos, tendo o desígnio da proteção das suas *intranets* que se encontram conectadas com a rede das redes, a Internet.

A Internet é responsável pela introdução de um conjunto elevado de vulnerabilidades em qualquer rede a ela interligada. A compreensão das questões relacionadas com a segurança da Internet, dos ataques a que se encontra exposta, torna-se então num passo essencial para a abordagem da segurança em redes com acesso à Internet e no desenvolvimento de novas tecnologias de segurança.

A segurança de dados consiste em tornar os dados dos clientes ilegíveis para depois serem transmitidos. Este método designado de criptografia permite que, mesmo existindo uma intercepção dos dados, seja necessário uma chave para os tornar perceptíveis. Apesar de bastante válida, a criptografia não é 100% segura, devido a existirem chaves criptográficas

que no passado foram consideradas seguras e que atualmente são facilmente quebráveis. A escolha de chaves e algoritmos recentes e robustos é essencial para que os dados se tornem seguros.

A utilização de dados cifrados numa rede considerada segura, é essencial para diminuir a probabilidade dos dados serem acedidos por terceiros, com objetivo de quebrar a cifra e descobrir a informação. Uma rede segura, irá também prevenir a transmissão de mensagens não autorizadas pela rede (14).

2.4.2 - História da Segurança de Redes

As preocupações de segurança e o interesse nesta área aumentaram após o crime praticado por Kevin Mitnick[3]. Kevin foi responsável pelo maior crime informático na história dos EUA, tendo provocado perdas de propriedade intelectual na ordem dos oitenta milhões de dólares em empresas como Nokia, Nec, Sun Microsystems, Novell, Fujitsu, e Motorola (15). *Os ataques protagonizados por Kevin Mitnick tiveram a particularidade de enfatizar a segurança para a propriedade intelectual.*

A evolução ocorrida graças à informação disponibilizada através da Internet, fez com que houvesse a necessidade da segurança da informação acompanhar as mudanças registadas. A resposta foi dada com aparecimento de novos mecanismos de segurança e simultaneamente através de um olhar mais atento e focado nas questões de segurança.

No passado, os protocolos desenvolvidos para as comunicações foram desenhados sem qualquer preocupação de segurança, não tendo sido contemplada na pilha de comunicações TCP/IP protocolos de segurança, o que levou a que a Internet ficasse vulnerável a ataques. Posteriormente, e devido aos problemas de segurança detectados, surgiram desenvolvimentos na arquitetura tornando assim as comunicações mais seguras.

Cronologia

A história da segurança de rede ou computadores pode-se ter iniciado por volta de 1930, altura em que Alan Turing conhecido por ser um matemático brilhante quebrou o código usado pela máquina Enigma. A Enigma era um dispositivo usado para converter mensagens legíveis em texto cifrado e vice-versa (16). Durante a segunda guerra mundial teve um papel essencial, garantindo a segurança das comunicações.

Por volta de 1960, o termo *hacker* é atribuído a um grupo de alunos do Massachusetts Institute of Technology (MIT). O Departamento de Defesa dos EUA começa a ARPANet[4], que ganha popularidade como um canal de transporte electrónico de dados e informações, abrindo o caminho para a criação da rede conhecida hoje como Internet.

[3] Conhecido por ter sido um dos *hackers* mais famosos (34).
[4] (*Advanced Research Projects Agency Network*) - Conhecida por ter ser a "mãe" da Internet. Foi desenvolvida pela agência Americana ARPA.

Na década de 70, foi desenvolvido o protocolo *Telnet* que abriu a porta para o uso público de redes que inicialmente estavam restritas a empresas, governo e meios académicos.

Nos anos 80, os *hackers* e crimes informáticos começaram a surgir. O gangue 414[5] foi apanhado pelas autoridades pouco tempo depois de ter entrado ilegalmente em sistemas secretos. A lei de fraude informática e de abuso foi criada em 1986 em virtude do crime cometido por Ian Murphy, no qual roubou informações de computadores militares. O estudante Robert Morris foi condenado por ter infectado mais de 6000 computadores ligados à Internet com o *worm* Morris[6]. Alertados e preocupados com o incidente provocado pelo *worm*, foi criado o CERT[7], com objetivo de alertar os utilizadores para as questões de segurança e vulnerabilidades existentes.

Nos anos 90, a Internet tornou-se pública, o que fez com que aumentassem exponencialmente as preocupações de segurança. Atualmente estima-se que 2 biliões de milhões (17) de pessoas utilizem regularmente a Internet, existindo diariamente um número elevado de incidentes de segurança reportados diariamente ao CERT.

2.5 - Ameaças, Vulnerabilidades e Riscos

Nos últimos tempos e mercê da evolução tecnológica ocorrida, a utilização de redes de computadores tornou-se uma dependência, seja para troca de informação, comércio electrónico ou até lazer. Para que haja troca de informação com fiabilidade, garantindo elevada disponibilidade aos intervenientes é necessário que estejam identificadas todas as ameaças que podem coexistir numa rede.

As ameaças podem tomar diversas formas, mas todas elas podem levar a uma perda de privacidade e à destruição maliciosa ou não intencional de informação e recursos.

A capacidade de anonimato e a desindividualização das ações executadas em rede são algumas das características que surgiram com o fenómeno de massificação das redes de longa distância, principalmente no que diz respeito à Internet. Estas fazem com que, na maioria dos casos, seja difícil localizar a origem das ameaças. Nos dias de hoje, um utilizador mal-intencionado facilmente consegue fazer passar-se virtualmente por qualquer outra pessoa, independentemente da sua localização, género ou grupo social, bastando para tal ter acesso aos recursos necessários.

A adopção de mecanismos de identidade electrónica, certificados digitais, autenticação biométrica são alguns dos mecanismos que permitem ultrapassar a "camuflagem" de indivíduos.

---

[5] Grupo de amigos e *hackers* que ganharam notoriedade nos anos 80.
[6] Um dos primeiros *worms* distribuídos pela Internet.
[7] (*Computer Emergency Response Team)* – Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores. www.cert.org.

2.5.1 - Ameaças

Uma ameaça consiste numa causa potencial de um incidente indesejado, que pode resultar num dano para um sistema ou organização (18). As ameaças na maioria dos casos traduzem-se em violações dos sistemas e surgem devido às vulnerabilidades e fraquezas existentes nos mesmos. Os sistemas estão sujeitos a diferentes tipos de ameaças:

- **Interrupção**: permite interromper uma comunicação e proceder à modificação da informação associada a um tipo de transação electrónica;
- **Usurpação**: aproveitamento da informação obtida associada a um tipo de transação electrónica de forma a ser utilizada em proveito próprio;
- **Fraude**: praticada contra elementos de informática, das quais são exemplos a sabotagem informática, o furto de dados e a espionagem informática.

As ameaças podem ser classificadas como:

- **Passivas**: são aquelas que não provocam alteração ou modificação da informação;
- **Ativas**: provocam uma modificação da informação intervindo nos estados de um sistema. Por exemplo descuidos por parte dos administradores de sistemas e falhas de *software* e *hardware*;
- **Acidentais**: não estão associadas a intenções premeditadas. Alguns exemplos de ameaças acidentais são a falta de formação que pode provocar descuidos na gestão da rede;
- **Intencionais**: existe uma intenção premeditada na execução. Podem passar, por exemplo, pela observação de dados com ferramentas simples de monitorização de redes ou então por ataques sofisticados baseados no conhecimento do funcionamento do sistema. Os ataques intencionais podem ser realizados diretamente ou indiretamente. No caso de direto, o intruso incide o ataque diretamente sobre um objeto (para chegar a determinado objeto o intruso pode atacar diversos objetos). Já ao invés, no indireto, o atacante não ataca diretamente o objeto, obtém informação por formas indiretas, por exemplo: estatísticas, escuta de tráfego de rede, perguntas a base de dados ou outros que lhe permitam inferir informação sem lhe aceder diretamente.

2.5.2 - Vulnerabilidades

Vulnerabilidade é um dos poucos conceitos da segurança de informação que levanta poucas dúvidas. É definida como uma falha ou fraqueza existente no *hardware, software* ou num processo que poderá levar a que um sistema seja comprometido.

O NIST define-a como sendo "uma falha ou fraqueza nos procedimentos do sistema de segurança, desenho, implementação ou controlos internos que poderá resultar numa falha de segurança ou na violação da política de segurança do sistema" (19). Já o ITSEC refere que uma vulnerabilidade é "a existência de uma debilidade, desenho ou erro de implementação,

que poderá levar a um evento inesperado e indesejado que pode comprometer a segurança de um sistema, rede, aplicação ou protocolo" (20).

As vulnerabilidades permitem que as ameaças sejam concretizadas, podendo serem desencadeadas de forma intencional ou fortuitamente.

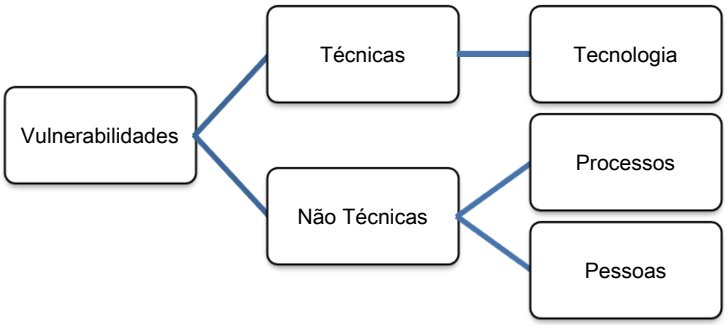

Figura 6 - Tipos de vulnerabilidades

Existem diversos tipos de vulnerabilidades (Figura 6), podendo serem categorizadas de técnicas ou não técnicas. As técnicas possuem como base a tecnologia e todas resultam das falhas existentes nesta. As classificadas de não técnicas, por norma resultam de factores sociais ou processos mal definidos.

2.5.3 - Relação entre Ameaças e Vulnerabilidades

O conceito de vulnerabilidade e ameaça são conceitos adjacentes que por vezes são confundidos, no entanto, são conceitos distintos.

Figura 7 - Relação entre ator, motivação e vulnerabilidade

Uma vulnerabilidade não pode ser explorada a menos que haja uma potencial ameaça e um ator (agente de ameaça). O ator que poderá ser uma pessoa, organização ou até governo, possui motivações que podem ser de diversas índoles (financeiras, políticas,…). O que inicialmente poderá ser considerado de uma ameaça de pequena dimensão, uma

vulnerabilidade poderá transformar numa ameaça recorrente ou de grande dimensão. A relação entre a tríade vulnerabilidade, ator e motivação é visível na Figura 7.

2.5.4 - Risco

Tal como acontece com outros termos, o risco também possui diferentes definições. O NIST definiu-o como sendo "o impacto resultante da probabilidade, que uma ameaça irá exercer numa vulnerabilidade existente num sistema de informação e o resultado que terá este impacto na organização se a ameaça se concretizar" (21). A Microsoft definiu o risco como sendo "a probabilidade de concretização de uma vulnerabilidade ser explorada, levando a um grau de perda de confidencialidade, integridade ou disponibilidade de um ativo" (22).

Para que seja possível correr riscos é necessário fazer a gestão de riscos. Só assim é possível tirar vantagem das oportunidades (e dos riscos inerentes) que surgem. As organizações que tiram proveito desta situação possuem uma durabilidade maior.

Os conceitos de ameaça, vulnerabilidade e risco estão relacionados. A vulnerabilidade é uma característica de um sistema que o torna indefeso a certos ataques, sendo que o ataque tenta tirar partido dessas vulnerabilidades através de um conjunto de ações. Já o risco é o dano resultante da execução de um ataque efectuado com sucesso. Como forma de diminuir as vulnerabilidades existentes, detectar e anular ataques e minimizar os riscos decorrentes dos ataques bem-sucedidos, existem um conjunto de políticas e mecanismos que compõem a defesa.

2.6 - Atacantes, Ataques e Motivações

Um dos passos fundamentais para o sucesso na implementação da segurança numa organização, diz respeito ao conhecimento que temos sobre o inimigo. O responsável pela segurança deve analisar os tipos de "intrusos" existentes, perceber quais os seus perfis e características, que comportamentos tomam, assim como, entender as suas motivações e os ataques praticados.

O general chinês Sun Tzu, autor do livro Arte da Guerra (23), refere na sua obra a importância de conhecer o inimigo com o qual vamos cruzar como sendo determinante na obtenção do sucesso nesta luta.

"Se conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas" (23).

Independentemente da experiência que um responsável pela segurança possui, este deverá ter sempre em conta que existem intrusos com mais experiência e conhecimentos, e que um dia poderá ser confrontado com alguém com mais valências e esperteza.

A imprevisibilidade é uma das características dos intrusos que aumenta consideravelmente a complexidade do trabalho do responsável pela segurança. O administrador, em virtude desta, deverá preparar-se sempre para o pior cenário que poderá ocorrer, ficando assim apto para responder facilmente a intrusos com poucas qualificações.

A complexidade, interoperabilidades e dimensão das redes geridas pelos responsáveis de segurança, são algumas das particularidades que fazem com que estas se tornem também imprevisíveis, aumentando assim os riscos de segurança. Um destes casos sucede quando existem sistemas desconhecidos pelos administradores, que são passíveis de possuir vulnerabilidades, que podem vir a ser exploradas por intrusos.

Um dos exemplos onde salta à vista a imprevisibilidade por parte dos intrusos diz respeito à exploração das vulnerabilidades existentes no *Adobe Acrobat Reader*[8]. Nesta situação, o intruso recorre a uma vulnerabilidade conhecida de um *plugin*, usado diariamente nos *browsers*, para atacar um sistema, podendo assim de forma simples ultrapassar sistemas complexos de segurança, como é o caso de *firewalls*.

As características de imprevisibilidade e saberes avançados, que alguns intrusos apresentam, colocam em causa as medidas de prevenção de segurança. Não basta ter servidores funcionais, atualizados ou recorrer a utilização de mecanismos de segurança de última geração para deixar de correr riscos e de sermos vistos como potenciais alvos de ataque. Independentemente dos mecanismos usados, os intrusos encontram sempre uma forma de superar a defesa.

Estes factores colocam em causa se se deve abdicar da prevenção em prol da recuperação, visto que mais cedo ou mais tarde, podemos sofrer um ataque que nos provoque danos.

A prevenção e recuperação são componentes de segurança que não se substituem um ao outro. Apesar de ser um dado adquirido que a prevenção casualmente falha, não deve ser abandonada, sendo necessária, mas não suficiente como componente de segurança. É preferível prevenir intrusões que recuperar delas. A recuperação é um mecanismo essencial para complementar os casos em que a prevenção não permite resguardar de ataques.

2.6.1 - Atacantes e Suas Motivações

Ao longo dos anos, e acompanhando a evolução ocorrida nas tecnologias, o significado do termo *hacker* tem sofrido diversas alterações. Na atualidade, existem duas definições para o descrever com significados opostos. Um, descreve-o como sendo um entusiástico de computadores que gosta de explorar todos os seus detalhes e capacidades, enquanto o outro, como alguém com objetivos maliciosos que tenta descobrir informações confidenciais ou intrometer-se em sistemas.

[8] Vulnerabilidade Adobe Acrobat Reader http://www.wisec.it/vulns.php?page=9.

No passado, e antes de alcançar um termo depreciativo, o termo *hacker* indicava alguém perito em escrever e alterar programas com conhecimentos avançados possuindo a habilidade de através de programação conseguir que os computadores fizessem "tudo". Ao invés, presentemente são vistos como pessoas que tentam ter acesso a sistemas não autorizados com um conjunto distinto de objetivos onde se inclui o roubo e modificação da informação.

Os acontecimentos históricos e as crises possuem um papel preponderante na conduta dos *hackers* e na seleção dos seus alvos. Nos tempos que correm é frequente ouvir falar acerca de atos de *hacking* com motivos políticos ou sociais, em virtude da crise em que a maioria dos países atravessa. Durante estes períodos, os ataques espelham os sentimentos dos *hackers* sobre os eventos que marcam a atualidade.

2.6.1.1 - Tipos de *Hackers*

Existem diversos subtipos de *hackers* que são qualificados em função das suas filosofias de *hacking.* Os maiores subtipos são, *crackers, hackctivistas* e ciberterroristas.

Crackers

Os *crackers* são classificados como indivíduos com pouca ética nas suas ações e caracterizados por quebrarem a segurança dos sistemas recorrendo a mecanismos obscuros e ilegais. Nos meados dos anos 80, e em virtude da generalização do termo de *hacker* por parte dos meios de comunicação social, os *hackers* que não se reviam em comportamentos criminais, criaram o termo *cracker.* Esta tentativa de diferenciar os entusiásticos de computadores dos criminosos através do termo, revelou-se falhada, visto que os dois termos são frequentemente confundidos.

Apesar das confusões frequentes entre os termos, para o público em geral, os *hackers* puristas referem que as diferenças entre as ações de ambos são discrepantes. Por exemplo, *cyber* terroristas, *cyber* vândalos ditos como *hacker* criminais não são *hackers* mas sim *cracker.*

Ao longo dos tempos, e talvez fruto do amadurecimento, tem-se registado uma tendência de alguns *hackers* em migrar do lado do "mal" para o lado dos defensores da segurança. Aproveitando assim o seu conhecimento e técnicas que outrora foram utilizadas com objetivos maléficos. Em alguns casos, estes *hackers* passaram a colaborar com empresas de segurança ou agências governamentais com objetivo de detetar e corrigir as falhas de segurança.

Hacktivistas

Os *hacktivistas,* são fruto de um "casamento" entre *hackers* e ativistas cuja missão tem como objetivo expressar, destacar ou promover através de meios eletrónicos, o que consideram de causas. Estas podem ser sustentadas com base em motivações políticas, religiosas ou de qualquer outra natureza incluindo por vezes atos de desobediência civil.

Tal como acontece no mundo dos ativistas, também os *hacktivistas* recorrem a diferentes estratégias com objetivo de conseguir fazer passar as suas mensagens. A aplicação prática

pode implicar recorrer a métodos de *hacking* como, bombardeamento automático através de mensagens de correio electrónico, *web defacing*[9], *virtual sit-ins*[10], assim como vírus e *worms*.

***Ciber*terroristas**

A crescente utilização tecnológica fez aumentar quase de forma exponencial a utilização dos sistemas computacionais, tornando dependentes deles alguns sistemas cruciais para uma sociedade, como é o caso dos sistemas de comunicação, os sistemas bancários, rede elétrica ou até o controlo de tráfego (aéreo, marítimo e rodoviário).

A dependência da utilização da Internet e a sua característica de interconexão global, a partir da qual é possível aceder a todos os sistemas a ela ligados, fez surgir um novo tipo de terrorismo, o chamado ciberterrorismo. Este tipo tem como objetivo o aproveitamento do ciberespaço para a condução de ações terroristas, podendo em determinados casos, as suas ações possuírem um poder disruptivo e impacto social de dimensões incalculáveis.

Um ataque, para que possa ser considerado como ciberterrorismo, terá que ter como objetivo a interrupção ou controlo de um serviço essencial sendo sustentado com base em motivações políticas e/ou religiosas.

2.6.2 - Ataques

A confidencialidade, integridade, privacidade e disponibilidade são atributos essenciais no contexto de segurança. Existem diversos tipos de ataques que em função do seu tipo afectam estes atributos. A relação entre o tipo de ataque, os atributos de segurança afectados e os tipos de mecanismos usados para prevenir este tipo de ataques é observável na Tabela 1.

Atributo de Segurança	Método de Ataque	Mecanismo de proteção
Confidencialidade	*Eavesdropping, Hacking, Phishing, DoS, IP Spoofing*	*IDS, Firewall, Criptografia, IPSec, SSL*
Integridade	*Virus, Worms, Trojans, Eavesdropping, DoS, IP Spoofing*	*IDS, Firewall, Anti-Malware, IPSec, SSL*
Privacidade	*Email bombing, Spamming, Hacking, DoS, Cookies*	*IDS, Firewall, Anti-Malware, IPSec, SSL*
Disponibilidade	*DoS, Email bombing, Spamming, System Boot Record Infectors*	*IDS, Anti-Malware, Firewall*

Tabela 1 - Métodos de Ataque e Proteções de Segurança (24)

Os ataques mais comuns podem ser divididos em diversas categorias. Alguns, como é o caso de *eavesdropping* ou *phising* conseguem obter informações dos sistemas ou informações pessoais. Outros, possuem a capacidade de interferir no funcionamento dos sistemas como

[9] Desfiguração de sítio electrónico com objetivo de mudar aparência visual.
[10]Forma de desobediência civil eletrónica.

acontece com os vírus, *worms e trojans*. Existem ainda os que consomem os recursos dos sistemas sem necessidade e que são denominados de ataques DoS ou DDoS.

Eavesdropping

Este tipo de ataque consiste na intercepção de comunicações por parte de alguém não autorizado para o fazer. O ataque passivo *eavesdropping* consiste apenas na escuta das mensagens de rede, ao invés no modo ativo, o atacante escuta e introduz algo na comunicação (24).

Vírus

Programas que se podem replicar e espalhar entre computadores. Uma vez executados os ficheiros contaminados com o vírus, o mesmo fica ativo no sistema. A probabilidade de contaminação é maior quando a infeção acontece em unidades de rede (24).

Worms

Similares aos vírus na capacidade de multiplicação. Ao contrário dos vírus, não existe necessidade de abrir ficheiros para que ocorra propagação. Existem dois tipos principais de *worms*: os *mailing worms* e os *network-aware*. Os *mailing worms,* utilizam como meio o correio electrónico de forma a infectar outros computadores. Os *network-aware worms* fazem parte dos problemas graves de segurança da Internet. Este tipo possui a particularidade de selecionar o alvo a atacar, e quando acede a este, procede à sua infecção através de um *trojan* ou de outro meio (24).

Trojans

Os *Trojans* pertencem à categoria de programas maliciosos para os utilizadores finais. O programa atua como um cavalo de Tróia, permitindo, tal como na lenda, ao atacante ter acesso ao sistema. Os *trojans* atuais tentam passar por programas legítimos.

Phishing

O *phising* é um tipo de ataque que surgiu nos últimos anos com objetivo de aproveitar a falta de conhecimentos por parte dos utilizadores. Tem como finalidade obter informações confidenciais de individuais, grupos ou organizações, tais como dados pessoais, números de cartão de crédito ou outra qualquer informação sensível. Este tipo de ataque, por vezes, baseia-se no envio de uma mensagem de correio electrónica fraudulenta, tentando passar por instituições credíveis de forma a enganar o utilizador.

Ip *spoofing*

Ataque que consiste em mascarar o endereço IP do atacante com o endereço de outro indivíduo, permitindo assim esconder a identidade durante um ataque o que dificulta a detecção e prevenção do mesmo. Este tipo de ataque permite também fazer passar por outro utilizador através do uso do mesmo endereço IP, tendo assim os acessos ao qual a vítima tinha direito. Este tipo de ataque é conhecido como sendo um ataque cego, visto que apesar de ser

feita a falsificação de um remetente, as respostas irão sempre para o endereço original falsificado.

Negação de serviço

Conhecido também por DoS, este ataque tem como finalidade tornar os recursos de um sistema indisponíveis para os seus utilizadores. O atacante aguarda até ter a confirmação que o serviço fica indisponível. O alvo típico deste tipo de ataque são os servidores Web. Existem ataques de negação de serviço que são feitos de forma distribuída (DDoS), onde um computador controla vários computadores distribuindo as tarefas de negação de serviço por eles.

2.6.3 - Fases de um ataque

De forma a perceber o processo de detecção de intrusos é necessário entender todas as ações que fazem parte de um ataque. Um ataque é constituído por cinco fases sendo elas: reconhecimento, exploração, reforço, consolidação e pilhagem (Figura 8).

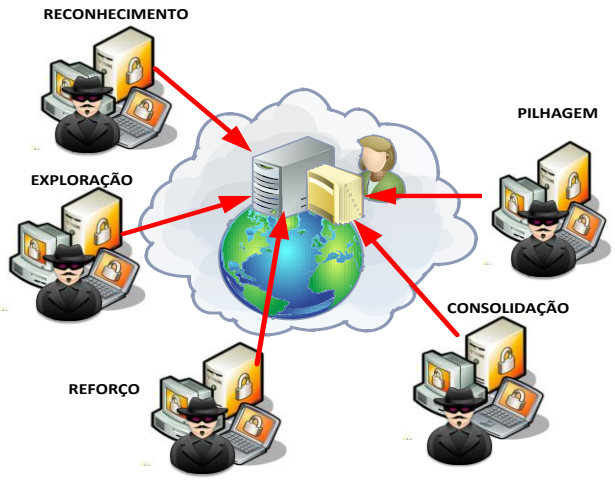

Figura 8 - As cinco fases de um ataque

2.6.3.1 - Reconhecimento

Na fase de reconhecimento, o intruso tenta reunir o máximo de informação possível sobre a vítima antes de iniciar o ataque. Nesta fase, é feita a validação da conectividade entre ambos, o levantamento de serviços a correr e análise de vulnerabilidades susceptíveis de virem a ser exploradas. Os intrusos que verificam e trabalham as vulnerabilidades antes de procederem à fase de exploração possuem maior probabilidade de sucesso na exploração do alvo.

Geralmente durante esta fase e antes do ataque são realizadas algumas atividades relevantes de *hacking* com dois objetivos:

1. Melhorar a probabilidade de êxito na operação do ataque;
2. Aumentar a probabilidade de anonimização do atacante (esconder a identidade do atacante).

O reconhecimento, não tem que ser obrigatoriamente realizado recorrendo a técnicas ou conhecimentos apurados, por vezes poderá ser um processo pouco técnico, que poderá ser feito através de diferentes tipos de mecanismos/técnicas de onde se destacam as seguintes:

- Engenharia Social;
- Reconhecimento Físico;
- Reconhecimento através de Internet;
- Reconhecimento da Rede;
- Reconhecimento DNS.

Quando o reconhecimento é realizado sem existir interação entre o atacante e a vítima, diz-se que o mesmo é feito de forma passiva. Este tipo pode ser tão simples como identificar as pessoas que entram e saem de um prédio. Outros exemplos são: o ato de pesquisar na Internet informação relativa a um indivíduo ou empresa; a engenharia social; o "*dumpster diving*[11]" e a escuta de redes.

Já ao invés, no reconhecimento ativo, o atacante interage com a vítima com objetivo de adquirir as informações necessárias. O reconhecimento da rede com objetivo de descobrir máquinas, endereços e serviços de rede é um desses casos. Este tipo, permite ao atacante ter acesso a um conjunto vasto de informação mas aumenta consideravelmente o risco do atacante ser detectado durante as manobras de reconhecimento.

2.6.3.2 - Exploração

A exploração de um ataque diz respeito ao passo em que o atacante comete o abuso/violação sobre o alvo. Por vezes um abuso de um serviço consiste em fazer uso ilegítimo de um modo legítimo de acesso. Poderá parecer um contra censo, mas esta situação acontece quando por exemplo, um atacante acede a um sistema autenticado ao qual não está autorizado, fazendo uso de um utilizador e palavra-chave "roubadas" através de engenharia social ou qualquer outro método de extorsão.

O *subversion* consiste noutro tipo de exploração que tem como objetivo a manipulação dos serviços de forma a terem comportamentos não previstos pelos programadores, tirando assim benefício das suas vulnerabilidades. Um exemplo deste caso é a vulnerabilidade conhecida

[11] Ato de vasculhar lixo.

como *Buffer Overflow in Core Microsoft Windows DLL*[12] do servidor Microsoft IIS[13] indiciada no CERT em 2003 que permite a quem explore a falha ter controlo total do sistema.

Ao invés do *subversion***,** que não provoca falhas nos serviços, apenas explora as suas vulnerabilidades, a violação faz com que o serviço deixe de funcionar e o atacante ganhe acesso ao sistema com os mesmos privilégios que o serviço possuía antes da falha.

Na maioria das vezes, o processo de exploração com o recurso a *exploits* obriga que os atacantes comuniquem com as vítimas recorrendo aos protocolos usados diariamente e respeitando os seus padrões. Esta obrigação poderá traduzir-se numa desvantagem para os intrusos, devido ao aumento do risco de detecção durante o cumprimento das regras de comunicação. Noutros casos, os atacantes não necessitam de seguir os padrões definidos devido a existirem serviços que quando confrontados com dados inesperados e comportamentos inadequados estes acabam por "morrer".

2.6.3.3 - Reforço

O reforço, diz respeito à fase em que os atacantes tentam aumentar os privilégios sobre os computadores e/ou sistemas comprometidos na fase de exploração. A utilização de determinados tipos de *exploits* na fase de exploração, permite que o acesso aos sistemas seja feito com o modo mais privilegiado de permissões, ao passo que outros apenas garantem acesso com permissões de utilizador. Para estes casos, os atacantes necessitam de encontrar uma forma de escalar os privilégios para o modo mais elevado tendo como meta a obtenção do controlo total sobre o sistema comprometido.

A transferência das ferramentas necessárias para o escalonamento de privilégios, por diversas vezes é feita recorrendo a protocolos como FTP ou TFTP. Noutras situações, e em virtude das limitações impostas pelos privilégios dos utilizadores, é necessário recorrer a protocolos cifrados como é o caso do SCP[14].

Os atacantes com conhecimentos avançados, por norma, transferem as suas ferramentas recorrendo aos mesmos canais de comunicação utilizados para realizar o exploit das vítimas.

As ferramentas colocadas nas vítimas permitem aos intrusos ter o controlo sobre o sistema da vítima, conseguindo adicionar contas, remover registos de atividade dos sistemas, disfarçar processos e ficheiros que sejam provas da presença ilegítima do atacante.

Em casos mais avançados são instalados túneis que permitem através do sistema comprometido comunicar com o exterior, seja através de canais cifrados ou através de túneis

[12] Referência a vulnerabilidade no CERT http://www.kb.cert.org/vuls/id/111677.
[13] Servidor HTTP criado pela Microsoft.

[14] O protocolo SCP (*Secure Copy)* é idêntico ao protocolo RCP do BSD com a diferença que os dados são cifrados durante a transferência de forma a maximizar a segurança.

ocultos. Este tipo de mecanismos são conhecidos por *backdoors* e permitem usar os sistemas para realizar ataques a terceiros.

2.6.3.4 - Consolidação

O processo de consolidação ocorre quando o atacante ou intruso comunica com o sistema da vítima recorrendo ao *backdoor*. Este mecanismo, pode ter a forma de serviço que se encontra à "escuta" e ao qual o atacante se liga ou de um sistema que aguarda por uma sequência específica dos campos do protocolo IP, TCP… para ser ativado. Outra das hipóteses é ser o próprio *backdoor* a estabelecer comunicação entre o sistema comprometido e o atacante. Este tipo de ferramenta, por norma, possui a particularidade de ser silenciosa, não se notando a sua presença.

A opção de instalação de um *backdoor* por parte do atacante quando existe a hipótese de utilizar o método do *exploit* é questionável, mas é explicada pelas seguintes possibilidades:

1. Utilização de *exploits* que impliquem falhas no sistema que apenas são ultrapassáveis através do reiniciar do mesmo;
2. Correção de vulnerabilidades por parte do administrador de sistema e consequente perda de acesso ao sistema;
3. Risco de ataque e correção de vulnerabilidades por parte de terceiros perdendo-se o controlo do sistema;
4. Menor risco de detecção de *backdoor* por parte de mecanismos de IDS.

2.6.3.5 - Pilhagem

Quanto alcançada esta fase, o atacante está prestes a cumprir o seu plano, que poderá consistir no roubo de informação sensível, construir uma base sólida para efetuar ataques incisivos dentro da organização ou proceder às etapas de reconhecimento e exploração com objetivo de atacar outros sistemas. Esta fase corresponde à fase de maior exposição do atacante perante o administrador de sistema.

Por norma, os intrusos tentam passar despercebidos tendo sempre o máximo cuidado para não chamar à atenção nem deixar rasto, limitando a sua ação à de "observador" de tráfego. Esta análise permite a recolha de dados dos colaboradores legítimos da organização, possibilitando em qualquer altura assumir a sua identidade dentro da organização.

Nas organizações em que a prevenção e detecção têm como foco quase exclusivamente os atacantes externos, descorando assim as possibilidades internas, um atacante interno à organização passa despercebido ao responsável pela segurança.

Fase	Objetivo	Risco Detecção	Vantagem Intruso	Desvantagem Vitima
Reconhecimento	Descobrir máquina, servidores, aplicações e serviços	Médio a Elevado	Os intrusos durante vários períodos recorrem a padrões de tráfego para fazer a descoberta de máquinas e serviços	Diferenças consideráveis entre o tráfego gerado pelo intruso e a da vítima
Exploração	Abuso, violação de serviços	Médio	Intrusos podem explorar serviços escondendo *exploits* no tráfego	Alguns dos *exploits* são identificados como trafego ilegítimo pelos IDS
Reforço	Utilização de ferramentas para escalar privilégios ou disfarçar presença	Elevado	Encriptação permite esconder as ferramentas	Facilidade de fechar o tráfego de saída dos servidores
Consolidação	Comunicação via *backdoor*	Baixo a médio	Com total controlo sobre o sistema basta usar a criatividade	O perfil de tráfego pode revelar padrões pouco comuns
Pilhagem	Roubo de informação	Baixo a médio	Quando se opera através de uma suposta máquina de confiança a atividade do atacante poderá ser difícil de detectar	Administradores mais atentos sabem os padrões de tráfego que as suas máquinas possuem sendo fácil de detectar desvios

Tabela 2 - Diferentes estados e riscos durante as fases de um ataque

Durante as diferentes fases que compõem um ataque existem diferentes riscos que se encontram sintetizados na Tabela 2.

2.7 - Modelo de Segurança em camadas

Em 2008 o SANS[15] propôs um modelo de segurança de redes (NSM – *Network Security Model*) constituído por sete camadas, à semelhança do modelo OSI, desenvolvido em 1983 pelo *Internationl Organization for Standardization* (ISO). O NSM surgiu com a finalidade de colmatar a falta de um modelo genérico de segurança de redes que pudesse ser aplicado em qualquer implementação de segurança ou dispositivo.

Física
VLAN
ACL
Software
Utilizador
Administrativo
Departamento TI

Figura 9 - Modelo de Segurança de Redes

[15] Sysadmin, Audit, Network, Security Institute http://www.sans.org.

O processo de detecção de falhas no modelo OSI (Figura 9) é feito através da análise de todas as camadas do modelo no sentido baixo para cima, até encontrar a camada responsável pela falha. No modelo NSM o diagnóstico é feito no sentido contrário, ou seja, de cima para baixo. Detetada a camada onde teve origem o ataque, pode-se concluir que todas as camadas acima também falharam. Este tipo de funcionamento, além de permitir que rapidamente seja detetado se o ataque comprometeu outros, permite também definir como proteger a infraestrutura de futuros ataques iguais ao ocorrido.

2.7.1 - Camada Física

A camada física diz respeito a toda a segurança física da infraestrutura, sejam servidores, computadores ou outros equipamentos. A sua finalidade é prevenir os atacantes de aceder às instalações e com isso ter acesso aos dados que se encontram armazenados nestes equipamentos.

O motivo de ter sido escolhida para a primeira camada do modelo, deve-se ao facto de ser considerada um dos maiores pontos de falha em qualquer rede.

O que vale ao administrador de rede possuir mecanismos de controlo avançados como *firewalls*, se fisicamente podem ser acedidos pelos atacantes e comprometidos desta forma?

No NSM, quando ocorre uma falha de segurança em qualquer camada abaixo da camada física, significa que a camada física também fracassou, isto porque o atacante consegue manipular os dados como se se encontrasse dentro da infraestrutura.

Proteção da camada física

De todas as camadas existentes no NSM, a camada física é a mais fácil de garantir a sua segurança, não necessitando de recorrer a tecnologias avançadas. O modelo NSM proposto pelo SANS indica cinco formas de aumentar a segurança da camada física:

1. **Segurança exterior** – Quando o tipo de informação é considerada crucial e de extrema importância deve-se considerar a proteção do exterior dos edifícios através da inclusão de dispositivos físicos tais como: cercas, arame farpado, barreiras…;
   Este tipo de medidas apenas faz sentido para infraestruturas militares e governamentais que suportem o armazenamento de informação vital;
2. **Dispositivos de controlo de acesso** – Apesar de arcaicos, a utilização de mecanismos de controlo como portões, portas e fechaduras (mecânicas ou eléctricas) produzem resultados eficazes no controlo de acesso a infraestrutura de suporte à informação;
3. **Alarmes** – Os alarmes são considerados os melhores mecanismos na segurança da infraestrutura física de rede. Estes mecanismos podem estar ligados diretamente a uma central de segurança e alertar automaticamente em caso de intrusão;
4. **Câmaras** – Fazem parte do último mecanismo recomendado no modelo NSM para a proteção da camada física. Quando vistos, funcionam na maioria das vezes como elemento intimidador. Estes tipos de elementos devem ser distribuídos pelos espaços

considerados cruciais no acesso ao Centro de Dados e também dentro do próprio Centro de Dados.

Para complementar os mecanismos de segurança física é recomendado a existência de seguranças. Além de poderem controlar os acessos aos edifícios e salas, por parte de pessoas autorizadas, podem também alertar para atividade suspeita em redor dos edifícios.

2.7.2 - Camada VLAN

A camada VLAN do modelo NSM diz respeito à utilização de VLAN no contexto da segurança. Uma VLAN é uma rede local que agrupa um conjunto de computadores e/ou servidores de maneira lógica e não física, comunicando independentemente da sua localização e como se pertencessem a um único domínio *broadcast* ou rede lógica (25).

As VLAN são um mecanismo importante no contexto de segurança, permitindo agregar grupos de computadores com as mesmas características e objetivos. A diferenciação de departamentos com características diferentes dentro de uma organização faz parte das boas práticas, devido ao facto de não existir partilha de informação comum.

Proteção da camada VLAN

O modelo NSM refere que o primeiro passo na implementação de segurança através de VLAN é definir quais são as redes públicas e privadas. As redes públicas destinam-se a equipamentos/dispositivos externos, tais como: DNS, FTP, servidores de Web, ao invés, as redes privadas, albergam os utilizadores e dispositivos internos. Por uma questão de organização e segurança, as VLAN internas deverão ser subdivididas por departamento.

As VLAN são consideradas um elemento essencial no modelo NSM, permitindo organizar o acesso por parte de utilizadores a dispositivos/servidores. A implementação de segurança em VLAN depende de mecanismos de controlo de acesso como ACL. Apesar de fazer sentido associar as VLAN e ACL numa camada apenas, o modelo NSM não contemplou esta opção justificada pela possibilidade de alterações frequentes nas VLAN sem que estas sejam reflectidas nas ACL e vice-versa.

2.7.3 - Camada ACL

A camada ACL diz respeito à criação e manutenção de listas de controlo de acesso que podem ser aplicadas em *routers, switches* e *firewalls*. O seu funcionamento consiste em permitir ou negar o acesso entre computadores, redes e VLAN. Um conjunto de ACLs bem escritas permite aumentar o nível de segurança da infraestrutura para um nível elevado, apesar de não ser suficiente, uma vez que o processo de criação de ACLs é muito delicado. Um pequeno erro numa ACL poderá significar uma porta aberta para utilizadores não autorizados e uma restrição para utilizadores autorizados.

Segurança da Camada ACL

O segredo para a criação das ACL passa por permitir apenas o essencial, seja tráfego de entrada ou de saída. Se uma instituição necessitar de acessos vindos somente do exterior com destino aos seus servidores Web através de HTTP e HTTPS deverão ser criadas apenas ACL que permitam a entrada de tráfego com destino ao porto 80 e 443. A existência de ACL desnecessárias ou de grande dimensão fazem com que o processo de segurança seja uma tarefa difícil de manter para o administrador de segurança.

Por norma, os administradores preocupam-se na maioria das vezes com concepção de ACLs de entrada destinadas a tráfego que tenha origem na internet e o destino seja a rede da organização ou rede interna. Na fase de desenho de ACLs, o administrador deverá também preocupar-se com o tráfego de saída, permitindo apenas o necessário e restringindo tudo o resto.

O processo de criação de ACLs obriga que o administrador de redes possua um conhecimento de todos os fluxos de comunicação, assim como de todas as portas envolvidas (sejam de origem ou de destino).

A capacidade de permitir e negar tráfego com destino aos serviços necessários, a proteção da camada de *software* através do bloqueio do acesso a serviços que possuem vulnerabilidades conhecidas e a capacidade de permitir identificar os danos causados por um ataque a um computador/servidor comprometido, são algumas das mais-valias que justificam as ACLs como um elemento importante no modelo NSM.

2.7.4 - Camada *Software*

A camada *software* é responsável por uma quantidade significativa de problemas de segurança. O modelo NSM, nesta camada, realça a importância de manter o *software* atualizado e corrigido, evitando assim a exploração de vulnerabilidades por parte dos atacantes. Uma das preocupações por parte do administrador de segurança é de saber quais os *softwares* que estão instalados, as suas versões e atualizações efectuadas. Antes de proceder a alguma atualização ou correção, o administrador deverá saber quais as suas implicações, assim como os problemas que vão ser resolvidos.

Segurança da Camada *Software*

Uma das formas de implementar segurança nesta camada é a de aplicar as últimas correções e atualizações disponíveis. Esta ação é muito importante em *software* de servidor tais como *Apache*[16], *IIS,* que se encontram bastante expostos, sendo por vezes, desafios tentadores devido aos serviços que suportam. Se um servidor possui vulnerabilidades conhecidas, os atacantes vão tentar tirar proveito delas para conseguirem entrar no sistema.

[16] Servidor Apache criado em 1995 por Rob McCool cerca de 48% dos servidores HTTP são suportados por este *software.*

O conhecimento dos serviços que estão a correr num determinado servidor é um aspecto fundamental na segurança, permitindo, em caso da existência de padrões anormais de tráfego destinado a esses serviços, suspeitar que algo possa ter sido comprometido.

A camada *software* no modelo NSM é a primeira camada que sendo comprometida permite o acesso aos recursos de rede e permite também que toda a informação existente no servidor seja acedida por parte do atacante. Isto acontece porque já se ganhou acesso ao servidor.

2.7.5 - Camada Utilizador

O utilizador possui um papel preponderante na questão da segurança da organização. O modelo NSM refere que, reforçando o conhecimento dos utilizadores acerca das questões de segurança de redes, permite que exista o seu auxílio na detecção e alerta de possíveis problemas de segurança, que serão ou não, confirmados posteriormente pelos administradores de segurança.

O reforço do conhecimento do utilizador deverá ser feito através de: informação sobre conhecimentos básicos de segurança; alerta para os perigos existentes; noções de funcionamento do sistema e por fim indicação das aplicações autorizadas na organização.

Segurança da Camada Utilizador

A forma de aumentar a segurança da camada utilizador do modelo NSM, consiste em formar os utilizadores nos sistemas e aplicações que utilizam no dia-a-dia. Se perceber como funciona o seu sistema, o utilizador facilmente consegue detectar anormalidades no seu funcionamento, alertando o administrador para esse facto. Um sistema que, sem razão aparente, fica lento, será motivo de alerta por parte do utilizador. O administrador deverá então averiguar se as razões da lentidão dizem respeito a problemas de segurança ou a outro motivo.

A segurança da camada utilizador é muito importante, porque se for comprometida, a conta do utilizador também o será, permitindo que o atacante faça uso das suas credenciais para ter acesso a dados que anteriormente estavam inacessíveis. Os atacantes, apesar da camada administrativa ser mais aliciante, escolhem por questões de estratégia a camada utilizador como alvo dos seus ataques. Esta estratégia é tomada em virtude da vulnerabilidade dos utilizadores e ao facto de serem menos entendidos no contexto da segurança. Por vezes, as técnicas utilizadas para efetuar este tipo de ataques, baseiam-se em técnicas de engenharia social.

2.7.6 - Camada Administrativa

A camada administrativa é bastante idêntica à camada utilizador. A grande diferença diz respeito ao nível e importância da informação com que os membros desta camada lidam no dia-a-dia.

Segurança da Camada Administrativa

Os administradores devem ser "treinados" com os mesmos mecanismos referidos na camada utilizador mas atingindo um nível mais detalhado. Tendo em conta a responsabilidade dos seus cargos na organização é importante passar uma preocupação relativa aos assuntos de segurança, dando assim credibilidade ao processo perante todos. O seu papel preponderante na inclusão de novos funcionários na organização, tendo a missão de ensinar as boas práticas de segurança no dia-a-dia. Na maioria dos casos, funcionam como interface entre o utilizador e os administradores de segurança, comunicando a estes quando um utilizador carece de ajuda, tornando assim o processo mais célere.

À medida que se baixa nas camadas que constituem o modelo NSM proposto pelo SANS, as consequências resultantes do comprometimento tornam-se mais devastadoras. No caso da camada administrativa falamos de utilizadores com contas de altos privilégios com acesso a informação sensível e muitas vezes confidencial.

2.7.7 - Camada Departamento TI

O departamento TI é composto por todos os profissionais da organização que trabalham nesta área. Nele constam técnicos responsáveis pela área de segurança, técnicos de rede, especialistas de suporte, gestores de serviços e gestores de rede. Ao comparar com a camada anterior do modelo, encontramos bastantes semelhanças, com a diferença que as contas utilizadas pelo departamento TI possuem os privilégios máximos de administrações.

O departamento TI é responsável por implementar e controlar o modelo NSM na organização.

Segurança da Camada Departamento TI

Para o reforço da segurança é essencial que todos os elementos do departamento possuam conhecimentos de segurança, percebam a estrutura de rede e saibam as bases da política de segurança em vigor na organização.

A ocorrência de uma falha de segurança nesta camada poderá tornar toda a infraestrutura de rede vulnerável. O atacante, em virtude dos privilégios atribuídos aos utilizadores do departamento TI, facilmente consegue ter acesso a dispositivos de rede (*routers*¸ *firewalls*, servidores) podendo controlar ou paralisar a rede da organização. O resultado de um ataque desta natureza poderá representar perdas financeiras elevadas para a organização, além de afectar a sua imagem.

2.7.8 - Relação entre o modelo NSM e o modelo OSI

Se analisarmos o modelo NSM (Tabela 3) podemos constatar que a sua estrutura é bastante similar à apresentada pelo modelo OSI. Esta semelhança não é uma coincidência, mas sim devido ao modelo OSI, com a sua estrutura invertida ter servido de base para a criação do NSM como modelo de segurança. Tal como o modelo OSI, o NSM é um modelo composto

por sete camadas, com a particularidade de quando uma camada falha todas as camadas acima falham também.

Modelo NSM	Modelo OSI (Invertido)
Física	Física
VLAN	Ligação Lógica
ACL	Rede
Software	Transporte
Utilizador	Sessão
Administrativo	Apresentação
Departamento IT	Aplicação

Tabela 3 - Comparação das camadas do modelo NSM e modelo OSI invertido

Nestes dois modelos é possível estabelecer uma comparação entre todas as camadas (Tabela 4).

Modelo NSM		Modelo OSI (Invertido)	
Camada	**Característica**	**Camada**	**Característica**
Física	Aspectos relacionados com a segurança física da infraestrutura	Física	Ligação física da rede
VLAN	Segmentação de VLANs	Ligação Lógica	As segmentações são feitas na camada ligação e com base nos endereços MAC
ACL	Implementação de ACL	Rede	As implementações de ACLs são feitas com base na camada rede e possuem como base os endereços IP
Software	*Software*, atualizações e correções de segurança	Transporte	Descreve como é feita a comunicação entre ambas as extremidades da ligação *Software*
Utilizador	Utilizador que tem a capacidade de utilizar a máquina local	Sessão	Lida coma comunicação naquela máquina local
Administrativo	Utilizadores administrativos que tem a capacidade de direcionar utilizadores	Apresentação	Como os dados são direcionados
Departamento IT	Manutenção de todas as camadas garantindo que toda a rede funciona corretamente	Aplicação	Apresentação dos dados

Tabela 4 - Relação entre o modelo NSM e modelo OSI invertido

A camada física em ambos os modelos diz respeito aos aspectos físicos da rede. No NSM o seu foco está relacionado com a segurança física da infraestrutura, já no modelo OSI com os aspetos relacionados com a ligação física da rede.

Na segunda camada, tanto a camada VLAN do NSM como a camada ligação no OSI, operam com VLAN e endereços MAC.

Na terceira camada, ambas lidam com endereços IPs. Enquanto a camada ACL do NSM tem a seu cargo a implementação de ACL, no modelo OSI a camada cobre o endereçamento IP.

Na quarta camada, ambas lidam com as ligações na rede entre máquinas. No que diz respeito ao modelo NSM esta preocupa-se com o *software* e suas correções, enquanto no OSI descreve como se procede a comunicação entre ambas as extremidades das ligações de *software*.

Na quinta camada, em ambos os modelos existe relação com a máquina local. Se no NSM a camada diz respeito ao utilizador que é capaz de usar a máquina local, já no OSI, esta camada lida com a comunicação naquela máquina local.

Na sexta camada, em ambos os modelos o assunto está relacionado com funções administrativas. Se no caso do NSM diz respeito a utilizadores administrativos que têm a capacidade para encaminhar utilizadores, já no OSI a camada diz respeito à forma como os dados são direcionados.

Por fim na última camada, o departamento IT do modelo NSM é responsável pela manutenção de todas as camadas e por garantir que toda a rede funciona corretamente. Já a camada aplicação no modelo OSI é responsável pela apresentação dos dados.

2.7.9 - Implementação do Modelo NSM

O sucesso da implementação do modelo NSM depende da estratégia adoptada para este efeito. Para tal, é recomendado estruturar a implementação num conjunto de níveis de segurança com diferentes medidas. A progressão de nível está associada ao aumento do grau de complexidade das ações a implementar, e só será feita depois de cumpridas as metas propostas nas camadas do modelo. Na implementação é essencial que seja atribuída a mesma importância a todas as camadas que compõem o modelo.

As boas práticas para a implementação deste modelo aconselham que numa primeira fase, todas as camadas sejam trabalhadas da mesma forma de um modo superficial. Já numa segunda, deve-se aprofundar as questões de segurança em todas as camadas.

A Tabela 5 enumera algumas medidas a implementar em ambas as fases para todas as camadas.

Medidas/metas		
Camada	**Fase 1**	**Fase 2**
Departamento TI Administrativa Utilizadores	Fornecer literatura sobre segurança de redes aos elementos destas camadas; Literatura de carácter mais técnico para os elementos do departamento TI;	Aprofundar os conhecimentos sobre segurança de rede de todos os elementos; Mostrar como a segurança afecta o seu a dia-a-dia; Tornar a camada humana mais forte;
Software	Verificar se o *software* está atualizado e possui as últimas correções de segurança;	"Olhar" para o *software* instalado e tomar decisões acerca do *software* a remover; Decidir quais as permissões que os utilizadores dos sistemas devem ter;
ACL	Se não estiverem implementadas ACLs, escrever ACLs genéricas; Se existirem proceder à sua análise e introduzir melhorias;	Criar novas VLANs para segmentar a rede; Criar ACLs para controlar o tráfego; À medida que se criam VLANs devem ser colocadas na rede de forma a permitir apenas o necessário restringindo tudo o resto;
VLAN	Verificar se existem VLANs implementadas, se sim qual o seu objetivo e onde estão aplicadas; Se não existirem deve-se criar VLANs genéricas;	
Física	Verificar se existe alguma segurança física implementada, se não existir implementar medidas de segurança em geral;	Aplicar fechaduras com controlo de acessos; Câmaras em redor e dentro da infraestrutura;

Tabela 5 - Mecanismos de implementação do modelo NSM

Existem algumas máximas que devem ser cumpridas para que a aplicação do modelo NSM atinja os objetivos esperados. A ter em conta:

1. Nenhuma camada se deve sobrepor a um processo em curso noutra camada;
2. Não é necessário implementar medidas de segurança de rede por nenhuma ordem específica;
3. Todas as camadas do modelo devem trabalhar coordenadamente, tal como acontece no modelo OSI.

2.8 - Perímetro de Segurança

Os dias de garantir a segurança de uma organização, recorrendo a uma barreira bem definida, como se de um muro se tratasse deixando de fora os mal-intencionados, acabaram. As empresas e organizações alteraram os seus modelos de negócio e a forma de colaborar com parceiros, clientes e funcionários, o que fez com que fossem removidas "barreias e proteções" e abertas portas traseiras.

Surgiram novos tipos de terminais que anteriormente eram considerados como internos e com os novos desafios passam a integrar o perímetro. O desafio passa por conseguir definir uma solução forte que proteja todos os ativos existentes e acessíveis na infraestrutura.

2.8.1 - O que é um Perímetro

No passado, a definição de perímetro era simples de definir. Podia por exemplo ser um castelo para proteger a sua aldeia. Nestes casos é fácil de definir, visualizar e criar uma política de proteção para proteger as fronteiras do perímetro estabelecido.

Antes do perímetro IT se ter transformado uma barreira dinâmica, um *firewall* era tudo o que era necessário para definir e estabelecer o perímetro de segurança. Dentro do *firewall* a zona era considerada de confiança e segura, já fora do *firewall* insegura.

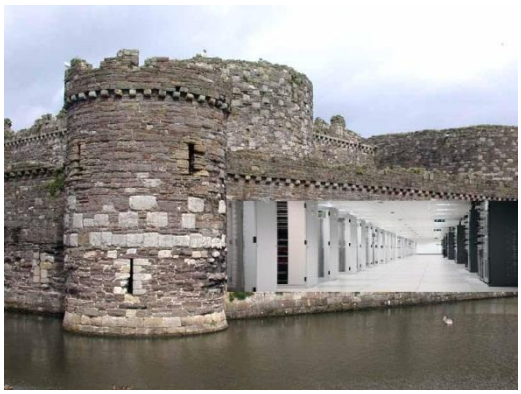

Figura 10 - Perímetro de segurança

Atualmente, o perímetro é cada vez mais definido por cada nó que compõe a rede. Além disso, os protocolos e dispositivos das redes atuais conseguem ultrapassar facilmente as barreiras tradicionais de segurança de perímetro. Alguns desses exemplos são:

- Aplicações que ultrapassam as políticas de *firewalls;*
- Dispositivos móveis;
- Pontos de acesso sem fio que são instalados sem autorização;
- Acesso direto à internet em alguns dispositivos.

A utilização das aplicações por parte dos utilizadores é o objetivo primordial. Por vezes, para facilitar o seu uso dão-se acessos excessivos às aplicações, o que permite ultrapassar a política de segurança estabelecida.

Os dispositivos móveis possuem a particularidade de se conseguirem mover e ligar a várias redes em diferentes localizações. Alguns pontos de ligação podem ser feitos no perímetro da organização, outros nem por isso. Isto requer que os dispositivos móveis funcionem em determinadas vezes como perímetro da organização.

O aparecimento das redes sem fios teve como consequência o aumento de ameaças nas redes das organizações. Redes desprotegidas e a introdução de pontos de acesso sem fio não autorizados, representam um dos maiores buracos de segurança nas infraestruturas de segurança.

O acesso direto à Internet através de qualquer dispositivo é um dos atributos mais difíceis de controlar. Este tipo de dispositivos podem ser pessoais e quando ligados diretamente a um computador da organização permitem ultrapassar as barreiras de segurança. A definição do perímetro deve ter este tipo de acesso.

2.8.2 - Evolução do Perímetro de Segurança

O termo de perímetro de segurança é um termo bastante amplo que possui um conjunto diferente de implicações e significados e que tem evoluído, acompanhando assim a história nas TI.

No início da era digital, os sistemas existentes eram constituídos por computadores individuais de grande porte e encontravam-se localizados em salas seguras. A entrada e saída de dados nesses sistemas era feita recorrendo fisicamente à sala onde estavam alojados. Os mecanismos de segurança resumiam-se a garantir a segurança física do local e a existência de mecanismos de controlo de acesso ao local (26).

O perímetro encontrava-se bem definido e a segurança encontrava-se num nível físico.

Posteriormente foram introduzidos terminais com teclados e monitores, ligados diretamente a um sistema constituído por um computador central. Ao contrário da fase anterior, a entrada de dados podia ser feita através de várias localizações sendo apenas condicionada a uma determinada distância máxima do computador central. Os mecanismos de controlo faziam parte integrante do computador.

Perímetro bem definido mas com aumento de problemas na segurança física.

O aparecimento de dispositivos de acesso remoto veio permitir a comunicação direta entre computadores, terminais e o sistema central. A introdução deste tipo de comunicações

contribuiu para a introdução de novos mecanismos de controlo de acesso. A camada de controlo de acesso ao sistema central deixa de ser suficiente.

Apesar dos sistemas serem remotos, o perímetro encontrava-se bem definido. Foi necessário criar mecanismos adicionais de controlo de acesso, de forma a controlar o acesso feito pelos utilizadores. Diversos utilizadores tinham acesso ao mesmo CPU, logo tinha que existir autenticação.

O paradigma de um ponto único de acesso mudou drasticamente com a disseminação da internet, interligando os sistemas de grande porte. O aumento do poder de computação fez com que os sistemas se tornassem pessoais e domésticos deixando de existir a necessidade de autenticação local no contexto referido anteriormente. A utilização de *modems* para ligar a Internet e posteriormente as redes de alta velocidade de banda larga, permitiram que os PC se ligassem em rede e se agrupassem.

À medida que os sistemas cresceram e se tornaram mais potentes, surgiu a necessidade de acesso remoto aos sistemas das organizações. Além de promover o ambiente de trabalho em casa, o acesso remoto permite a interligação com a rede da organização aos colaboradores que se encontram fora, dando assim acesso a todos os recursos internos. O acesso remoto é implementado na maioria dos casos recorrendo a *virtual private networks* (VPN) sobre uma ligação Internet. Como consequência do acesso remoto, a autenticação teve que ser reintroduzida de forma a salvaguardar problemas de segurança nos sistemas acedidos remotamente.

O acesso à Internet não se confinou apenas a computadores pessoais como no passado. Surgiram diversos dispositivos sem fios e dispositivos móveis que permitem o acesso à Internet em qualquer lugar e consequentemente acesso ao ambiente corporativo da organização.

Uma das dificuldades resultantes dos sistemas e aplicações serem independentes é a dificuldade de localizar onde as aplicações se encontram alojadas ou em que computador a aplicação é executada. Dispositivos como telefones ou máquinas industriais possuem a capacidade de aceder à Internet e permitir, por vezes, o acesso remoto.

O Perímetro tornou-se difuso, qualquer dispositivo pode ser o perímetro. Na maioria dos casos são dispositivos móveis que o compõem.

O perímetro tornou-se numa barreira dinâmica que tem de ser redefinida e protegida. Os sistemas que interagem com o perímetro da rede tornam a rede dinâmica, devendo ser protegidos através da criação de um perímetro para sistemas que seja capaz de fazer parte do perímetro de rede. Outro desafio existente é a dificuldade em controlar no perímetro as aplicações que disponibilizam acesso via *browser* e que correm em dispositivos locais. As ferramentas tradicionais de perímetro não são suficientes para tal.

2.8.3 - Definir o Perímetro

No passado, conhecer todo o desenho da rede era de extrema importância para a manutenção da segurança. Atualmente e se cada nó é considerado o perímetro da rede, conhecer o desenho da rede é uma mera questão quando comparada com os limites do perímetro.

O facto de as redes serem extremamente dinâmicas faz com que seja importante o responsável pela segurança estar sempre vigilante das alterações ocorridas. Deve existir uma avaliação e análise contínua da rede de forma a serem identificados quaisquer abusos ou mau uso dos recursos.

2.8.3.1 - Ferramentas de Análise

Existem duas abordagens possíveis na análise do perímetro e todo o tráfego que circula de/para o perímetro. Uma primeira abordagem consiste na utilização de ferramentas de monitorização em modo passivo, enquanto a segunda, na utilização em modo ativo.

Modo Passivo

A utilização de um *scanner* de rede e vulnerabilidades permite descobrir os dispositivos ligados na rede e saber quais as suas capacidades na rede. Além de descobrirem a rede, detectam vulnerabilidades existentes nos dispositivos encontrados. Este tipo de aplicações possui a capacidade de detecção de computadores de secretária, servidores, *routers*, *switches*, *firewalls* e dispositivos de segurança. Quando são identificados, o *scanner* analisa as configurações, as correções de segurança existentes, sistema operativo e aplicações instaladas, assim como, todas as vulnerabilidades existentes que podem vir a ser exploradas.

Estes tipos de ferramentas são consideradas de passivas porque apenas fazem *scan* quando são invocadas manualmente. O *Nessus*[17], *IBM Proventia Network Enterprise Scanner*[18] *e QualysGuard*[19] *Vulnerability Managment* são algumas das ferramentas que estão incluídas nesta categoria.

Modo Ativo

Este tipo de ferramentas funciona 24x7, monitorizando os padrões de tráfego, comunicações e dados transmitidos. Com os dados recolhidos, permite criar uma "fotografia" da rede com os padrões de comunicações existentes entre os dispositivos que constituem a rede. Estes dados garantem uma visão completa de todo o perímetro existente na infraestrutura.

A atividade de uma ferramenta de monitorização ativa permite ainda detectar tráfego anormal, ameaças de segurança, atividades que abalem a performance da rede ou violações de políticas existentes.

---

[17] http://www.nessus.org/products/nessus.
[18] http://www-01.ibm.com/software/tivoli/products/network-enterprise-scanner/#.
[19] http://www.qualys.com/products/qg_suite/vulnerability_management/.

Dentro da categoria de ferramentas de modo ativo destacam-se alguns exemplos como é o caso de: *Peakflow SP: Traffic Anomaly Detection*[20] e *IBM Proventia Network Anomaly Detection System*[21].

2.8.4 - Zonas de Rede

Um conceito chave na definição dos perímetros consiste em segregar a rede criando diferentes zonas de segurança. A utilização de *firewalls* de perímetro, para segmentar áreas importantes deixou de ser suficiente, devendo todas as áreas da rede pertencer a uma zona de segurança e todos os nós possuírem a capacidade de atuar como perímetro.

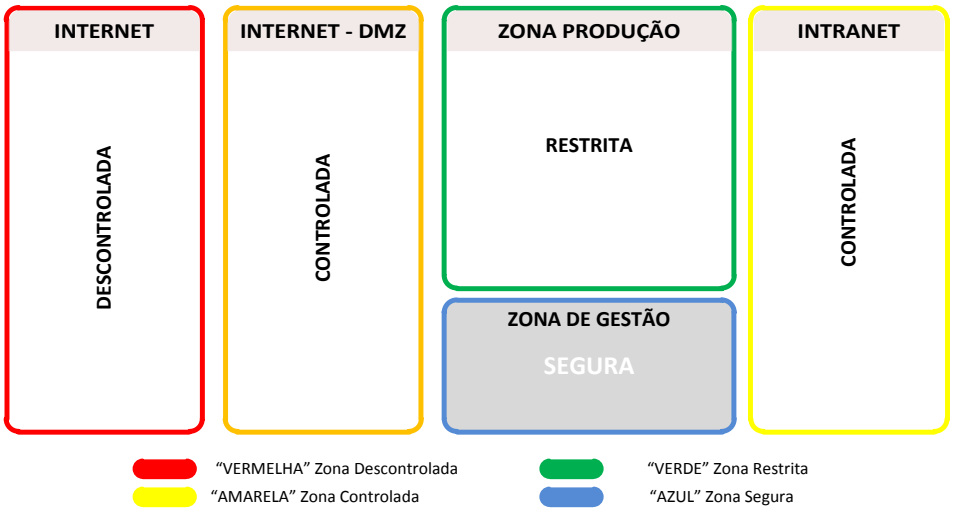

Figura 11 - Diferentes Zonas de Segurança

A criação de zonas de segurança (Figura 11) carece da classificação dos diversos componentes da zona, assim como a definição dos diferentes tipos de mobilidade e classificação existentes. A adopção da estratégia de criação de zonas permite limitar os incidentes e violações de segurança às zonas onde ocorreram.

Os perímetros de rede possuem a particularidade de isolar zonas com políticas de segurança diferenciadas. Esses limites servem para implementar restrições no tipo de tráfego que é permitido na zona. Os *firewalls* são os equipamentos que possuem a capacidade de permitir e negar o tráfego, implementando a política de tráfego de rede. São também responsáveis por criar limites entre duas ou mais redes, atuando como se de um escudo se tratasse. Apesar de serem importantes mecanismos de segurança, tornam-se insuficientes quando compõem a única linha de segurança da organização.

[20] http://www.arbornetworks.com/peakflowsp.
[21] http://www-935.ibm.com/services/uk/en/it-services/ibm-proventia-network-anomaly-detection-system-ads.html.

2.8.4.1 - Classificação

Atualmente, a classificação foca-se quase exclusivamente na classificação de dados e utilizadores, sendo que, apesar da importância na classificação da infraestrutura de comunicações e *hardware*, esta é negligenciada na maioria das vezes.

Os esforços investidos no QoS fizeram com que a classificação das comunicações ficasse descurada. Apesar do esforço, o resultado ficou aquém, resumindo-se à priorização ou não do tipo de tráfego que circula na rede.

Para que uma classificação seja feita corretamente, deve-se efetuar a classificação de forma a determinar quando, onde e como, deve ser aumentada ou diminuída a proteção da classes analisadas. As classes a ter em conta numa classificação são: utilizadores; dados; *hardware e c*omunicações (Tabela 6).

Classe	Descrição
Utilizadores	A classificação dos utilizadores depende da correspondência dos utilizadores aos recursos com que interagem na rede. Deve ser feita uma disciplina de gestão de identidades. Os utilizadores devem ser definidos tendo em conta o acesso que necessitam assim como a sua localização dentro da topologia de rede. Nas definições dos utilizadores deve estar incluído a zona de segurança ao qual o utilizador pertence.
Dados	É uma área com bastante maturidade que está mais virada para a classificação do conteúdo dos ficheiros do que dos dados. Apesar de por vezes a política da organização não permitir o armazenamento de ficheiros em discos locais, os utilizadores conseguem-no fazer em determinadas ocasiões. A classificação dos dados em algumas organizações é implementada através dos mecanismos de *backup*. Deve-se verificar se a classificação de dados atende os padrões de qualidade e se é realmente tida em conta.
Hardware	A classificação de *hardware* é focada nos ativos tangíveis dentro da organização. Os computadores de secretária são considerados itens imóveis quando alojados em salas com acesso controlado. Os computadores móveis devem ser classificados separadamente como dispositivos de trabalho móvel em virtude de puderem estar expostos a pessoas externas se não forem devidamente protegidos. As mesmas considerações devem ser tomadas para os telefones móveis devido à possibilidade destes dispositivos puderem armazenar dados classificados. As impressoras por norma encontram-se localizadas em salas de impressão com acesso restrito enquanto que os servidores em salas limitadas e muito controladas. Atualmente existem alguns *gadgets* nas organizações, tais como discos externos, leitores MP3, leitores de cartões que podem ser considerados como perímetro e que devem ser incluídos na classificação de *hardware* e de dados.
Comunicações	A criação de zonas de segurança permite classificar todas as comunicações existentes na rede. As comunicações devem ser classificadas de forma a identificar o tráfego legítimo e o que não é. Existem diversas decisões que são baseadas no tráfego tais como: qual o tráfego que atravessa a *firewalls*, sistemas de detecção de intrusão e quando e onde é necessário efetuar autenticação de utilizadores.

Tabela 6 - Classificação de Classes

2.8.4.2 - Mobilidade e Conectividade

A mobilidade (Figura 12) é um dos conceitos essenciais nas questões de segurança. De forma a garantir a segurança é necessário que seja examinada a mobilidade de todos os nós que compõem a rede, incluindo outras redes que por alguma razão acoplam com a rede. As redes sem fio devem ser analisadas/investigadas tendo em conta as questões de segurança de toda a infraestrutura de rede. A forma como os utilizadores móveis se ligam à rede da organização é outro dos factores que deve ser revisto.

Figura 12 - Mobilidade e conectividade de utilizadores

Conectividade em redes de área local

A conectividade em redes locais é expectável de existir em qualquer local numa organização. No entanto, a existência de conectividade poderá ser vista como uma falha de segurança. Na utilização de zonas de segurança, uma porta de rede configurada numa zona de segurança qualquer, poderá significar uma porta de entrada para qualquer utilizador mal-intencionado, permitindo assim ignorar os mecanismos de segurança implementados.

A utilização de uma infraestrutura baseada em tecnologia sem fios destinada a utilizadores internos, visitantes, clientes ou fornecedores da organização, poderá ser uma solução para os problemas de segurança referidos. Nesta abordagem, devem ser criadas zonas de segurança destinadas aos diferentes tipos de utilizadores, que após a sua autenticação, serão movidos para estas.

Outra abordagem, consiste na utilização de tecnologia de autenticação na rede local. Esta solução garante que apenas utilizadores e/ou dipositivos com privilégios consigam ter acesso à rede local, negando o acesso a todos os restantes.

Conectividade em redes sem fios

Atualmente, a maioria dos dispositivos móveis existentes vêm equipados com dispositivos sem fios que permitem ter acesso a redes sem fios em qualquer hora e local. No mundo global de hoje, existem inúmeros locais que permitem ter conectividade à internet, seja em cafés, aeroportos, hotéis,… Uma vez ligados à Internet, qualquer dispositivo consegue facilmente ter

acesso às redes locais das organizações, seja através do uso de VPN ou outra qualquer solução.

A conectividade sem fios em locais fora da organização permitiu que os utilizadores estejam disponíveis em locais que no passado não seria possível. Apesar da capacidade de presença ter aumentado, a utilização de redes sem fios desconhecidas fez que tenham surgido problemas de segurança e com que o perímetro da organização e a sua segurança tenha sido alargado até ao utilizador em particular.

As redes sem fios tiveram a capacidade de fazer com que as redes internas das organizações ficassem disponíveis a desconhecidos e não mais limitadas aos perímetros dos edifícios.

Portas dos dispositivos

Muitos perigos de segurança numa organização surgem através de portas USB. Seja através de discos portáteis, leitores MP3 ou até ligações de acesso à Internet não organizacionais. Para resguardar a organização de ataques desta natureza é necessário utilizar *software* de monitorização de ligações USB em dispositivos portáteis, computadores de secretária e servidores. Existem poucas tecnologias que permitem fazer o log da atividade proveniente de portas USB.

2.8.5 - Segurança do Perímetro

Na maioria dos casos, aquando a implementação de segurança é dada primazia à utilização de mecanismos que protegem a rede, descurando-se a segurança individual nos dispositivos. Os antivírus são uma exceção a esta situação, sendo uma ferramenta usada há longos anos e vista como essencial na maioria das organizações.

A utilização de mecanismos de proteção de rede, deixa de ser suficiente quando cada sistema com capacidades de rede compõe o perímetro de segurança da organização. Para este desafio, devem ser aplicadas soluções que protejam os dispositivos individualmente, os dispositivos de rede e que consiga combinar ambos.

Os perímetros de segurança são constituídos por diversos tipos de dispositivos. Os mais utilizados são computadores de trabalho, servidores e dispositivos móveis. Os computadores de trabalho são usados para tarefas de serviço podendo existir mais que um utilizador a aceder ao sistema simultaneamente. Os servidores, por norma são colocados em locais centrais, sendo o acesso a estes dispositivos feito através de serviços especiais, como é o caso de partilha de ficheiros, impressoras ou aplicativos.

Apesar de todos os dispositivos utilizarem a infraestrutura de rede com as mesmas características, o administrador tem que estar preparado para lidar com tipos de ataques distintos em servidores e computadores de trabalho. As medidas de proteção a aplicar nestes dispositivos também devem ser distintas.

O comportamento relativo às questões de segurança é diferenciado em função do tipo/importância do dispositivo. Por exemplo, a aplicação do bloqueio de um serviço num

computador de trabalho como contra medida de resposta a um incidente de segurança, terá um impacto reduzido na organização. Pelo contrário a aplicação de uma medida da mesma natureza num servidor poderá ter consequências enormes.

A definição de perímetro pode ser resumida dizendo que o perímetro encontra-se em frente do administrador. Qualquer computador, qualquer dispositivo com capacidade IP na organização compõe o perímetro e deverá ser tratado como tal.

As questões de segurança são bastantes ambíguas devido a determinadas condições e ambientes que as rodeiam. Por exemplo, na leitura de um documento, será que podemos assumir que o documento não sai do perímetro de segurança da organização? Um documento pode ser controlado através de autenticação para garantir que o mesmo é acedido por pessoas autorizadas dentro do perímetro de segurança. E se este documento for impresso, conseguimos garantir?

Que classificação é dada a um documento? Um documento até pode ser classificado de público, mas será que quando está em elaboração também o é? Ou será classificado de privado?

O utilizador, por norma, não tem noção do tipo de acesso que utiliza na leitura e acesso a dados. Não sabe e não tem interesse em saber o meio utilizado no acesso à Internet e a sua segurança. Preocupa-se sim com a facilidade e conveniência.

A conveniência é uma característica delicada na segurança. Na maioria das vezes tende a ser priorizada em relação ao acesso a dados de forma segura, abdicando da segurança em prol da facilidade. Esta forma de estar conduz a problemas de segurança nas organizações.

A questão inerente é que qualquer caminho que seja utilizado no acesso inicial a dados, deve ser tido em conta quando se considera o perímetro, seja através de uma ligação de rede ou através de um dispositivo USB. O perímetro inicia-se onde os dados se movem. Se os dados movem-se de forma intencional e dentro dos limites da política de classificação e de mobilidade então tudo está de acordo com o estabelecido.

A proteção dos dados que se movem de forma não intencional pode ser efectuada recorrendo a uma combinação de mecanismos que permitem a proteção das redes utilizadas pelos dispositivos móveis e a proteção dos dispositivos de forma individual. Esta abordagem permite perceber onde chega o perímetro dinâmico e como proteger os dados que circulam sobre ele.

2.8.6 - Considerações

Existem determinadas considerações que devem ser tomadas na implementação de detecção, proteção e análise de sistemas quando se pretende definir ou redefinir o perímetro de segurança. Algumas passam por abandonar métodos e definições que deixaram de ser válidos para os desafios atuais, enquanto outras pela adopção de novas estratégias e conceitos, tais como:

- Os *firewalls* como mecanismo único de segurança não são suficientes para garantir a segurança do perímetro;
- Os *firewalls* controlam o tráfego, mas não previnem um ataque realizado através de uma porta aberta conhecida;
- Os *softwares* de antivírus são reativos;
- O controlo de aplicações é essencial;
- Computadores, servidores e dispositivos móveis devem ser tratados de forma igual no que diz respeito a conteúdos maliciosos;
- Apesar de não ser suficiente, a autenticação de utilizadores deve ser sempre usada;
- As redes internas são constituídas por uma mistura de tecnologias onde a maioria das vezes os utilizadores navegam livremente entre elas, escolhendo a que mais lhe convém.

O processo de redefinição de perímetro é uma tarefa demorada onde no seu percurso vão ser palmilhados caminhos sem saída. A chave do sucesso para a sua proteção encontra-se no utilizador, já que o "seu" *host* compõe o perímetro. O utilizador deve por isso, estar habilitado, educado para se tornar responsável pelas suas ferramentas de trabalho e cumprir controlos e os regulamentos da organização.

Esta página foi intencionalmente deixada em branco

3 - Boas Práticas no Desenho de Arquiteturas de Segurança

A metodologia apresentada não podia ter outra base de suporte que não a velha máxima de que não se pode gerir e controlar aquilo que não se conhece, ou por outras palavras, que não se podem tomar decisões sem se saber onde é necessário intervir e com que se conta.

Neste capítulo, para além da gestão de risco que é fundamental em qualquer organização vai ser introduzida a arquitetura de referência de segurança SAFE. Posteriormente vão ser tidas em conta as evoluções das aplicações e os desafios de segurança resultantes desse avanço. Serão também analisados os *firewalls* da próxima geração como mecanismos que respondem aos desafios e ameaças atuais.

3.1 - Gestão de Risco

A gestão de risco é o processo de reconhecimento de um conjunto de medidas que permite conferir à organização o nível de segurança pretendido. Este processo é um componente importante do programa de segurança de informação, sendo composto por um conjunto de fases em que os riscos são determinados e classificados. Posteriormente são enumeradas medidas de segurança, que possuem a missão de reduzir ou eliminar os riscos a que a organização se encontra exposta.

A principal missão do processo de gestão de risco não é o de proteger apenas os ativos de informação, mas sim proteger a organização e a capacidade que esta tem para realizar a sua missão. Logo, o processo de gestão de risco não deve ser tratado como uma função técnica executada pelos responsáveis de segurança, mas sim como uma função de gestão essencial da organização e à organização.

Para que seja possível correr riscos é necessário fazer a gestão de riscos. Só assim é possível tirar vantagem das oportunidades (e dos riscos inerentes) que surgem. As organizações que tiram vantagem desta situação possuem uma durabilidade maior.

A gestão de risco é a agregação de três processos que possuem as suas raízes em leis, regulamentos e diretivas. Os três processos são: avaliação de risco, mitigação de risco e avaliação (Figura 13).

Figura 13 - Processo Gestão de Risco

Muito resumidamente, a avaliação de risco tem como função determinar onde se encontram os riscos e qual a sua dimensão. Já a mitigação de risco, possui a responsabilidade de avaliar, priorizar e implementar controlos com objetivo de minorar o risco. Por fim, a avaliação, considerada crucial para o processo de gestão de risco, caracterizada por ser contínua e evolutiva. Antes do início de um novo ciclo a gestão de risco deve ser avaliada e determinada.

3.1.1 - Gestão de Risco Reactivamente ou Proativamente

Existem duas correntes metodológicas que permitem realizar o processo de gestão de riscos, uma recorre a estratégias reativas enquanto a outra a proativas. No passado, a abordagem utilizada consistia na utilização de métodos reativos que se baseavam na análise feita a acidentes ocorridos.

A forma de encarar os problemas por parte da abordagem reativa, foi responsável pela atribuição do título pejorativo de "escola de gestão de risco do *Indiana Jones*" (26). A mítica frase "*Don´t worry, I´ll think of something"* nos filmes de *Indiana Jones* ao qual este herói recorria perante situações de dificuldade, fez com que surgisse esta graça. Este é o comportamento natural quando se utiliza a abordagem reativa. Ou seja, não se preocupar com os problemas até que eles sucedam.

A estratégia reativa pode ser abordada de duas formas. A mais positiva, está em constante monitorização na procura de riscos conhecidos. Se algum deles se tornar um problema efetivo, existem recursos reservados e prontos a lidar com o risco. Num segundo modo (mais comum), nada é feito até que um incidente ocorra.

Neste tipo de abordagem, os seguintes pontos são utilizados para gerir os incidentes de segurança:

- Proteger a vida humana e a segurança das pessoas;
- Conter os danos;
- Avaliar os dados;
- Determinar causa do dano;
- Reparar os dados;
- Rever resposta e atualizar política.

3.1.1.1 - Abordagem Proativa

A abordagem proativa (Figura 14) é uma estratégia inteligente de gestão de risco. Num primeiro momento são identificados os potenciais riscos, para depois ser efectuada a avaliação de probabilidade e de impacto, classificando-os por relevância. Com base na informação recolhida é elaborado um plano de gestão de risco. O seu objetivo é evitar o risco, mas sabendo de antemão que não é possível ser infalível perante todos os riscos.

Uma abordagem proativa eficaz poderá reduzir significativamente o número de incidentes de segurança na organização, sem que estes desapareçam definitivamente.

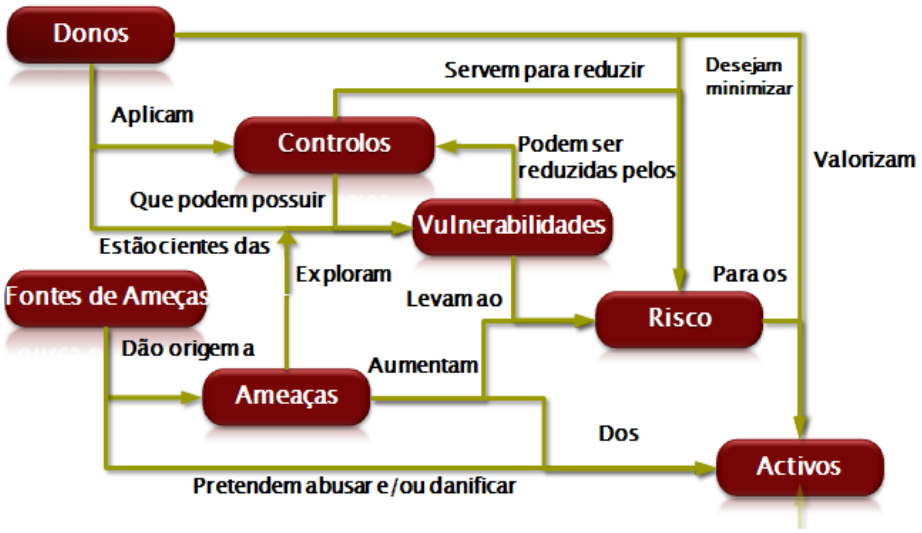

Figura 14 - Visão da abordagem proactiva

No desenvolvimento do plano de resposta, deve ser tido em conta a utilização de ambas as metodologias. O objetivo é complementar a abordagem reativa com a proativa, garantindo assim o melhor das duas metodologias.

Para a elaboração de uma abordagem proactiva deve ser tido em conta o seguinte:

- Identificação dos ativos da organização (Tabela 7);
- Determinar as causas de um dano resultante de um ataque contra um ativo da organização;
- Determinar a forma de minimizar o risco de ataque com a utilização de controlos apropriados.

Ativos da organização	
• Servidores • Computadores de Secretária • Portáteis e PDAs • Switches e Routers • Software de aplicações • Ferramentas Desenvolvimento • Código Fonte • Acesso VPN • Dispositivos de Backup	• Correio Electrónico • Integridade de Dados • Ficheiros dos Servidores • Informação de Clientes • Infrasestrutura de Rede • DHCP • Disponibilidade dos sites • Reputação • …

Tabela 7 – Exemplos de Ativos

3.1.2 - Avaliação de Riscos

Avaliação de riscos é um dos elementos mais importantes do processo de gestão de risco, sendo considerada a pedra angular para todos os outros elementos. É extremamente complexa, podendo ser abordada através de duas lógicas de ação diferenciadas. A análise qualitativa e a quantitativa.

3.1.2.1 - Análise Quantitativa

A abordagem quantitativa tem como missão, o cálculo de resultados numéricos objetivos que expressem a probabilidade de cada factor de risco e as suas consequências sobre os objetivos do projeto. Pode ser estimado por exemplo, o valor real de cada ativo, o custo de substituição, o custo de perda de produtividade…

Esta análise é efectuada através de:

1. **Atribuir valor dos ativos**;
2. **Determinar o SLE (*Single Loss Expentancy*)** – Total do valor perdido com apenas uma ocorrência do risco;
3. **Determinar o ARO (*Annual Rate of Occurrence*)** - Total de vezes esperadas que ocorra o risco durante um ano;
4. **Determinar o ALE (*Annual Loss Expentancy*)** – Quantidade que se perde num ano se o risco não for atenuado;
5. **Determinar o ROSI (*Return On Security Investment*)** – ALE (antes de aplicação de controlo) – ALE (depois de aplicação de controlo) = ROSI.

Para os diferentes cálculos existentes na análise quantitativa, deverá ser usada a mesma objetividade, garantindo assim a existência de equilíbrio entre todos.

3.1.2.2 - Análise Qualitativa

A análise qualitativa é um processo de avaliação do impacto resultante dos factores de risco identificados. Através deste, são determinadas as prioridades para resolver os potenciais factores de risco, dependendo sempre do impacto que eles terão.

Abordagem qualitativa é efectuada tendo por base:

1. Estimar valores relativos;
2. Determinar as ameaças que cada ativo possa encarar;
3. Determinar quais vulnerabilidades possam vir a ser exploradas pelas ameaças identificadas;
4. Determinar controlos que minimizem os riscos e seu custo (aproximado);
5. Executar uma análise custo-benefício.

A diferença entre este tipo de análise e a quantitativa (Tabela 8) é que, a avaliação qualitativa não atribui valores fixos aos ativos, perdas e controles. Atribui sim, valores relativos e subjetivos como baixo- médio-alto, vital-crítico-importante,…

	Quantitativa	Qualitativa
Benefícios	Os riscos e ativos são priorizados com base em valores financeiros	Permite a visibilidade e compreensão da classificação de risco
	Os resultados facilitam a gestão de risco no que diz respeito ao retorno sobre o investimento de segurança	Fácil de chegar a consenso
	Os resultados de gestão são expressos em valores monetários (€/$)	Não é necessário quantificar a frequência da ameaça ou qualquer valor de ativos
	Precisão tende aumentar ao longo do tempo	Mais fácil de envolver pessoas que não são especialistas de segurança ou computadores
Desvantagens	Os valores de impacto atribuídos aos riscos são baseados em opiniões subjetivas	Diferenciação entre riscos importantes é insuficiente
	Muito demorado	Difícil de justificar o investimento em controlos quando não existe base para uma análise custo-beneficio
	Os cálculos podem ser complexos de fazer	Os resultados dependem da qualidade da equipa de gestão de risco criada para o efeito
	Resultados apresentados em termos monetários podem dificultar a interpretação pelas pessoas que não são técnicas	
	Processo exige conhecimentos e experiência	

Tabela 8 – Abordagem Quantitativa vs. Qualitativa

3.1.2.3 - Processo Avaliação de Risco

De forma a compreender o processo de avaliação de risco é essencial definir o conceito de risco. Tal como acontece com outros termos, o risco também possui diferentes definições. O NIST definiu-o como sendo "o impacto resultante da probabilidade, que uma ameaça irá exercer numa vulnerabilidade existente num sistema de informação e o resultado que terá este impacto na organização se a ameaça se concretizar" (21). A Microsoft definiu o risco como sendo "a probabilidade de concretização de uma vulnerabilidade ser explorada, levando a um grau de perda de confidencialidade, integridade ou disponibilidade de um ativo" (22).

O risco, em poucas palavras, pode ser definido como sendo onde a ameaça se cruza com a vulnerabilidade. Tendo em conta a definição de risco, o objetivo do processo de avaliação de risco é identificar e avaliar os riscos existentes em determinado ambiente. O grau de profundidade da avaliação difere em função de factores como a criticidade e sensibilidade do sistema.

De forma a atender o objetivo da avaliação de risco, o NIST na sua publicação NIST SP 800-30 definiu um processo constituído por nove etapas (19):

1. Caracterização do Sistema;
2. Identificação de Ameaça;
3. Identificação de Vulnerabilidade;
4. Análise de Controlo;
5. Determinação de Probabilidade;
6. Análise de Impacto;
7. Determinação de Risco;
8. Recomendações de Controlo;
9. Documentação de Resultados.

Posteriormente na publicação NIST SP 800-100, com objetivo de simplificar, o processo de análise de risco foi reduzido para seis etapas. Sendo que a etapa 4 a 7 foram agregadas numa apenas (Figura 15).

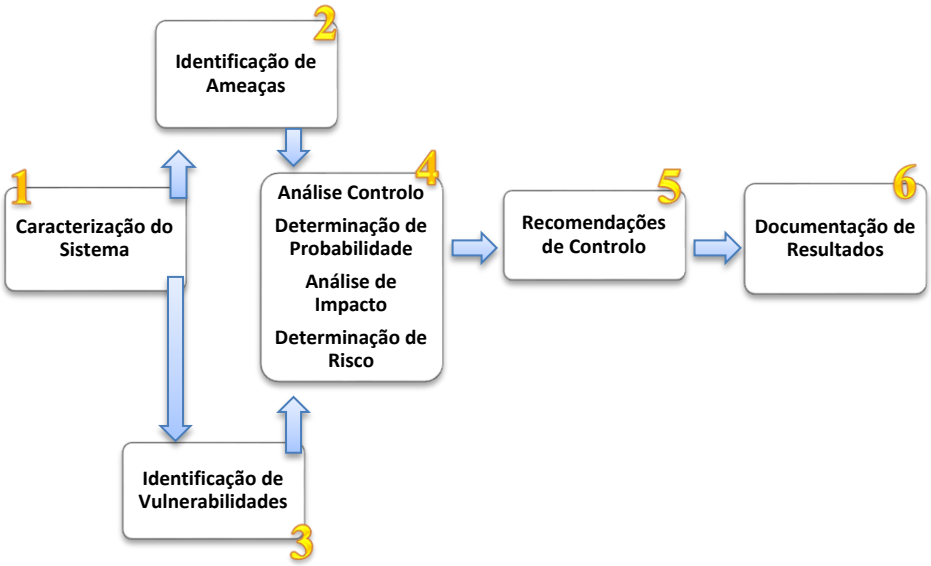

Figura 15 - Processo de Avaliação de Risco

A probabilidade de uma ameaça explorar uma vulnerabilidade é estimada avaliando a motivação das ameaças, oportunidade e os métodos que podem conduzir à sua exploração. O impacto resultante do incidente é considerado através da análise dos seus efeitos na confidencialidade, integridade e disponibilidade dos sistemas e dos dados que o compõem.

3.1.2.4 - Etapa 1 - Caracterização do Sistema

A primeira etapa num processo de avaliação de riscos consiste em definir o desígnio do esforço. Nesta fase, são identificados os limites do sistema juntamente com os recursos e as informações que o compõem. A utilização de questionários, entrevistas e ferramentas de procura automática são algumas das técnicas que, quando combinadas ou utilizadas individualmente permitem recolher a informação necessária.

Na caracterização do sistema, o nível de esforço e profundidade a atingir na gestão de risco, deve ser ajustada em função da relevância do sistema e do seu impacto. Um sistema de pouco impacto não necessitará certamente de testes aprofundados de segurança.

A caracterização do sistema deverá descrever no mínimo os seguintes componentes:

- *Hardware;*
- *Software;*
- Interfaces do Sistema;
- Dados;
- Pessoas que utilizam e suportam os sistemas;
- Sistema e a importância dos dados;
- Sistema e a sensibilidade dos dados.

Além dos componentes referidos existem outros factores que podem influenciar a segurança do sistema, tais como:

- Requisitos do sistema;
- Arquitetura e política de segurança da organização;
- Topologia da rede;
- Fluxos de informação do sistema;
- Controlos de gestão, operação e de segurança implementados ou previstos;
- Mecanismos de segurança física e ambiental.

Os resultados alcançados nesta fase servem de base para todas as etapas restantes. Qualquer erro ou imprecisão resultante da caracterização do sistema poderá significar o aparecimento de erros em catadupa à medida que o procedimento avança.

A etapa 1 originará um parágrafo com a caracterização do sistema onde será exibida uma "foto" do ambiente do sistema e seus limites.

3.1.2.5 - Etapa 2 – Identificação de Ameaças

Como já foi definido anteriormente, uma ameaça é o potencial que uma determinada fonte de ameaça tem para explorar com sucesso uma vulnerabilidade específica, sendo que, a fonte de ameaça diz respeito a qualquer circunstância ou evento com potencial para causar danos num sistema.

O objetivo desta etapa é o de identificar a origem das ameaças que detêm capacidade para explorar as fraquezas do sistema. Para que seja determinada a probabilidade de ocorrência de uma ameaça, é necessário considerar as fontes de ameaças, potenciais vulnerabilidades e os controlos de segurança existentes na organização.

Existem dois tipos de fontes de ameaças: 1) surgem com intenção e utilizam métodos orientados para exploração intencional de vulnerabilidades; 2) situações que acidentalmente podem ativar vulnerabilidades. Dentro das fontes de ameaças mais comuns pode-se efetuar uma categorização em três áreas:

- Ameaças Naturais;
- Ameaças Humanas;
- Ameaças Ambientais.

Na avaliação das fontes de ameaças, torna-se importante considerar todos as potenciais fontes que de alguma forma, podem causar desastres num sistema, mesmo as que possuem uma probabilidade diminuta de ocorrerem.

Ameaças	
Ameaças Humanas	Descuido
	Abuso do utilizador
	Entrada dados com erros
	Violações intencionais e não intencionais dos procedimentos
Ameaças Técnicas	Intrusão
	Falha no Sistemas
	Saturação dos Recursos
Ameaças de Ambiente	Fogo
	Terramoto
	Tornado
	Corte de Cabos
	Sobreaquecimento

Tabela 9 - Diferentes tipos de ameaças

Apesar da importância de todos os tipos de ameaças (Tabela 9), as motivações (Tabela 10) e os recursos existentes para a realização de ataques tornam as ameaças humanas como sendo as mais perigosas. Se olharmos para a história, verificamos que os grandes ataques conhecidos tiveram sempre como origem as ameaças humanas.

Fontes de Ameaças	Motivações	Ações
Hackers, Crackers	Desafio	*Hacking*
	Ego	Engenharia Social
	Rebeldia	Intrusão de Sistemas
		Acesso não Autorizado a Sistemas
Criminosos	Destruição de informação	Crimes de Computadores
	Acesso a informação ilegal	Atos Fraudulentos
	Interesses monetários	Suborno
	Alteração não autorizada de dados	*Spoofing*
Terroristas	Chantagem	Bomba/Terrorismo
	Destruição	Sistema de Ataque (DoS, DDoS)
	Exploração	Penetração de Sistema de penetração
	Vingança	Adulteração de Sistema
Espionagem Industrial	Vantagem competitiva	Exploração Económica
	Espionagem económica	Roubo de Informação
		Invasão de Privacidade
		Engenharia Social
		Acesso não autorizado ao sistema
Internos (poucos conhecimentos, negligentes, desonestos, …)	Curiosidade	Chantagem
	Ego	Visualização de Informação Proprietária
	Inteligência	Fraude e Roubo
	Ganhos financeiros	Suborno
	Vingança	Venda de Informações Pessoais
	Erros intencionais	Intrusão do Sistema
		Sabotagem do Sistema
		Acesso não autorizado ao sistema

Tabela 10 - Ameaças Humanas: Fontes de Ameaças, Motivações e Ações

A etapa identificação de ameaças deve culminar com a elaboração de uma "declaração de ameaça" composta por uma listagem detalhada indicando as origens das potenciais ameaças e um gráfico mostrando as motivações e ações necessárias para as ameaças humanas. A declaração deverá ser personalizada e ajustada à organização que se destina.

3.1.2.6 - Etapa 3 - Identificação de Vulnerabilidades

A vulnerabilidade é uma falha ou debilidade nos procedimentos do sistema de segurança, no desenho, implementação ou mecanismos de segurança que podem ser executada (acidentalmente ou intencionalmente) e resultar numa violação de segurança ou violação da política de segurança da informação.

A análise das ameaças presentes num sistema deve incluir análise das vulnerabilidades existentes no ambiente que rodeia o sistema. O objetivo desta etapa é o de desenvolver uma lista de vulnerabilidades (falhas ou debilidades) que podem vir a ser exploradas pelas fontes de ameaças. Na Tabela 11 é feita a relação entre alguns exemplos de vulnerabilidades e as ameaças associadas.

Vulnerabilidade	Fontes de Ameaça	Ação
Contas de funcionários antigos não foram removidas do sistema	Empregados Antigos	Ligarem-se à rede da organização e terem acesso a dados proprietários
Firewall permite acesso remoto a SSH e contas convidado estão ativas no sistema	Utilizadores não autorizados (*hackers*, empregados antigos, criminosos, terroristas)	Usar o ssh para aceder a um servidor e ter acesso a ficheiros
Os fabricantes identificaram problemas de segurança mas as correções não foram aplicadas	Utilizadores não autorizados (*hackers*, empregados antigos, criminosos, terroristas)	Ter acesso a dados sensíveis utilizando as vulnerabilidades conhecidas dos sistemas
Datacenter antigo com sistema antifogo baseado em aspersores; As lonas que possuem a finalidade de proteger o *hardware* da água não estão colocadas	Fogo, pessoas negligentes	Os aspersores serem ligados no *datacenter*

Tabela 11 - Relação Vulnerabilidade / Ameaças

As vulnerabilidades podem ser encontradas em diversos componentes tais como:

- **Configuração de Hardware** – Servidores, estações de trabalho, *routers, switches, firewalls;*
- **Aplicações de Software** – Como estão instaladas? Onde estão instaladas? Que direitos possuem?
- **Políticas e Procedimentos de Segurança** – Estão completos? Atualizados? São conhecidos?
- **Humanos** – Procedimentos que não são cumpridos, Pessoal não é formado/treinado.

A identificação de vulnerabilidades pode ser feita através da realização de testes de segurança ou recorrendo à utilização de uma lista de verificação de requisitos de segurança. As estratégias e metodologias adoptadas variam de acordo com a natureza do sistema e a fase em que este se encontra.

Para cada tipo de vulnerabilidades, a descoberta de vulnerabilidades pode ser feita através de:

- **Configuração de Hardware** – Para cada componente preencher um formulário de análise de risco para depois realizar testes de penetração*;*
- **Aplicação de Software** – Preencher um formulário de criticidade e análise de risco para cada aplicação;
- **Políticas e Procedimentos de Segurança** – Completar em cada ano uma análise de qualidade das políticas e procedimentos de segurança;
- **Humanos** – Analisar os ficheiros de registo e relatórios de incidentes.

A pesquisa de vulnerabilidades diverge em função do estádio em que se encontra o sistema. Num sistema que ainda não está desenhado/implementado, a procura de vulnerabilidades deve-se centrar nas políticas e procedimentos de segurança da organização, assim como nas análises realizadas pelos fabricantes dos produtos de segurança.

Se o sistema já se encontra implementado, a identificação de vulnerabilidades deverá ser expandida de forma a incluir informação mais específica, tal como as funcionalidades de segurança planeadas.

Vulnerabilidades	
• Portas Abertas	• Configuração de *Software*
• Janelas Abertas	• Sistemas não Monitorizados
• Sistemas Mal Configurados	• Protocolos Desnecessários
• Ausência de *Patches*	• Procedimentos mal definidos
• Antivírus Desatualizado	• Credenciais Roubadas
• Aplicações Mal Desenvolvidas	• Palavras-chave Fracas
• *Spyware*	• Violações não Reportadas

Tabela 12 - Exemplos de Vulnerabilidades

Por último, se o sistema já se encontra em funcionamento, a identificação de vulnerabilidades deve incluir uma análise das funcionalidades de segurança e mecanismos usados para proteger o sistema. Na Tabela 12 são enumeradas algumas vulnerabilidades que ocorrem diversas vezes.

3.1.2.7 - Etapa 4 - Análise de Risco

A análise de risco requer que sejam avaliados/determinados diversos factores, como é o caso dos mecanismos de segurança em funcionamento e a probabilidade destes serem ou não eficazes na proteção dos sistemas. O impacto resultante da falta de eficácia dos mecanismos é outro dos factores que devem ser tidos em conta.

Não é possível estimar o nível de risco associado à exploração com sucesso de uma determinada vulnerabilidade, sem se considerar a eficácia dos mecanismos de segurança implementados e/ou previstos para diminuir, ou até quem sabe eliminar por completo o potencial de exploração de determinada ameaça. As quatro etapas constituídas por análise de controlo, determinação de probabilidade, análise de impacto e determinação de risco são praticamente realizadas em simultâneo por se encontrarem intimamente ligadas.

Análise de Controlos

O seu objetivo é o de analisar os controlos de segurança empregados, com propósito de minimizar a probabilidade de uma ameaça explorar uma vulnerabilidade em particular.

Os controlos de segurança podem ser subdivididos em dois grupos: os que recorrem a mecanismos considerados técnicos e os não técnicos. Os técnicos, incluem dispositivos de *hardware*, *software*, controlo de acesso, identificação, autenticação… Os considerados não técnicos são controlos operacionais onde se incluem as políticas de segurança, procedimentos operacionais, entre outros.

Qualquer tipo de controlo pode ser ainda classificado como sendo de prevenção ou detecção. Os de prevenção têm a finalidade de impedir as tentativas de violação das políticas de segurança. Já os de deteção possuem a missão de alertar as violações ou tentativas de violação à política de segurança.

A análise de controlo pode ser efectivada recorrendo a uma *checklist* ou um questionário tendo como base os requisitos da segurança do sistema. Além de permitir validar o incumprimento da segurança, a *checklist* possibilita o registo do seu cumprimento. Para que seja válida e produza resultados, é necessário que a *checklist* seja atualizada ao longo dos tempos e espelhe as alterações ocorridas na organização, sejam mudanças nas políticas de segurança ou nos requisitos.

A análise de controlos possui como saída uma lista com todos os controlos/mecanismos usados pelo hardware de rede e uma outra com os usados nas aplicações.

Determinação de Probabilidade

Para determinar a probabilidade da ocorrência de uma vulnerabilidade, será necessário considerar um conjunto de factores:

1. Capacidade e origem das fontes de ameaças;
2. Natureza das vulnerabilidades;
3. Existência e a eficácia dos controlos de segurança existentes.

A probabilidade de uma vulnerabilidade ser explorada de forma bem-sucedida por parte de uma ameaça, será descrita em termos qualitativos (Tabela 13). Por exemplo, numa situação em que o atacante possui conhecimentos avançados, a motivação para realizar um ataque é elevada e os mecanismos de controlo de segurança implementados são ineficazes, a probabilidade de ocorrência classificar-se-ia como sendo elevada.

Nível	Definição de probabilidade
Alto	Fontes de ameaça altamente motivada e altamente capaz; Controlos de segurança ineficazes
Médio	Fontes de ameaça altamente motivada e altamente capaz; Controlos de segurança eficazes e capazes de impedir que a vulnerabilidade seja explorada
Baixo	Fontes de ameaça sem motivação ou capacidade, ou controlos capazes de reduzir a probabilidade da vulnerabilidade ser explorada

Tabela 13 - Definição de Probabilidade

Análise de Impacto

O impacto é outro dos factores usado na determinação do nível de risco. Uma análise adequada além de considerar o impacto que este tem nos sistemas, nos dados e na missão da organização, considera também a criticidade e sensibilidade dos dados da mesma.

Antes de encetar o processo de análise de impacto é necessário obter as seguintes informações:

- Missão do sistema;
- Criticidade dos sistemas e dados;
- Sensibilidade dos sistemas e dados.

A sensibilidade dos dados e do sistema pode ser determinada com base em: nível de proteção necessária para manter o sistema; disponibilidade; integridade e confidencialidade dos dados. Independentemente do método utilizado para determinar a sensibilidade de um sistema e seus dados, o proprietário dos dados e do sistema será sempre responsável por determinar o nível de impacto no seu sistema.

O impacto adverso vem:

- **Perda de Integridade** – A integridade dos dados e do sistema refere-se aos requisitos que permitem proteger a informação contra modificações impróprias. A integridade perde-se quando existem modificações não autorizadas nos dados, seja através de forma intencional ou acidental;

- **Perda de Disponibilidad**e – Um sistema indisponível poderá implicar perda de produtividade, perdas monetárias e até significar o afectar da missão da organização;

- **Perda de Confidencialidade** – Informação classificada de confidencial é acedida sem autorização.

Tal como a determinação do risco, a análise de impacto é classificada de forma qualitativa (Tabela 14), e terá como saída para cada vulnerabilidade identificada uma estimativa da magnitude do impacto provável.

Magnitude	Definição de impacto
Alto	Exercício da vulnerabilidade pode resultar em custos elevados ou significar um impedimento na missão da organização ou na sua reputação
Médio	Exercício da vulnerabilidade pode resultar em custos elevados ou pode prejudicar a missão da organização ou a sua reputação
Baixo	Exercício da vulnerabilidade pode resultar na perdas de alguns ativos, ou pode afectar perceptivelmente a missão da organização ou a sua reputação

Tabela 14 - Magnitude da definição do impacto

Determinação de Risco

O NIST definiu o risco como sendo " o impacto resultante da probabilidade, que uma ameaça irá exercer numa vulnerabilidade existente num sistema de informação e o resultado que este impacto terá na organização se a ameaça se concretizar". Uma vez determinada a probabilidade e o impacto, o risco poderá então ser determinado.

PROBABILIDADE X IMPACTO = RISCO

O risco deve ser representado por uma matriz 3x3 (Tabela 15), onde é dado como entrada a probabilidade de ameaça (Alta, Média ou Baixa) e o impacto da ameaça (Alto, Médio ou Baixo). Em algumas organizações, é necessário atingir um nível de detalhe maior, sendo por isso necessário utilizar uma matriz de 4x4 ou 5x5 onde podem ser incluídas probabilidades Muito Baixa/Muito Alta ou impacto Muito Baixo/Muito Alto.

PROBABILIDADE AMEAÇA	IMPACTO		
	Baixo (10)	Médio (50)	Alto (100)
Alta (1.0)	Baixo 10x1.0 = 10	Médio 50x1.0 = 50	Alto 100x1.0 = 100
Media (0.5)	Baixo 10x0.5 = 5	Médio 50x0.5 = 25	Médio 100x0.5 = 50
Baixa (0.1)	Baixo 10x0.1 = 1	Baixo 50x0.1 = 5	Baixo 100x0.1 = 10

Tabela 15 - Matriz Nível de Risco

A saída desta matriz (Tabela 15) representa o valor do nível de risco. O risco é considerado Alto quando o valor está compreendido entre 51 e 100; Médio quando se encontra entre 11 e 50 e Baixo entre 1 e 10.

A escala de risco qualitativa (Tabela 16) classificada de Alto, Médio e Baixo, representa o grau de risco que o sistema de informação se encontra exposto se uma vulnerabilidade identificada for explorada. Para acautelar ocorrência do risco devem ser tomadas algumas ações em função do nível de risco. Estas ações encontram-se referidas na Tabela 16.

Nível de risco	Ações a tomar
Alto	Existe uma necessidade enorme de medidas corretivas, o sistema pode continuar a trabalhar, mas é necessário colocar um plano de ação corretiva o mais rápido possível
Médio	São necessárias ações corretivas. É necessário ser desenvolvido um plano incorporando essas ações
Baixo	Controlos adicionais podem ser implementados ou o gestor pode decidir aceitar o risco

Tabela 16 - Níveis de Risco e Ações a Tomar

A determinação de risco resulta numa saída onde é atribuído um valor numérico para o par vulnerabilidade identificada / fonte de ameaça.

3.1.2.8 - Recomendações de Controlo

As recomendações de controlo têm como objetivo a redução do nível de risco num nível aceitável, sendo essenciais para a atenuação do risco ao qual a organização se encontra exposta. Quando se procede à recomendação de controlos deve ser tido em conta alguns factores:

- Eficácia das opções recomendadas;
- Legislação e regulamentação;
- Política da organização;
- Impacto operacional;
- Confiabilidade e segurança.

Dos controlos recomendados nem todos possuem a capacidade de minorarem as perdas. De forma a determinar quais controlos são adequados, deve-se efetuar uma análise custo benefício que permita mostrar que a utilização de determinado controlo permitirá diminuir o nível de risco.

Controlos			
	Físicos	Técnicos	Administrativos
Preventivo	Cartão de acesso	Monitorização de Redes e Sistemas	Formação de consciencialização dos funcionários
Detecção	Selos nos armários do arquivo morto	Mensagem após 3 logins incorretos	Auditoria dos procedimentos
Impedimento	Circuito de vídeo interno	Bloqueio da conta após 3 tentativas	Aprovação de direitos dos proprietários dos dados
Corretivo	Isolamento físico dos servidores	Alterações do *firewall* devido a eventos ocorridos	Ajuste dos procedimentos
Recuperação	Substituição de *hardware* …	Recuperação dos ficheiros recorrendo a backups, …	Contactar a polícia depois de falha de segurança

Tabela 17 – Exemplos de Controlos

Esta etapa terá como saída a recomendação da utilização de determinados controlos e soluções alternativas com objetivo de reduzir o nível de risco. Na Tabela 17 são enumerados alguns tipos de controlos existentes.

3.1.2.9 - Documentação dos Resultados

Concluído o processo de avaliação de risco composto pela identificação das fontes de ameaça e vulnerabilidades, análise dos riscos e a recomendação de controlos, deve-se proceder à documentação dos resultados obtidos através de um relatório.

O relatório de avaliação de risco deve ser suficientemente detalhado, de forma a permitir que os órgãos de gestão da organização se pronunciem sobre as ações apropriadas a tomar em resposta aos riscos identificados. Ao contrário das auditorias, que normalmente são apresentadas de forma acusatória, o relatório de avaliação de risco deve apresentar os resultados com uma abordagem sistemática e analítica na apresentação do risco, permitindo assim entender quais os riscos e os recursos necessários para corrigir e reduzir as eventuais perdas.

O relatório de avaliação deverá ser composto pelos seguintes elementos:

1. Introdução;
2. Descrição da abordagem utilizada na Avaliação de Risco;
3. Resumo com a caracterização do sistema;
4. Lista das Fontes de Ameaças;
5. Resultado da análise Vulnerabilidades/Fontes de Ameaças;
6. Resumo com o nível de risco e as recomendações.

3.1.3 - Mitigação de Riscos

A mitigação de riscos diz respeito à segunda fase do processo de gestão de riscos. A sua função é a de avaliar, priorizar e implementar medidas que permitam reduzir os riscos identificados no processo de avaliação de risco.

A eliminação de todos os riscos é uma missão impossível, sendo que a estratégia passa por recorrer à abordagem de menor custo, implementando controlos apropriados que permitam reduzir o risco a um nível aceitável e com impacto mínimo negativo sobre os recursos e missão da organização.

A mitigação de riscos pode ser alcançada com a utilização de algumas opções que permitem a sua redução, tais como: Aceitar o risco (aceita-se o risco e continua-se a operar); Evitar risco (pára-se o programa ou deixa-se de partilhar os dados); Transferir risco (usar opções que permitam compensar o risco, tais como seguros); Reduzir risco (implementar controlos que permitam diminuir o impacto e baixar a probabilidade de risco).

3.1.3.1 - Metodologia para Implementação de Controlos

A abordagem utilizada na implementação de controlos para a mitigação do risco é composta por uma metodologia de sete etapas:

1. **Priorizar ações com base no risco apresentado -** As ações de implementação devem ser priorizadas tendo em conta os níveis de risco presentes na avaliação de risco. A prioridade deve ser atribuída aos itens que possuem níveis de risco elevados, devendo ser tomadas medidas corretivas imediatas para proteger a organização do par vulnerabilidade/ameaça responsável;
2. **Avaliar as opções de controlos recomendadas -** Os controlos recomendados na avaliação de risco poderão não ser os mais apropriados para a organização. Deve ser analisada durante esta fase a compatibilidade, o grau de proteção e eficácia dos controlos recomendados, selecionando os controlos mais adequados para a redução do risco;
3. **Efetuar uma análise custo-benefício -** Para ajudar na escolha do controlo deverá ser feita uma análise custo-benefício para os controlos selecionados;
4. **Selecionar controlos adicionais -** Com base na análise custo-benefício será determinado o controlo mais adequado para a redução do risco. O controlo selecionado deverá combinar os aspectos técnicos, operacionais e de gestão para garantir a segurança adequada;
5. **Atribuir responsabilidades -** Com base na experiência e competência, são selecionadas as pessoas adequadas para a implementação dos controlos escolhidos, sendo-lhes atribuídas responsabilidades neste processo;

6. **Devolver um plano de ação -** Deve ser desenvolvido um plano de ação/implementação com a seguinte informação:
    - Riscos com o correspondente nível de risco identificado no relatório de avaliação de risco;
    - Controlos recomendados no relatório de avaliação de risco;
    - Priorizar ações (apenas para níveis de risco elevados);
    - Selecionar controlos e determinar viabilidade, eficácia, benefícios e custos;
    - Lista com recursos necessários para a implementação dos controlos escolhidos;
    - Lista com as equipas responsáveis pela implementação e seus membros;
    - Data de início da implementação;
    - Data de fim de implementação;
    - Requisitos de manutenção.
7. **Implementar os controlos -** Por norma, os controlos implementados reduzem o nível de risco mas não o conseguem eliminar definitivamente.

Esta abordagem pode ser representada através do fluxograma do anexo B onde são representadas as entradas em cada etapa e a saída que cada uma produz.

3.1.4 - Avaliação

As redes são caracterizadas por se encontrarem em constante mutação, fruto das necessidades de atualização, crescimento e do acompanhamento da evolução tecnológica. Ao longo dos tempos os seus componentes são substituídos, algumas aplicações trocadas enquanto outras atualizadas para versões mais recentes. Ocorrem também mudanças nas pessoas e funções, sendo por vezes necessário proceder à mudança das políticas existentes de forma a acompanhar as transformações. Todas estas alterações podem significar a exposição a novos riscos que anteriormente não foram previstos ou então foram mitigados e que como consequência das alterações, viram o seu nível de risco aumentado. Em virtude de tudo isto, o processo de gestão de risco é caracterizado por ser um processo permanente e em constante evolução.

Faz parte das boas práticas realizar o processo de avaliação de risco de 3 em 3 anos, no entanto, a condução do processo de gestão de risco deve ser feita periodicamente, sendo aconselhável sempre que ocorram alterações, mudanças no sistema, modificações nas políticas ou até mesmo introdução de novas tecnologias.

Para que um programa seja bem-sucedido é necessário ter em conta os seguintes factores:

1. Apoio total da administração da organização;
2. Participação ativa da equipa de TI no processo;
3. Competência da equipa responsável para realizar avaliação e identificação de risco e capacidade para reconhecer o custo-benefício dos mecanismos e salvaguardas que atendam às necessidades da organização;
4. Consciencialização e cooperação dos elementos que compõem a organização para seguirem os procedimentos e cumprimento das medidas e controlos adoptados;
5. Avaliação contínua do processo de gestão de risco.

A conjugação dos factores atrás referidos, são meio caminho para o sucesso de um processo de gestão de risco em qualquer organização.

3.2 - Cisco SAFE: Arquitetura de Referência de Segurança

As mudanças ocorridas nas redes nos anos transatos são responsáveis pelo aparecimento de serviços como virtualização, computação na nuvem *(cloud computing)*, plataformas baseadas em tecnologias *Web2.0* destinadas a colaboradores, parceiros e clientes. Como consequência da drástica evolução registada na tecnologia, as infraestruturas das organizações são obrigadas a acompanhar este desenvolvimento, correndo o risco de perder negócio e o comboio da inovação, se assim não o fizerem.

Paralelamente à evolução dos serviços, a tecnologia que lhes serve de apoio continua a desenvolver-se. Um exemplo disso diz respeito aos acessos à internet e ao aparecimento de novos dispositivos, sendo que, estes exemplos são responsáveis pelo aumento de mobilidade dos colaboradores. Se a Internet é omnipresente, a variedade de dispositivos disponíveis possibilita, em qualquer lugar e ocasião, ter acesso às ferramentas da organização.

Este cenário de evolução constante significa um desafio contínuo e complexo. A rápida proliferação de *botnets*, a sofisticação dos ataques, o crescimento alarmante do crime organizado e espionagem através da internet, o roubo de dados e identidade, são o exemplo de novas formas de ameaças que despontaram.

As ferramentas de segurança tradicionais possuem capacidade limitada para apoiar e garantir este avanço. Como fator chave de segurança, as redes quando desenhadas e implementadas devem ter a segurança como elemento integrado com objetivo de garantir a confidencialidade, integridade e disponibilidade dos dados e recursos dos sistemas.

No passado, atingir um nível adequado de segurança implicava introduzir um conjunto de mecanismos confinados ao perímetro da rede. Hoje, em virtude da complexidade e o nível de sofisticação que as ameaças possuem, a estratégia passa por ser inteligente na abordagem de segurança.

Algumas das maiores ameaças, ainda que negligenciadas na maior parte das vezes pelas organizações, encontram-se dentro das suas próprias redes e são resultantes, por vezes, de alguns equívocos de segurança onde se incluem:

Silos de segurança
Acontece quando uma infraestrutura de segurança é composta por diversos produtos de segurança adquiridos ao longo dos tempos e que funcionam sozinhos. Os problemas causados neste tipo de arquitetura abrangem:

- Falta de controlo central;
- Má visibilidade da saúde da rede;
- Incapacidade para recolher e partilhar entre os diversos equipamentos informações críticas de eventos de segurança;
- Pouca ou nenhuma colaboração para lidar com ameaças;

- Falta de integração entre os componentes de segurança e rede;
- Sobrecarga com a gestão e manutenção dos diversos elementos de segurança.

Decisões baseadas em medo

Por vezes, as organizações tendem a concentrar-se no improvável ao invés de se concentrarem no presumível. Ignorar problemas de segurança mais mundanos faz com que surjam ameaças através de questões de fácil resolução. Por exemplo, o simples fato de desligar as portas que não são utilizadas ou detetar pontos de acesso de redes sem fio não autorizados, possibilita reduzir o número de ameaças. A gestão de riscos deve ser parte de uma estratégia de segurança abrangente que vê a rede, os serviços de rede e elementos de segurança como um todo.

Produtos versus Gestão de Risco

A seleção dos produtos de segurança, na maioria das vezes, é feita recorrendo apenas a uma comparação de funcionalidades. Encontrando-se os produtos em constante desenvolvimento e mutação, será que faz sentido comparar funcionalidades? A qualquer instante um produto que não possuía determinada funcionalidade pode passar a ter.

A avaliação de produtos de segurança deve ser feita com base em critérios de gestão de riscos com o objetivo de garantir que o mecanismo adquirido responde, dentro do possível, aos riscos da organização e aos seus requisitos agora e num futuro próximo.

Política de segurança inadequada

A política de segurança é um fundamento essencial em qualquer estratégia de segurança. Em algumas organizações, este mecanismo não existe, noutras encontra-se desajustado à organização ou simplesmente ignorado. Um erro muito frequente na política de segurança diz respeito a focar a política apenas na colocação de produtos, dando pouca atenção ao apoio e segurança da rede da organização. Como resultado, surge um documento que não se encontra focado na continuidade de negócio e na redução de risco da organização, não sendo capaz de fornecer orientações para manter a gestão, controlo e visibilidade.

Os fatores referidos fazem com que as organizações nas questões de segurança tenham sido deixadas à sua própria sorte, recorrendo por vezes à aquisição de produtos (silos) de segurança com o intuito de resolver um problema caracterizado de amplo e integrado. A solução não passa por um produto ou tecnologia de segurança, mas sim por um conjunto de medidas e orientações específicas com base nas melhores práticas de segurança.

A Cisco com objetivo de ajudar e melhorar o processo de segurança lançou uma arquitetura denominada de SAFE. Esta arquitetura fornece as diretivas de segurança de projeto e implementação de infraestrutura de redes seguras e confiáveis. O modelo SAFE adota uma abordagem de defesa em profundidade, onde múltiplas camadas de proteção se encontram estrategicamente localizadas na rede, mas sob uma estratégia unificada.

3.2.1 - Cisco Security Control Framework (SCF)

A SCF representada na Figura 16 é uma *framework* de segurança usada na arquitetura Cisco SAFE, com o intuito de garantir disponibilidade de rede e serviços, garantindo a continuidade do negócio. Esta *framework* foi projetada de forma a responder às ameaças atuais e também a ameaças que apareçam no futuro.

Os princípios e ações da SCF são utilizados com intuito de identificar as tecnologias mais apropriadas e as melhores práticas de proteger cada lugar único existente na rede. O resultado é que várias tecnologias de segurança e aptidões são usadas em conjunto em toda a rede de forma a aumentar a visibilidade da atividade da rede, reforçar a política da rede e diminuir o tráfego anómalo (27).

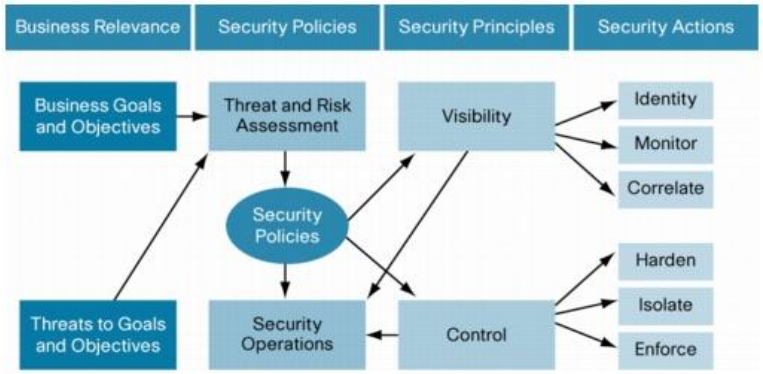

Figura 16 – *Security Control Framework* (27)

Os princípios fundamentais da SCF dizem respeito a maximizar a **visibilidade** dos dispositivos e eventos na rede e ao **controlo** dos utilizadores, dispositivos e tráfego existente. Nas categorias de visibilidade e controlo, a *framework* define seis ações de segurança para fazer cumprir a política de segurança:

Visibilidade

1. Identificar e classificar utilizadores, serviços, tráfego e dispositivos;
2. Monitorizar o desempenho, comportamentos, padrões de uso, eventos e sua conformidade com a política;
3. Recolher, analisar e correlacionar eventos do sistema;

Controlo

4. Dispositivos, serviços, servidores, aplicações e infraestrutura;
5. Isolar utilizadores, sistemas e serviços, quando necessário;
6. Impor controlos de acessos e políticas de segurança e mitigar os eventos de segurança.

Ciclo de vida da arquitetura

A crescente evolução registada nas necessidades do negócio, e das questões de segurança, obriga a que exista a necessidade de revisão e ajuste em qualquer implementação de segurança. Existem 5 passos chave no ciclo de vida da SCF que se encontram retratados na Figura 17.

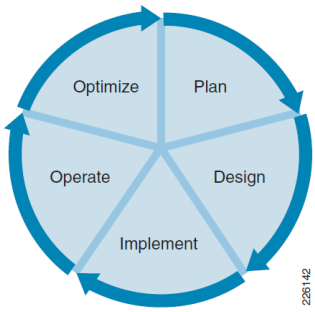

Figura 17 – Ciclo de Vida da SCF

1. Planear. Esta fase deve incluir uma análise de riscos/ameaças com objetivo de identificar os ativos e a conduta da segurança em funcionamento. No planeamento, deve estar incluída também uma análise de lacunas onde sejam indicados os pontos fortes e pontos fracos da arquitetura atual;
2. Desenhar. Nesta fase é criada um projeto detalhado que deverá incluir a seleção das plataformas, funcionalidades e as melhores práticas que serão usadas de forma a colmatar as lacunas identificadas na fase de planeamento;
3. Implementar. Esta fase segue o desenho. Aqui será feita a implantação e provisionamento das plataformas;
4. Operar. Manutenção da implementação e provisionamento das plataformas. Inclui a gestão e monitorização da infraestrutura;
5. Otimizar. É necessário existir avaliações regulares de forma a identificar e resolver possíveis falhas.

3.2.2 - Arquitetura de Segurança SAFE

A arquitetura de segurança SAFE inclui um conjunto de projetos validados de segurança, guias de implementação técnicos com o intuito de ajudar as organizações na sua segurança. Alguns dos benefícios da utilização da arquitetura Cisco SAFE, incluem:

- **Projetos detalhados, com base nas melhores práticas de segurança usadas em projetos reais de segurança**. Esta abordagem permite passar rapidamente do conceito à fase de implementação, permitindo assim poupar tempo e dinheiro. Este tipo de documentos possibilita também auxiliar na criação ou melhoria da política de segurança da organização;
- **Projetos modulares que possibilitam a melhoria da segurança de forma incremental**. Na maioria dos casos, as organizações não têm a possibilidade de reformular a infraestrutura de segurança por inteiro. A abordagem modular SAFE permite que as organizações melhorem o seu perfil de segurança faseadamente, podendo começar pela parte que mais convenha e careça de melhorias. Este tipo de abordagem só é possível porque os vários componentes da arquitetura SAFE fazem parte de uma estratégia integrada. O aumento da visibilidade e controlo de alguns componentes tem como consequência o acréscimo da saúde da rede.
- **Defesa em profundidade permite proteger contra as ameaças mais complexas**. No caso de ataques resultantes de múltiplos vetores de ameaças, muitos dos ataques

individuais são identificados como preocupações de baixo nível, sendo por vezes ignorados. A arquitetura SAFE permite que, entre diferentes dispostitos, além da partilha de informação sobre ameaças, seja também agregada informação que permite detetar, reportar e impedir as ameaças mais complexas.

- **Arquitetura detalhada e definida passo-a-passo**. Esta abordagem permite reduzir os custos associados com o desenho, desenvolvimento e implementação.
- **Colaboração entre os elementos de segurança e infraestrutura de rede.** Esta relação, além de criar uma forte componente de segurança, ajuda também a garantir a disponibilidade da rede e serviços.

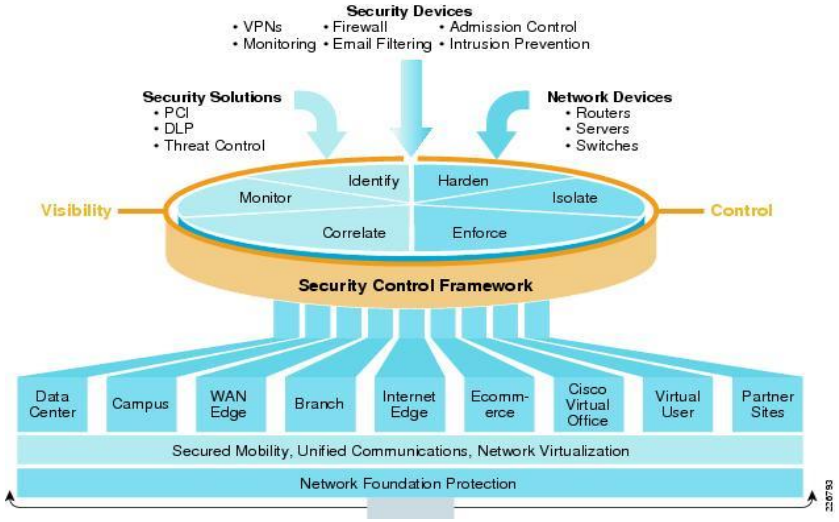

Figura 18 – Cisco SAFE (28)

3.2.3 - Princípios da Arquitetura

A arquitetura SAFE tem como finalidade fornecer diretivas com base nos seguintes princípios (28):

Defesa em Profundidade

O modelo SAFE segue a abordagem de defesa em profundidade, com objetivo de garantir a confidencialidade, integridade e disponibilidade de dados, aplicações, dispositivos e a da própria rede. Para aumentar a visibilidade e controlo, um conjunto de tecnologias de segurança e funcionalidade são implementadas em múltiplas camadas, mas usando a mesma estratégia.

Modularidade e Flexibilidade

O desenho da arquitetura SAFE é feito recorrendo a uma estrutura modular (Figura 19). A infraestrutura de rede é dividida em módulos funcionais onde cada um representa locais distintos com funções diferenciadas, como acontece por exemplo, com o campus ou centro de dados. Os módulos funcionais são então subdivididos em mais blocos ou camadas, tendo cada um uma função específica na rede (camada de acesso, distribuição,…).

A estratégia modular resulta no aumento de flexibilidade quando se trata da implementação, permitindo que seja feita de forma faseada.

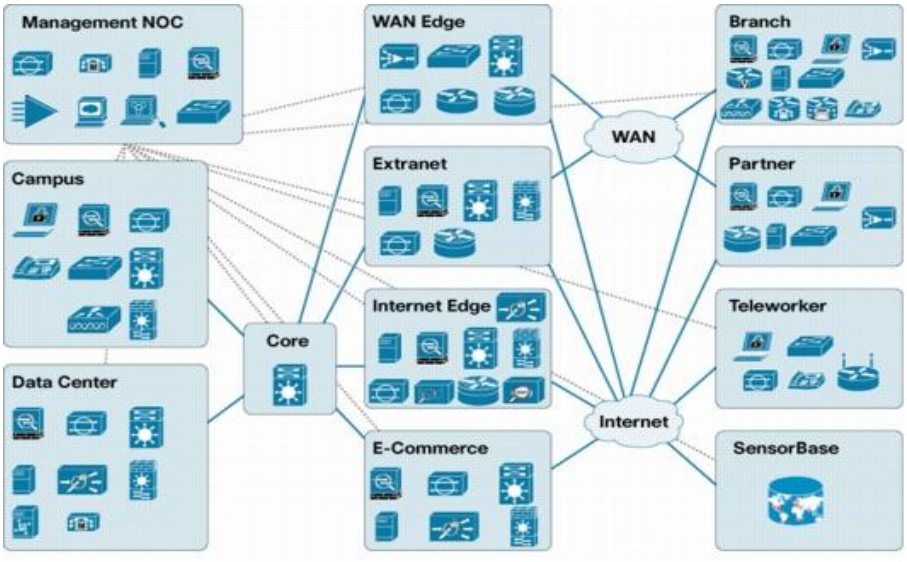

Figura 19 – Arquitetura modular da arquitetura SAFE (27)

Resiliência e Disponibilidade de Serviços

A arquitetura SAFE incorpora várias camadas de redundância com objetivo de eliminar pontos de falha e aumentar a disponibilidade da rede. Aqui devem ser contemplados interfaces redundantes, módulos de *backup*, dispositivos e caminhos redundantes.

Conformidade

A SAFE Cisco implementa uma linha de base de segurança como parte intrínseca da infraestrutura de rede. A linha de base de segurança incorpora um conjunto de práticas de segurança e funções habitualmente exigidas pelas normas e regulamentações, facilitando a realização da conformidade regulamentar.

Eficiência de Operação

A aplicação da arquitetura SAFE facilita a gestão e operação fornecendo uma visão unificada do estado global da rede. São definidos pontos de gestão e controlo centrais com objetivo de solucionar e isolar os problemas rapidamente.

Auditoria da Implementação

Os desenhos resultantes da arquitetura Cisco SAFE contemplam um conjunto de ferramentas para medir e verificar o funcionamento e aplicação de salvaguardas em toda a rede, fornecendo uma visão atual do panorama da segurança da rede e ajudando a avaliar o cumprimento de políticas de segurança, normas e regulamentos.

3.3 - Evolução das Aplicações

A sociedade contemporânea é marcada pelas tecnologias que deram origem a uma mudança social e organizacional. As organizações, de forma a responder à revolução tecnológica, permanecem num processo de pesquisa constante de novas tecnologias que permitam fazer frente aos desafios e à complexidade crescente na era atual. Se, a informação ganhou ao longo dos anos um papel preponderante nas organizações, com a revolução tecnológica as aplicações atingiram um lugar de destaque no funcionamento das organizações, trazendo consigo novos desafios de segurança.

O aparecimento das aplicações *Web* 2.0 teve como consequência, na maioria dos casos, uma mudança profunda na forma de trabalhar e interagir. Acompanhando a tendência, algumas organizações adoptaram mecanismos baseados em *Web* 2.0 como plataforma colaborativa onde recorrem a *blogs*, *wikis*, redes sociais entre outros.

Num passado recente, as aplicações eram instaladas em computadores e servidores confinados a ambientes fechados e controlados, sendo por isso simples de controlar e aplicar as políticas de segurança, com as de aplicações *Web 2.0* o mesmo não sucede. A capacidade que este tipo de tecnologia detém para contornar os mecanismos de segurança presentes faz com que o trabalho de segurança se torne mais complexo.

A maioria das aplicações deste tipo já se encontram "infiltradas" dentro das organizações, sendo resultante, em alguns casos, da estratégia da própria organização e noutros, num fenómeno chamado de consumerização *(consumerization)*, que de acordo com o *Gartner*[22] em 2015 constituirá a maior ameaça para as TI.

A consumerização, é um processo que ocorre à medida que os utilizadores vão encontrando tecnologia e aplicações pessoais mais poderosas ou capazes, sendo na maioria dos casos mais fáceis de instalar e utilizar do que as aplicações disponibilizadas pelas organizações.

3.3.1 - Classificação

O desafio atual não se encontra apenas no crescimento da diversidade de aplicações que ocorreu nos últimos tempos, mas sim na incapacidade que existe para classificá-las de boas ou más. Facilmente se classificam aplicações de boas e outras de más, mas a maioria encontra-se num meio-termo entre estas duas classificações, e se assim o é como se classificam?

Se tentarmos num firewall tradicional proceder ao tratamento da classificação de uma aplicação que se encontre num meio-termo como fazemos? A classificação de bom ou má de determinada aplicação parece possível de o fazer se correspondermos ao bom o permitir e ao mau o negar.

[22] Empresa de consultoria que desenvolve tecnologia relacionada com a introspecção necessária para os seus clientes tomarem decisões. http://www.gartner.com

Uma abordagem restrita apenas a duas classificações deverá ser alargada e ajustada às necessidades atuais. Se algumas aplicações em determinados contextos são vistas como "más" aplicações, noutros podem ser vistas como "boas". Um destes exemplos diz respeito às aplicações disponíveis na nuvem da *Google*. Em determinadas situações, a *Google Enterprise* pode ser usada para alojar toda a informação da organização e suportar todos os seus serviços. Noutras, pode funcionar como porta de saída da informação confidencial da organização.

A utilização das aplicações de redes sociais é outro dos exemplos, se as utilizamos para partilhar ou para fazer propaganda de um determinado bem ou produto, consideramos que este tipo de aplicação é boa, se forem usadas no contexto pessoal já é considerada como má devido à quebra de produtividade que provoca nos utilizadores da organização.

3.3.2 - Evasão

O processo de distinção dos diferentes géneros de aplicações poderá parecer simples, mas devido a um conjunto de factores não o é. Logo no projeto de determinadas aplicações e com objetivo de maximizar a sua acessibilidade, são contemplados mecanismos/funcionalidades que permitem circundar os *firewalls* convencionais. Estas habilidades permitem ao utilizador final usar as aplicações em diferentes circunstâncias com diferentes constrangimentos, aumentando assim a sua usabilidade. Se por um lado é aumentada a usabilidade, por outro, aumentam os riscos de segurança.

Algumas das estratégias usadas pelas aplicações com objetivo de contornar os mecanismos de segurança incluem:

- Utilização aleatória de portos: portos e protocolos são alterados de forma aleatória durante uma sessão;
- Recurso a portos não *standards*: utilização de porto 80 ao invés de por exemplo o 5050;
- Estabelecimento de túneis: caso de P2P, partilha de ficheiros,..
- Encriptação SSL: mascara o tráfego das aplicações, por exemplo através de HTTPS.

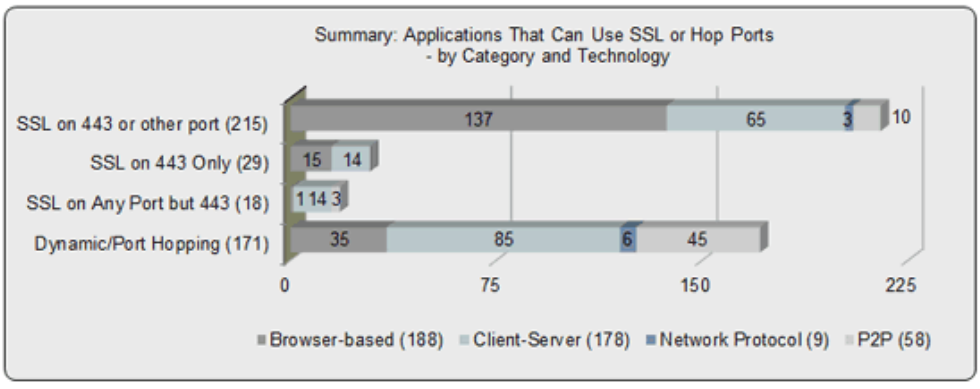

Figura 20 – Aplicações evasivas e suas estratégias (29)

Consultando o relatório publicado pela *Palo Alto Networks* elaborado em Maio de 2011 com o tema "The *Application Usage and Risk Report"* (29), conclui-se o seguinte relativamente à evasão das aplicações (Figura 20):

- Aplicações que de alguma maneira utilizam SSL representam 25% (262) das aplicações encontradas e são responsáveis pelo consumo de 23% da largura de banda. Prevê-se que este segmento cresça à medida que as aplicações como *Twitter, Facebook* e *Gmail* permitem a utilização de SSL;
- Aplicações dinâmicas representam 16% (171) das aplicações encontradas com um consumo de 13% da largura de banda. Este tipo de aplicativos inclui mensagens instantâneas, P2P, vídeo e foto.

Dos dados presentes na Figura 20 é curioso verificar que mais de metade das aplicações que recorrem a SSL não utiliza o *browser*. Diversas aplicações baseadas em arquiteturas cliente-servidor foram redesenhadas com objetivo de tirar proveito das tecnologias *web*. Ao mesmo tempo, determinadas empresas adoptam a utilização dos serviços alojados na nuvem de empresas como a *Google*, *Salesforce*,… que apesar de serem iniciados com um *browser* rapidamente se transformam numa arquitetura cliente-servidor.

Um caso gritante do sucesso na utilização das suas aplicações diz respeito ao Google. Consultando o relatório publicado pela *Palo Alto Networks* elaborado na primavera de 2010 com o tema "*Application Usage and Risk Report"* (30), é possível concluir que foram identificadas 22 aplicações Google, que se encontram distribuídas pelas seguintes categorias: produtividade (*Google Docs, Analytics, Calendar*), redes sociais (*Orkut*), comunicação (*Gmail, Gtalk, Voice*) e entretenimento (*YouTube, Picasa*). Como se pode constatar na Figura 21.

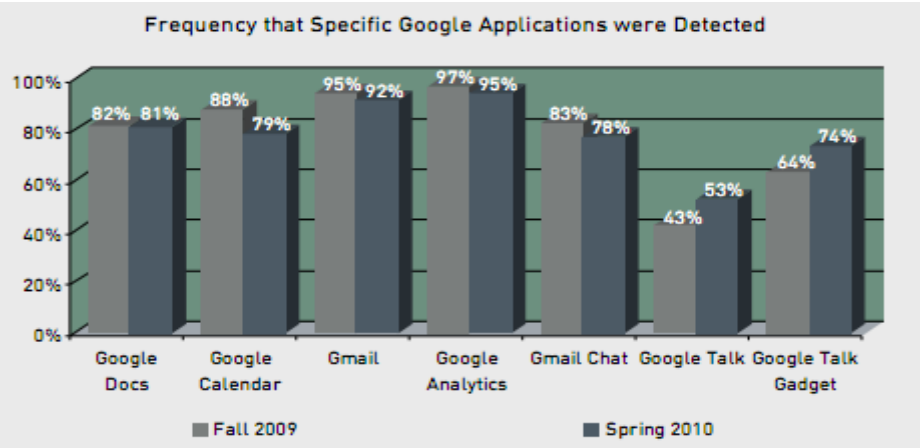

Figura 21 – Frequência de detecção das aplicações Google (30)

Estas aplicações foram encontradas com uma frequência indubitável nas organizações que participaram no estudo. Conclui-se também que, comparando com os dados do relatório de 2009, diminui ligeiramente a detecção destas aplicações, sendo que, foi registado um aumento do consumo da largura de banda das suas diferentes aplicações. Por exemplo o *Google Docs* passou a consumir mais 52% de largura de banda e viu o número de sessões aumentar em 42%.

3.3.3 - Ameaças

Com o aparecimento das aplicações *Web* 2.0 surgiu uma nova geração de ameaças de segurança, sendo que, a prevalência crescente de ataques resultantes da camada aplicação tornou-se uma tendência preocupante para as organizações e responsáveis pela segurança. Historicamente existia uma tendência de recorrer a um conjunto de defesas que forneciam a proteção da camada de rede. Com a predominância de aplicações que facilmente contornam estes mecanismos, as ameaças passaram a atacar diretamente os seus alvos sem qualquer oposição.

Se por um lado, as técnicas de evasão abordadas possuem a missão de facilitar a usabilidade das aplicações funcionando como portas de saída, por outro, permitem aos responsáveis pelas ameaças a sua exploração de forma a se infiltrarem nas redes, funcionando assim como porta de entrada. Ao contrário do passado, onde as ameaças tinham como foco as fragilidades das redes e serviços, no presente, o foco foi redirecionado para as debilidades existentes nas aplicações.

Se a todos estes factores juntarmos a confiança clara que os utilizadores colocam nas suas aplicações pode-se dizer então que estão reunidas as condições para a guerra começar, onde o elo mais fragilizado está do lado da organização.

3.3.3.1 - Alteração das estratégias de ataque

Em virtude de todas as alterações ocorridas, alguns atacantes também alteraram as suas estratégias. Em alguns casos, as mudanças consistiram no abdicar da sofisticação em prol da velocidade. A este fenómeno foi dado o nome de *zero-day exploit.*

O *zero-day exploit* significa tirar proveito de uma vulnerabilidade de segurança no mesmo dia em que a vulnerabilidade é universalmente conhecida. Ou seja, ocorrem zero dias entre o momento da descoberta até ao primeiro ataque. Normalmente, quando alguém detecta que uma aplicação contém um potencial problema de segurança, essa mesma pessoa notifica os responsáveis pelo seu desenvolvimento (às vezes o mundo em geral), de modo a que seja corrigida a falha. Durante este período o atacante vai tentar explorá-la.

As ameaças tornaram-se complexas e sofisticadas. Na maioria dos casos são praticadas de forma secreta, recolhendo silenciosamente os dados e passando o mais despercebidamente possível. Este tipo de comportamento, além de permitir a preservação da ameaça perante a

vítima, passa a imagem de conformidade. Um dos exemplos da sofisticação diz respeito à utilização de *exploits* ao nível do *kernel*, sendo mascarada a sua presença através de outros tipos de *malware.* Este estratagema permite realizar tarefas nefastas tais como captura de teclas ou ecrãs.

Outra das preocupações diz respeito a ataques direcionados ou as ameaças persistentes avançadas (APTs). Dentro deste tipo incluem-se ataques do tipo *Night Dragon*[23] ou à Operação Aurora[24], onde existe, por vezes, uma combinação de estratégias de engenharia social e ciber-ataques bem coordenados e dirigidos. Podem ser ainda empregados cavalos de Tróia, *software* de controlo remoto ou outros tipos de *malware*.

3.3.4 - Educação vs. Entretenimento

Ao longo dos tempos e como consequência do investimento na criação de redes de alta velocidade assim como na queda contínua dos custos da largura de banda, as Universidades têm apostado no incremento das suas ligações para a Internet. Atualmente, a maioria das principais Universidades Portuguesas encontram-se ligadas através de fibra óptica com débitos na ordem dos 10 Gbps, o que há uns anos atrás seria algo inimaginável. O aumento da largura de banda surge como necessidade de alargar a oferta online, oferecer aos utilizadores melhores recursos e serviços ou superar a sua carência.

A exaustação da largura de banda por vezes não significa que a rede da Universidade se encontre saturada ao ponto da única solução passar pelo seu aumento. Por vezes, poderá significar que os recursos existentes então sobrecarregados devido a uma utilização que não está de acordo com a premissa académica.

Um estudo realizado pela empresa PALOALTO[25], entre Junho de 2009 e Março de 2011 (31), junto de um conjunto de Universidades mundiais revela que 48% das aplicações descobertas (486 de 1022) consomem cerca de 86% da largura de banda disponível. Ao invés nos meios não Universitários a mesma categoria de aplicações mostra que 45% das aplicações (489 de 1075) consomem apenas 76% (31).

A variação de 10% poderá não ter grande impacto nem ser preocupante, o mesmo já não acontece com as variações de categorias que ocorrem entre o meio académico e o não académico, Figura 22.

- Nas redes universitárias, a partilha de ficheiros, a utilização de aplicações de foto e vídeo, são responsáveis pelo consumo de pelo menos três a seis porcento mais do que nos meios não académicos. As aplicações de áudio são caracterizadas pelo consumo de cerca de mais de dez pontos percentuais de largura de banda.

---

[23] https://kc.mcafee.com/corporate/index?page=content&id=KB71150
[24] http://www.mcafee.com/us/threat-center/operation-aurora.aspx
[25] Empresa de segurança de redes com soluções inovadoras na área dos NGFW. http://www.paloaltonetworks.com.

- Ao invés, nos meios não académicos existe um consumo de quase o dobro de aplicações categorizadas como utilitários de internet (*browsers*, *Google tools)* e de túneis encriptados. Em ambos os casos estas categorias de aplicações possuem um peso considerável.

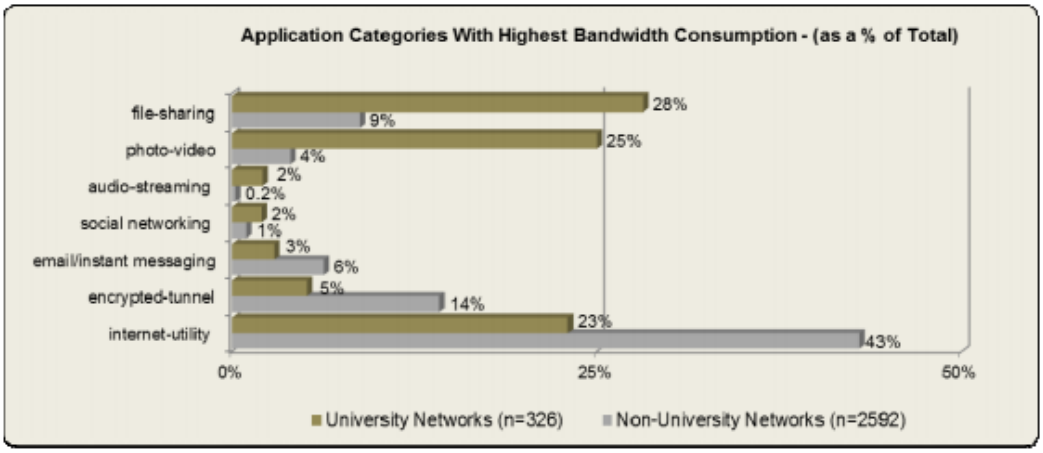

Figura 22 – Consumo de largura de banda em meio académico vs meio não académico (31)

Nos tempos atuais existe curiosidade em perceber o peso e o impacto que as redes sociais produzem dentro das instituições em virtude da sua *importância* na sociedade atual e dia-a-dia dos indivíduos.

Application Category	Non-University Networks		University Networks	
	# of Applications	% of Total Bandwidth	# of Applications	% of Total Bandwidth
File-sharing	113	9%	110	28%
Photo-video	95	4%	93	25%
Audio-streaming	31	0.2%	30	2%
Social networking	59	2%	60	2%
Email/instant messaging	129	6%	126	3%
Encrypted-tunnel	27	14%	23	5%
Internet-utility	35	43%	35	23%
Totals	489	78%	486	87%

Tabela 18 – Categorias com mais consumo de largura de banda (31)

O relatório revela dados surpreendentes no que diz respeito às redes sociais, Tabela 18. O peso desta categoria, tanto no meio académico como fora dele, é de apenas 2%. A existência de um valor tão pequeno quando a atividade social é imensa, poderá significar que no acesso a este tipo de serviço sejam utilizados outros tipos de dispositivos. Os *smartphones* são algumas alternativas que recorrendo à infraestrutura de dados do operador permitem ultrapassar os mecanismos de segurança da organização e "esconder" a atividade social diária em horário de laboração.

Através da análise da Tabela 18 é possível perceber também que aplicações da categoria correio electrónico/mensagens instantâneas possuem aproximadamente o dobro do impacto no que diz respeito a ambientes não universitários.

As redes académicas e científicas representam o mais antigo tipo de rede existente na sociedade. Surgiram em âmbito nacional e mundial com objetivo de assegurar uma concentração de interesses no desenvolvimento da educação e dos sistemas científicos e tecnológicos. O seu papel é o de promover a educação e a pesquisa, sendo que no contexto académico, a informação e o conhecimento são elementos fundamentais onde as redes cumprem (ou cumpriam) um papel determinante.

Das análises efectuadas conclui-se que as redes académicas deram lugar a redes de entretenimento e laser. Nos meios académicos verifica-se que existe um uso generalizado de aplicações não académicas onde salta à vista as relacionadas com entretenimento, colaboração e partilha de ficheiros. Aplicações como *Youtube*, vídeo podem indicar que a sua utilização poderá ser num ambiente misto onde se juntam interesses académicos e entretenimento.

3.4 - Desafios de Segurança 2011

Ao longo da história, a segurança vem se tornando numa das prioridades e preocupações mais relevantes para todas organizações. A sua importância é de tal forma que se tornou num requisito essencial para as organizações que pretendem competir numa economia caracterizada de globalizada e atingir resultados sustentáveis.

A crescente utilização da tecnologia, para além de criar vantagens competitivas, é responsável pelo aumento crescente de vulnerabilidades nos sistemas e tecnologias e no elevado grau de sofisticação que as ameaças apresentam dia para dia. Para além da complexidade, a história tem revelado que os interesses que movem os atacantes, as mudanças dos hábitos dos utilizadores são alguns dos fatores responsáveis pela constante mutação do tipo de ameaças e desafios de segurança nos últimos anos.

A Checkpoint, em 2011, no seu evento *Check Point Experience* realizado em 4 de Maio de 2011 em Barcelona, revelou a sua previsão dos 10 maiores desafios de segurança para 2011 (32) dos quais se destacam os seguintes pela sua importância e consonância com as previsões de outros fabricantes de segurança.

1. **Virtualização**

A virtualização é uma das tecnologias que nos últimos anos mais evoluiu e se implantou. O seu sucesso é resultante das poupanças obtidas com a sua utilização, na facilidade de implantação e gestão deste tipo de sistemas. Para além destas particularidades existem questões de segurança que justificam a sua utilização, como a facilidade do aumento da continuidade de negócio e recuperação a falhas, a existência de um único ponto de controlo de sistemas diversos e a capacidade adicional de auditoria que este tipo de sistemas fornece.

Apesar dos enormes benefícios, a virtualização é o foco regular de novas ameaças e *exploits*, existindo uma probabilidade elevada de exploração das suas vulnerabilidades. Os administradores de segurança e sistemas revelam, na maioria das vezes, falta de conhecimentos na camada adicional introduzida pelas plataformas de virtualização. Em algumas situações, as tecnologias de virtualização também se encontram ligadas às infraestruturas de rede e de armazenamento, necessitando por isso dum cuidado especial na implementação de controlos de acesso, permissões de utilizadores e controlos de segurança.

2. Cloud Computing

O *Cloud Computing* tal como a virtualização, tem sido uma área que nos últimos anos registou um enorme crescimento. As empresas, de dia para dia investem nesta abordagem a um ritmo frenético, armazenando as suas aplicações e ficheiros em serviços fornecidos na *cloud*.

Uma das principais vantagens é a redução dos altos custos com tecnologia e infraestrutura local, ganhando versatilidade e facilidade acedendo às suas aplicações de qualquer local.

Apesar dos benefícios na utilização deste tipo de tecnologia, existem diversos riscos no seu uso:

- **Perda de controlo sobre os dados:** Os dados sensíveis passam a ser processados fora da empresa. Este tipo de serviço foge do controlo "físico, lógico e pessoal";
- **Localização de dados**: Nos serviços alojados na *cloud* não se sabe a localização dos dados armazenados;
- **Segurança dos dados**: Como se garante a segurança dos dados da organização?
- **Interfaces inseguros:** Os interfaces de *software* usados pelos clientes para interagir com os serviços na *cloud* na maioria das vezes possuem problemas de segurança;
- **Perda de dados**: Os dados, apesar de se localizarem na *Cloud,* encontram-se em perigo de roubo.

3. Consumerização TI

A consumerização é um fenómeno que apareceu nos últimos anos resultante da experiência dos utilizadores com a tecnologia no dia-a-dia e como essa experiência influencia o uso de tecnologia em contexto de trabalho. Em alguns casos, os utilizadores pouco satisfeitos com as aplicações corporativas, procuram alternativas que sejam similares às utilizadas em contexto pessoal e melhorem as suas funções. Noutras situações, são utilizados equipamentos de consumo para trabalho como é o caso dos *smartphones* ou *tablets*.

Como a tecnologia desempenha um papel cada vez mais importante na vida pessoal, ficando as pessoas reféns da sua utilização, flexibilidade e conectividade, o utilizador quer que essas mesmas capacidades fiquem disponíveis em ambiente de trabalho.

A consumerização faz com que os funcionários levem para o ambiente de trabalho dispositivos móveis pessoais, que não são necessariamente permitidos ou geridos pelo departamento de TI, aumentando assim o risco de perda de informação

4. **Ameaças Atuais**

O cenário atual de ameaças é cada vez mais caracterizado pela sua sofisticação. A sua causa deve-se a motivos como o crime e lucro, guerra digital e *hacktivismo*. As recentes ameaças de maior dimensão incluem *Stuxnet*, operação Aurora e Zeus.

5. **Consolidação e Complexidade**

Atualmente as organizações lidam com um fenómeno consequente das infraestruturas de segurança serem constituídas por diversos produtos de segurança adquiridos ao longo dos tempos. Esta epidemia é responsável, na maioria dos casos, pela dificuldade e complexidade de gerir a infraestrutura de segurança. As organizações lidam também com um número crescente de prioridades de segurança sendo que os funcionários possuem poucas informações a respeito das políticas adotadas.
A tendência deverá ser a de convergir e unificar as tecnologias de segurança tornando o processo simples.

6. **Segurança e Perda de Dados**

As perdas de dados nas organizações poderão significar custos avultados. Na maioria das vezes as três principais fontes de perda de dados encontram-se nos dispositivos USB, portáteis, mensagens de correio eletrónico e webmails.

7. **Web 2.0**

Com a utilização crescente da Web 2.0 e o aparecimento de aplicativos de partilha de ficheiros, as empresas deparam-se com ameaças para o qual não se sentem preparadas. A consumerização aliada às aplicações *Web 2.0* é responsável pelo pisar do risco, que estabelece a fronteira entre o uso pessoal e profissional. Além das possíveis contra medidas a aplicar baseadas em tecnologia, este problema deverá passar sobretudo por um problema de educação e sensibilização dos utilizadores.

3.5 - *Firewalls* da Próxima Geração

Falar da segurança hoje em dia é falar num conjunto de mecanismos isolados que se revelam insuficientes para os desafios do quotidiano. Os *firewalls* encontram-se incluídos neste conjunto, sendo a escolha predominante no que toca à implementação de controlos de segurança. A sua popularidade resulta da facilidade de implementação, manuseamento e do seu rendimento.

Apesar de bastante frequentes, a tecnologia que suporta os *firewalls* tradicionais é medieval e desadequada para as necessidades atuais. A utilização de *firewalls* tradicionais no controlo de um perímetro de segurança é similar à de uma ponte num castelo. Isto é, apenas possui

aptidão para permitir ou negar acesso ficando à mercê de todos os outros desafios e problemas de segurança.

Ao olhar para a evolução histórica ocorrida na Internet, constata-se que existiram diversas transformações que tiveram consequências diretas na sua segurança. Factores como a mobilidade dos utilizadores, alteração do negócio, convergência de terminais e mudança das aplicações, são responsáveis por novos desafios de segurança e pelo fim do ciclo de vida dos *firewalls* tradicionais.

O caso mais gritante é visível na incapacidade que os *firewalls* tradicionais detêm para lidar com as novas aplicações de negócio, colaboração e entretenimento. A utilidade deste tipo de aplicações é inequívoca apesar do consumo excessivo de largura de banda, riscos de evasão, diminuição de produtividade e perda de dados que as caracterizam.

Com objetivo de colmatar as limitações dos *firewalls* tradicionais, as organizações investiram em diversos mecanismos complementares onde se incluem: servidores *proxy;* sistemas de detecção e intrusão e filtragem de URLs. Apesar de aumentarem a segurança das organizações revelam-se complexos, insuficientes e difíceis de gerir.

Os *firewalls* da nova geração conhecidos por *Next Generations Firewalls* (NGFW), apareceram para enfrentar os novos desafios de segurança resultantes da mudança dos processos de negócio, tecnologia e ameaças atuais.

Com os NGFW, o controlo e a segurança passa pela sessão e não pelos dispositivos. É possível limitar o acesso individual ou departamental a *sites* como o *Facebook* e *YouTube*. Impossibilitar o utilizador de aceder a jogos e outras aplicações das redes sociais ou até permitir que os funcionários possam ver as novidades nestes *sites* sem que possam interagir. O objetivo é conceder acesso apenas àqueles que necessitem, independentemente de trabalharem e acederem à Internet e à rede da empresa através de telemóvel, computador ou qualquer outro equipamento.

Os ficheiros e mensagens enviados para o exterior, através de correio electrónico ou outras aplicações (skype, Messenger), são analisados em tempo real e, se incluírem termos ou mensagens identificadas, o utilizador recebe uma mensagem a alertá-lo que a informação que está prestes a enviar contém dados confidenciais e que não está de acordo com a política da organização, questionando assim se a pretende enviar.

Os movimentos e atividade dos colaboradores são registados, o que permite através de análise concluir se o uso de determinada ferramenta é essencial para agilizar tarefas ou não, ou se determinados privilégios ou limitações contribuem para o aumento ou perda de produtividade.

As funções essenciais necessárias num *firewall* da próxima geração (NGFW) incluem a capacidade de:

- Identificação de aplicações, independentemente do uso de criptografia, porta, protocolo, técnicas evasivas ou SSL;
- Dar visibilidade e permitir o controlo das aplicações com base em políticas;

- Identificar com precisão utilizadores e usar a identidade como atributo usado nas políticas;
- Fornecer proteção em tempo real contra diversas ameaças, incluindo as existentes na camada aplicação;
- Integrar as funcionalidades de *firewalls* tradicionais com as capacidades de detecção e prevenção;
- Aplicação de qualidade de serviço às diferentes aplicações;

Além dos requisitos enumerados, estes dispositivos da nova geração possuem as capacidades dos *firewalls* tradicionais onde se incluí: filtragem de pacotes, utilização de *network-address-translation (*NAT) e *port-address-translation* (PAT), *statefull inspection* e suporte de *virtual private networks* (VPN).

O sucesso deste tipo de soluções reside na capacidade que detêm de combinar o papel dos *firewalls* tradicionais com competências avançadas que permitem integrar com tecnologias de identificação, alto débito e desempenho.

3.5.1 - Identificação de Aplicações

A correspondência entre protocolo e porta é um dos primeiros passos cruciais na identificação de aplicações, mas que por si só se revela insuficiente. A identificação requer uma fiscalização robusta que permita o controlo das aplicações e sessões que estão a ser usadas independentemente das tácticas de ocultação, protocolos, portas ou até mesmo encriptação.

As técnicas de identificação usadas nos dispositivos NGFW incluem:

- **Detecção do protocolo da aplicação** - Determina o protocolo da aplicação e se por alguma razão estiver a ser usado SSL faz a decriptação do tráfego com objetivo de o continuar a analisar. O tráfego é encriptado novamente depois das tecnologias de identificação terem atuado;
- **Descodificação do protocolo da aplicação –** Determina se o protocolo da aplicação inicialmente detectado corresponde ao "autêntico" ou se foram utilizados métodos de ocultação como é o caso de túneis;
- **Assinatura de aplicações –** Baseado em assinaturas, o motor procura por propriedades únicas nas características das transações com objetivo de identificar as aplicações corretamente independentemente do protocolo ou porta em uso. Esta funcionalidade permite dentro das aplicações detectar funções específicas como é o caso de aplicações utilizadas no *facebook*.
- **Heurística –** Para o tráfego que escapa na identificação com base em assinaturas, são aplicados mecanismos de heurística permitindo assim a sua identificação. Esta estratégia normalmente é aplicada em ferramentas como P2P ou VoIP, que por vezes recorrem a mecanismos de criptográfica proprietária.

A identificação das aplicações é um passo bastante importante. Mas será que apenas o seu reconhecimento é útil? O que adianta identificar se o utilizador não tiver sensibilidade para os riscos das aplicações? Na hora da tomada de decisão é necessário ter consciência dos riscos e ameaças inerentes na utilização de cada aplicação, daí ser importante selecionar mecanismos de NGFW que forneçam informação de vulnerabilidades, consumo de largura de banda, evasão…

3.5.2 - Identificação de Utilizadores

A identificação de utilizadores possibilita a criação de uma associação entre os utilizadores da organização e os endereços IP que lhe são atribuídos, permitindo assim ter acesso à visibilidade e ao controlo da atividade presente na rede. A integração dos NGFW com sistemas de diretório, como é o caso do LDAP ou *Active Directory* da Microsoft, é responsável por este objetivo em dois momentos. O primeiro verifica regulamente a relação utilizador endereço IP, seja através da integração existente entre o computador e o domínio ou recorrendo a técnicas de portal cativo. Num segundo momento, comunica regularmente com o diretório com o intuito de recolher informações relevantes dos utilizadores (o seu papel, grupos,). Esses detalhes possibilitam:

- Ter visibilidade acerca de quem é responsável pelas aplicações, conteúdo e tráfego relativo a ameaças na rede;
- Permitir a utilização da identidade como atribuição das políticas de controlo de acesso;
- Facilitar a procura de problemas e a resposta a incidentes.

A utilização de mecanismos de identificação de utilizadores possibilita a atribuição de direitos de utilização de aplicações de forma inteligente e optimizada. Se por um lado existem algumas aplicações que podem ser consideradas de risco elevado, devendo por isso ser impedidas, por outro lado, essas aplicações podem ser consideradas essenciais na atividade de determinados utilizadores. Com este mecanismo consegue-se atribuir permissões a utilizadores ou grupo de utilizadores de forma diferenciada.

Outra das vantagens claras nesta funcionalidade prende-se com a mobilidade dos utilizadores, onde a integração com diretórios permite que dentro da organização o utilizador, independentemente da sua localização, terá sempre garantido os seus direitos. Esta situação é possível em computadores integrados no domínio da organização ou através da utilização de um portal *web* integrado com autenticação no serviço de diretório.

3.5.3 - Identificação de Conteúdos

A identificação de conteúdos dota os NGFW da capacidade de prevenção em tempo real de ameaças no tráfego permitido, do controlo de todas as atividades associadas à navegação *web,*

assim como, a filtragem de ficheiros e dados. Este módulo, na maioria das vezes é constituído pelas seguintes funcionalidades:

- **Prevenção de ameaças** – Impede que ameaças do tipo *sypware*, vírus e vulnerabilidades penetrem na rede, independentemente das aplicações e tráfego onde residem;
- **Filtragem de URLs** – Usada para a classificação de conteúdos. Quando integrada, permite aos administradores o controlo e monitorização da atividade de navegação dos elementos das organizações. Conjugando esta funcionalidade com a identificação de utilizadores é possível atribuir políticas de navegação por utilizadores ou grupos de utilizadores.
- **Filtragem de dados e ficheiros** – Tirando a vantagem da inspecção das aplicações, permite execução de políticas que reduzem o risco de transferência de dados sensíveis ou confidenciais. Esta funcionalidade complementa a granularidade da identificação das aplicações, permitindo controlar a transferência de ficheiros dentro das aplicações (*Skype, MSN, Gtalk,)*.

A identificação de conteúdos tráz como mais-valia aos departamentos de TI das organizações a habilidade para parar ameaças, a redução do uso inapropriado de Internet e a capacidade de prevenir a fuga de dados confidenciais da organização.

3.5.4 - Perda de informação sensível

A informação é cada vez mais essencial e vital para o sucesso dos negócios. A sua violação ou perda é um dos maiores receios que as organizações enfrentam nos dias de hoje. Apesar da sua importância é frequente existirem notícias sobre incidentes de perda ou partilha de informação confidencial. Em Dezembro de 2008, como consequência de um P2P instalado numa rede militar, foi partilhada uma base de dados militar contendo informações pessoais de cerca de 24000 soldados do exército Americano.

Infelizmente é frequente existirem incidentes de segurança deste tipo, na maioria das vezes devido a utilização de aplicações que são expressamente proibidas pela política de segurança mas que não são validadas recorrendo a tecnologia adequada.

Em virtude das preocupações de perda de informação sensível e confidencial, surgiu a necessidade das instituições salvaguardarem o que consideram vital para o seu negócio, a sua informação. Alguns anos atrás não existia esta carência, não havendo por isso a necessidade de criar mecanismos que permitissem a salvaguarda de *Data Loss Prevention.*

A informação vital de uma organização pode ser partilhada através de correio electrónico, mensageiros, redes sociais, telefone, papel, …. Resumindo sobre qualquer meio que sirva para armazenar e/ou partilhar informações. Apesar de poderem existir políticas ou mecanismos físicos para a implementação de DLP, sabemos que o que se está a fazer é aumentar o custo/tempo de conseguir a informação. Basta olhar para a utilização de um cofre

como salvaguarda da informação. Todos podem ser abertos, demorando uns 3 minutos e outros vários dias ou semanas.

Para que a tarefa de salvaguarda de DLP tenha sucesso é importante tomar medidas dentro de uma "Política de Prevenção à Perda de Informações", aplicando-as a todos os colaboradores, prestadores de serviço ou qualquer outro que tenha acesso a informação vital e confidencial dentro da organização. Nestas medidas pode ser incluído, por exemplo, a elaboração dos seguintes documentos:

- Política de uso dos ativos virtuais;
- Termo de compromisso de confidencialidade.

As políticas, apesar de fazerem parte do primeiro passo, não são suficientes para garantir a segurança dos dados devendo a organização ser dotada de meios para monitorizar toda a informação que sai independentemente do meio utilizado.

Existindo a necessidade de implementação de mecanismos que monitorizem toda a informação, não fará sentido a sua integração nos mecanismos de segurança da organização? Ou até nos *firewalls*? Os NGFW permitem a utilização deste tipo de tecnologia que garante a salvaguarda da informação.

3.5.5 - Controlo de Políticas

A identificação das aplicações, utilizadores e conteúdos é uma tarefa importante que ajuda a perceber quais são as aplicações em uso na organização, por quem são utilizadas e para que fim são usadas. Este primeiro passo é essencial na aprendizagem do tráfego que circula na rede.

Uma vez pintado o quadro da rede da organização e percebidos os fluxos das aplicações, a tecnologia e os seus comportamentos, o próximo passo consiste na aplicação de políticas que respondam às necessidades das organizações. Ao contrário dos *firewalls* tradicionais que se limitavam a responder com um "permito" ou "nego", os NGFW possibilitam aplicação de respostas de controlo complexas e bastante refinadas.

Exemplos de algumas opções das políticas de controlo dos NGFW:

- Permitir ou negar;
- Permitir mas procurar *exploits*, vírus e outras ameaças;
- Permitir com base em horários, utilizadores ou grupos;
- Decifrar e inspecionar;
- Aplicar regras de QoS;
- Permitir ou restringir determinadas funções das aplicações.

4 - Avaliação da Arquitetura de Segurança Existente

O objetivo deste trabalho pressupõe a definição de uma nova arquitetura e mecanismos de segurança para a rede do IPL. Como para decidir é necessário avaliar, nesta seção do documento será realizada uma avaliação da arquitetura de segurança, assim como dos mecanismos em laboração. Alguns dos fatores que justificam a necessidade de avaliar antes de decidir são:

- Identificar a magnitude do problema e fornecer elementos que comprovem a necessidade de uma nova solução;
- Compreender os mecanismos em vigor, os pontos fracos e avaliar a eficácia das soluções implantadas;
- Fornecer dados que por base possam ser usados para monitorizar o sucesso da nova solução.

No decorrer desta etapa, serão identificadas fraquezas no desenho e limitações na infraestrutura. Inicialmente será caracterizada a infraestrutura de rede, sendo posteriormente apresentada a avaliação da arquitetura e dos mecanismos que a compõem. Com o intuito de conhecer o uso dado à rede do IPL e perceber o risco que advém desse uso, é apresentado um relatório de análise de visibilidade de aplicações e segurança com resultados bastante surpreendentes e interessantes.

4.1 - Caracterização da Infraestrutura de TI

O IPL é uma instituição pública de ensino superior politécnico, ao serviço da sociedade, destinada à produção e difusão do conhecimento, criação, transmissão e difusão da cultura, da ciência, da tecnologia e das artes, da investigação orientada e do desenvolvimento experimental.

É caracterizado por ser a única instituição pública de ensino superior do distrito de Leiria, ocupando o título de terceiro maior politécnico do país. Atualmente possui uma população constituída por mais de 12000 estudantes sendo aproximadamente 1200 funcionários, docentes e não docentes.

Enquanto infraestrutura de comunicações, o IPL encontra-se suportado num *backbone* comutado de fibra óptica que lhe permite transportar diversos canais de 1Gbps, oferecendo comunicações e recursos quase sem limites para os seus alunos, docentes, funcionários e não docentes. É uma infraestrutura baseada na tecnologia IP (*Internet Protocol*), o que a torna extremamente flexível e interoperável com outras redes.

Nos diversos Campus do IPL, não existe uma verdadeira distinção entre a camada de distribuição e o core da rede. Os equipamentos de core têm sempre funções de distribuição e vice-versa.

Os polos remotos localizados em Leiria e Caldas encontram-se ligados a Leiria através de uma solução de rede privada, implementada com o recurso a um sistema de transmissão por micro-ondas. A solução é suportada numa ligação sem fios em banda licenciada com uma largura de banda aproximada dos 100 Mbps *full-duplex*, sendo que, como *backup* existem caminhos alternativos a 10 Mbps *half-duplex* em banda não licenciada. O esquema da ligação encontra-se representado na Figura 23.

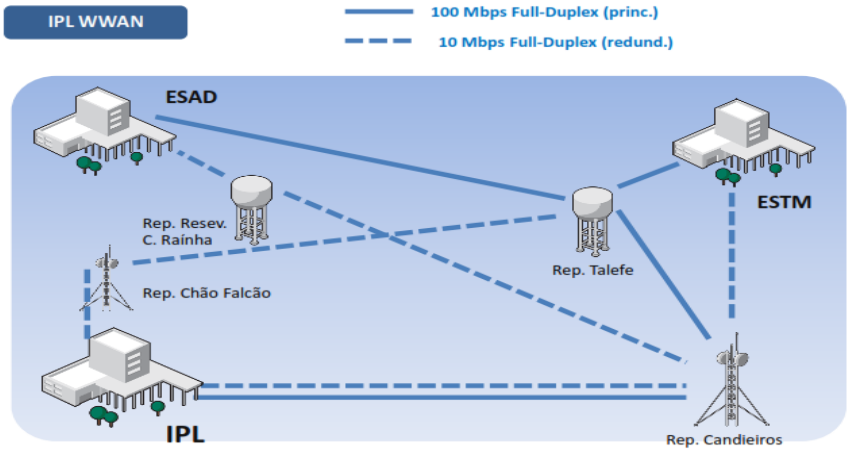

Figura 23 – Ligação WWAN de Leiria, Caldas e Peniche

4.1.1 - Ligação Internet

O IPL encontra-se ligado à Internet através de uma ligação em fibra óptica entre o IPL e a FCCN, suportada num cabo de 24 fibras com cerca de 180 Km. A ligação existente permite transportar diversos canais de 10Gbps, sendo que, apenas 200 Mbps desse tráfego é comercial.

Os polos remotos para o caso de falha na WWAN entre Leiria, Caldas e Peniche, possuem localmente uma ligação ADSL para a Internet que serve de complemento e *backup* da ligação principal.

4.1.2 - VLANs

Desde à muito que o IPL decidiu realizar a segmentação das suas redes através da utilização de VLANs. Esta opção surgiu devido às inúmeras vantagens das quais se destacam:

- **Aumento do nível de segurança** – Através das VLANs é possível conceber uma separação de domínios lógicos, o que permite que na camada dados seja dificultado o acesso a quem não pertença ao mesmo domínio;
- **Independência da topologia física** – Garante um alto nível de flexibilidade porque os domínios lógicos podem ser alterados, sem que haja necessidade de adquirir mais equipamentos ou realizar qualquer alteração na rede física;
- **Aumento no desempenho** – Os domínios de *broadcast* ficam limitados, sendo estas transmissões restringidas somente a cada domínio, evitando desta forma tráfego desnecessário.

Como a rede interna que compõe o IPL apresenta uma dimensão considerável e existem diversas sub-redes com necessidades específicas que necessitam de níveis de proteção em relação às restantes, existiu a necessidade de dividir as redes de forma a segmentar o tráfego entre estas. Nos diferentes campus existem as diferentes sub-redes:

- Redes de alunos – Divididas por cursos e tipo;
- Redes de docentes – Divididas por departamentos;
- Redes de funcionários – Divididas por tipo de serviço;
- Redes sem fios – Divididas por tipo de utilizador;
- Redes de serviços – Divididas por tipos de serviços TI (VoIP, Servidores, …)
- Redes de Gestão – Divididas pelos diferentes tipos de equipamentos.
- ….

Em cada polo, na sua rede interna existe um conjunto de VLANs diferenciado que não é conhecido nos outros polos. Este desconhecimento deve-se à arquitetura descentralizada que o IPL apresentava até 2007, sendo que existem algumas situações (VoIP e alguns serviços) onde a VLANs é partilhada por todos os Campus.

A gestão das VLAN é feita de forma local, utilizando o protocolo do fabricante *cisco* VTP para a sua gestão. A comunicação entre VLANs por defeito encontra-se negada, sendo apenas permitida nos casos em que é estritamente necessário.

4.1.3 - Endereçamento

Cada unidade orgânica do IPL possui uma classe privada IPv4 atribuída para a rede interna, sendo que, os endereços encontram-se distribuídos pelas diferentes VLANs existentes. A atribuição dos endereços, na maioria das vezes, é feita de forma centralizada através do serviço DHCP.

No que diz respeito ao endereçamento público, cada instituição possui um conjunto de endereços atribuídos para distribuir pelos seus serviços (DNS, Web, RADIUS,…). Esta

abordagem foi tomada antes da centralização do IPL onde cada Instituição era responsável pela gestão da sua unidade TI.

Apenas existe pegada de endereçamento IPv6 na interligação com a FCCN e em alguns projetos académicos.

4.1.4 - Redes sem fios

O IPL possui uma infraestrutura de comunicações sem fios, proliferada por todas as suas escolas. A rede é constituída por cerca de 200 pontos de acesso do fabricante cisco, distribuídos pelos diversos Campus, o que representa uma cobertura aproximada dos 90%. Esta rede surgiu com a iniciativa eduroam[26] que fornece acesso à rede sem fio para pesquisa e educação à comunidade universitária e seus convidados.

A tecnologia assenta nos padrões 802.11b e 802.11g, sendo que, mais recentemente foi implantado 802.11n nos locais estratégicos dos edifícios mais atuais. As vantagens na utilização de 802.11n dizem respeito às taxas elevadas de transmissão e à cobertura espacial disponibilizada.

A rede sem fios do IPL disponibiliza dois SSID (eduroam e guest-e-U) que servem para identificar duas redes distintas. O SSID eduroam, é um identificador de rede oculto que se destina à rede do projeto eduroam e a servir toda a sua comunidade, sendo caracterizado pela utilização do protocolo de segurança WPA. O guest-e-U originário do início do projeto e caracterizado por ser difundido, não possui qualquer tipo de segurança. A sua missão é disponibilizar acesso a informação que permita ajudar na configuração da rede eduroam. Este SSID serve de suporte a terminais que não consigam utilizar a rede eduroam. Nestas situações é utilizado um mecanismo de *webbased login* autenticado no Radius.

Dentro da rede sem fios existem quatro perfis diferenciados de utilizadores:

- Alunos do IPL
- Docentes do IPL
- Funcionários do IPL
- Convidados eduroam

A distinção dos utilizadores é feita através da autenticação, sendo que em função do tipo utilizador são atribuídos privilégios distintos. Este processo só é possível devido à existência de uma infraestrutura de autenticação composta por 802.1 X, *Radius* e *Active Directory* da Microsoft, como se pode verificar na Figura 24.

[26] Iniciativa eduroam http://www.eduroam.pt/.

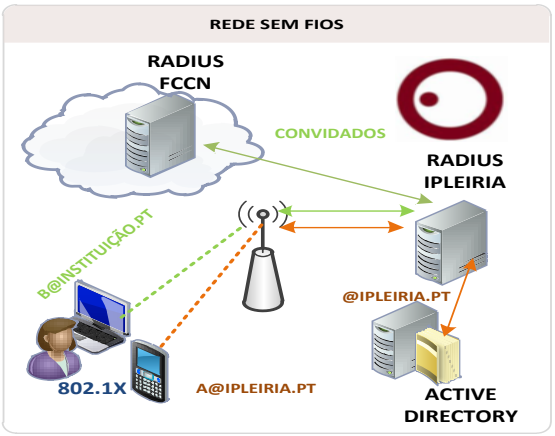

Figura 24 – Infraestrutura rede sem fios

Por questões de regulamentação do projeto eduroam é obrigatório a atribuição de endereços públicos aos utilizadores convidados em *roaming* nas instituições.

4.1.5 - Autenticação

A infraestrutura de autenticação do IPL assenta no serviço de diretório da Microsoft conhecido por *Active Directory (AD)*. Os diversos serviços existentes no IPL são autenticados no domínio IPLeiria.pt suportado no AD. A autenticação de serviços como VPN e redes com fio é feita através da mesma infraestrutura de autenticação.

4.1.6 - Tipos de utilizadores

As Universidades e Politécnicos são caracterizadas por serem meios abertos de pouco controlo físico de segurança onde sem qualquer dificuldade, qualquer pessoa consegue entrar e ter acesso aos seus recursos.

A definição do tipo de utilizadores é um dos aspectos de segurança muito importante em redes Universitárias, tendo em conta que esta dispõe duma comunidade de utilizadores bastante numerosa e complexa em termos das necessidades de utilização dos recursos.

No IPL, e, genericamente sem chegar ao nível detalhe das diferentes características dos utilizadores, são identificados os seguintes tipos: alunos, funcionários não docentes, docentes, convidados e externos.

Os alunos são caracterizados por pertencerem a uma escola do IPL, existindo casos em que estão alunos a frequentar o IPL mas que pertencem a outras Instituições de Ensino Superior, como ocorre nos cursos dados em parceria ou nos alunos de Erasmus.

Os funcionários encontram-se distribuídos pelos diversos serviços que compõem o IPL. Existem funcionários permanentes e funcionários temporários como é o caso dos estagiários ou participantes em projetos ou programas do centro de emprego e formação profissional.

Os docentes pertencem a uma determinada escola, podendo leccionar em todas as escolas do IPL. Como acontece com os funcionários, existem docentes a tempo inteiro e temporários.

Aos convidados pertencem os alunos, docentes e funcionários de outras instituições que por alguma razão se encontram no IPL e fazem uso da infraestrutura sem fios ao abrigo do projeto *eduroam*.

Por último, os externos. Aqui inserem-se as pessoas que pertencem a entidades ou organizações externas e que prestam serviço no IPL direta ou indiretamente através de projetos ou outro tipo de parceria.

Os utilizadores do tipo: aluno, funcionário e docentes a partir do momento que pertençam ao IPL é-lhes atribuído uma conta que permite ter acesso a toda a infraestrutura de dados e recursos disponibilizados.

4.1.7 - Acessos remotos

O serviço de acesso remoto via VPN , visa permitir o acesso seguro à rede de comunicações do IPL aos membros da comunidade académica, independentemente do local onde se encontrem.

A VPN utiliza recursos de criptografia para garantir a integridade e a confidencialidade dos dados transmitidos através da rede pública. Este serviço pode ser acedido pelos clientes sendo independente da ligação de dados utilizada. O uso deste serviço implica a instalação de um cliente VPN específico por parte do cliente.

4.1.8 - Sistemas operativos

Sendo um ambiente académico constituído por escolas de diferentes tipos, existe uma diversidade de sistemas operativos na organização. Destaca-se a utilização de clientes baseados em Windows, Linux e Mac OS. Na gama dos dispositivos móveis, a preferência recai na utilização de iOS[27] e android[28].

4.1.9 - Dispositivos e Mobilidade

Nos últimos anos, a mobilidade dos utilizadores alterou-se devido à proliferação do uso de novos dispositivos móveis nas infraestruturas. Os utilizadores passaram a fazer o uso primordial de dispositivos como portáteis, PDAs, telefones “inteligentes” e mais recentemente de Tablets. Das estatísticas existentes de acesso na rede sem fios, estima-se que mais de 60%

[27] Sistema operativo destinado a dispositivos móveis como é o caso do iPhone, iPod Touch ou iPad.
[28] Sistema operativo móvel destinado a telemóveis.

da população académica detenha equipamentos desta natureza, sendo que, existem utilizadores que possuem mais do que um dispositivo.

No que diz respeito à mobilidade, verifica-se que cada vez mais os utilizadores privilegiam a utilização da infraestrutura de rede sem fios através de dispositivos móveis.

A maioria dos dispositivos móveis são geridos e controlados apenas pelo proprietário. Os Serviços Informáticos do IPL não possuem forma de garantir a conformidade de segurança nestes dispositivos, assim como, o controlo das aplicações e mecanismos de segurança instalados.

4.2 - Avaliação da Arquitetura e Mecanismos de Segurança

Uma arquitetura de segurança para uma infraestrutura de TI atua como um manual em relação ao qual um programa de gestão de segurança é executado. Numa arquitetura define-se: o conjunto de serviços de segurança que devem ser implementados para satisfazer os requisitos do negócio; os elementos requeridos para implementar esses serviços e os níveis de serviços requeridos a esses elementos para conseguir gerir as ameaças identificadas, i.e. manter o nível de risco dentro dos limites aceites pela organização.

De acordo com a arquitetura SAFE da Cisco, os principais elementos de uma arquitetura de segurança são; a infraestrutura tecnológica de suporte e o controlo de acessos; o programa de gestão de segurança; a manutenção dos níveis de serviço e a análise de vulnerabilidades.

Grupo de Elementos	Elementos
Infraestrutura e Controlo de Acessos	Requisitos de disponibilidade e resiliência tecnológica
	Segurança do Perímetro Externo e Prevenção Contra Intrusões
	Identificação, Autenticação, Autorização e Gestão de Contas de Utilizadores
	Segurança nos Acessos Remotos
	Monitorização de Segurança
Programa de Gestão de Segurança	Gestão Centralizada da Infraestrutura
	Identificação de Requisitos, Definição de Política e Procedimentos de Segurança
	Organização da Segurança
Manutenção dos Níveis de Serviço	Definição, Implementação de Configurações Mínimas de Segurança
	Formação de Utilizadores
	Gestão de Incidentes, Configurações e Alterações de Segurança
Análise de Vulnerabilidades	Prevenção, deteção e remoção de *software* malicioso e Controlo de Acesso a Conteúdos na Internet
	Análise de Vulnerabilidades
	Proteção de Informação Confidencial

Tabela 19 – Principais elementos de uma arquitetura de segurança

Nos pontos seguintes será avaliada a arquitetura de segurança da infraestrutura de TI do IPL de acordo com a metodologia e pontos referidos anteriormente. Para cada ponto, caso se

identifiquem, serão sugeridas medidas na proposta de arquitetura estudada no Capítulo 5, com objetivo de melhorar a infraestrutura. Na avaliação será dada especial atenção à arquitetura, visto tratar o principal foco neste estudo.

4.2.1 - Avaliação da Arquitetura Existente

A arquitetura de segurança do IPL é caracterizada por ser uma arquitetura com alguns anos de laboração e se encontrar desajustada às necessidades e desafios atuais. Surgiu em 2004, ao abrigo do projeto Campus Virtual[29] com objetivo de colmatar os problemas de segurança existentes e para servir de suporte aos desafios lançados com a implementação do projeto.

Durante a execução do projeto, o IPL era caracterizado por ser uma instituição descentralizada onde cada escola possuía autonomia, cabendo a si a gestão local dos recursos existentes. No que diz respeito aos departamentos de TI, cada instituição detinha os seus recursos humanos e as suas infraestruturas de TI. A única infraestrutura partilhada por todas as instituições dizia respeito ao acesso à Internet que se encontrava localizado na Escola Superior de Tecnologia e Gestão sendo gerido pelo departamento de TI afeto a este local.

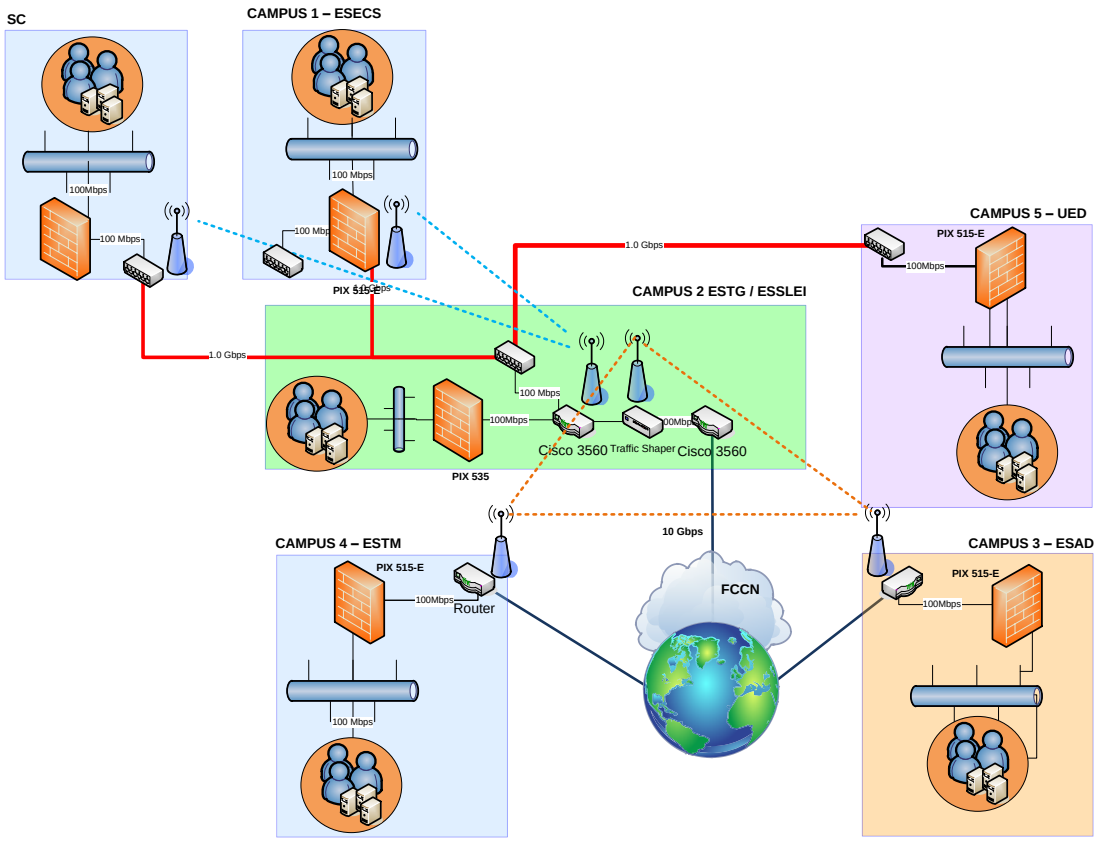

Figura 25 – Arquitetura de segurança antes da centralização

[29] Projeto Campus Virtuais, iniciativa da UMIC http://www.e-u.pt/PresentationLayer/eU_homepage.aspx.

O projeto da arquitetura de segurança e serviços, presente na Figura 25, teve em conta a descentralização. Foram contempladas infraestruturas de segurança semelhantes em cada escola do IPL tendo sido também criadas zonas de segurança idênticas. A solução, consistiu na aquisição de *firewalls* tradicionais (*Cisco Pix*) e na criação de DMZs (zonas desmilitarizadas) diferenciadas com o intuito de segurar e limitar os perímetros das diferentes infraestruturas de rede a alojar, assim como os serviços a fornecer.

A comunicação entre as diferentes instituições do IPL era efetuada recorrendo a endereçamento público como se de uma instituição estranha se tratasse, isto apesar da partilha do acesso à Internet.

Em 2007, o IPL procedeu à reestruturação administrativa e financeira passando por isso a estar centralizadas no IPL as operações daquela natureza. Como reflexo da centralização, os recursos de TI foram unificados, dando origem a uma unidade denominada serviços informáticos com a responsabilidade de gerir todos os recursos e infraestruturas TI do IPL. A centralização foi ainda responsável pelo surgimento de novos desafios do qual se destacam:

- Junção e centralização das aplicações financeiras, académicas e recursos humanos;
- Criação de sistema de autenticação único;
- Unificação de serviço de correio electrónico;

As exigências a que a centralização conduziu, fizeram com que a arquitetura tivesse que responder a todos os desafios impostos rapidamente sem que fossem realizadas intervenções profundas na arquitetura. A primeira necessidade foi a criação de uma DMZ para os serviços centralizados.

A escolha recaiu pelo alojamento dos serviços na DMZ existente no *Campus 2*, e deveu-se aos seguintes factores:

- Localização central do Campus;
- Débitos e funcionalidades do *firewall* existente;
- Campus com maior número de utilizadores;
- Existência de mecanismos de QoS e priorização de aplicações.

A arquitetura, ao longo dos tempos, tem-se revelado insuficiente apresentando diversas limitações para as necessidades existentes. Da sua análise destacam-se as seguintes:

1. Solução suportada em equipamentos *firewalls* obsoletos e descontinuados pelo fabricante;
2. Baixos débitos dos *firewalls*, funcionando com pontos de estrangulamento da rede. O core da rede funciona a 1Gbps, sendo que na maioria dos casos os *firewalls* apenas suportam 100 Mbps;
3. Não existe redundância dos equipamentos de segurança. No caso de falhar algum equipamento deste tipo a rede ficará isolada, existindo apenas acesso local;

4. Os equipamentos de segurança não possuem mecanismos de reposta a ataques do tipo IDS/IPS;
5. Os perímetros e zonas de segurança existentes encontram-se desajustados às necessidades do IPL e aos desafios atuais;
6. O endereçamento IP público do IPL encontra-se distribuído pelos diversos componentes da arquitetura o que faz com que não seja feita de forma eficiente e que exista desperdício de recursos;
7. Não existe quaisquer mecanismos de controlo de acesso à rede com fios. Um utilizador pode aceder a uma tomada de rede e ligar um dispositivo tendo acesso imediato à infraestrutura do IPL;
8. As políticas de segurança são estáticas e encontram-se distribuídas pelos diferentes componentes da arquitetura da Figura 25. Isto significa que os utilizadores que se encontrem em mobilidade pelos Campus do IPL percam os acessos a que têm direito ou então que os gestores da infraestrutura de segurança sejam obrigados a replicar os acessos pelos diferentes componentes da arquitetura;
9. A gestão da infraestrutura de segurança é feita de forma individual, o que significa que se for necessário abrir a comunicação com destino a um determinado porto para toda a comunidade seja necessário aceder a todos os componentes da arquitetura para o fazer;
10. Não permite a visibilidade dos utilizadores assim como realizar o rastreio de toda a sua atividade;
11. A arquitetura não permite tirar partido dos dois centros de dados existentes.

4.2.2 - Infraestrutura e Controlo de Acessos

Nesta fase serão avaliados os requisitos de disponibilidade da infraestrutura em análise assim como a segurança do perímetro da rede, acessos remotos e redes sem fios, gestão de identidades e utilizadores e o processo de monitorização de segurança.

Requisitos de disponibilidade e resiliência

A infraestrutura de IT do IPL suporta um nível de utilização contínuo, 24 horas 7 dias por semana, exigindo-se dela, tempos de indisponibilidade máximos inferiores a 2 horas. Nestas condições, a utilização de uma infraestrutura de comunicações redundantes, sistemas críticos redundantes e serviços IP redundantes é uma necessidade.

A rede de comunicações LAN do IPL compõe-se de um core suportado em diversos equipamentos *Cisco 6500* e 3560, que fornecem ligação a diversos *switches* espalhados pelos campus. Os *switches* de *edge* não possuem redundância de conectividade ao core.

Recomendação
Nos *switches* de *edge* que não possuem redundância de conectividade podem ser criados caminhos alternativos através de canais *wireless*.

Deve ser ponderada também a introdução de uma solução de monitorização de equipamentos de comunicações em termos de tipo e quantidade de tráfego processado, alertas gerados sobre desempenho, disponibilidade e tráfego anómalo.

Segurança do Perímetro Externo

A arquitetura do IPL não assegura que nas ligações entre redes de comunicações internas do IPL e o exterior estejam instalados mecanismos para controlo de tráfego e proteção contra tentativas de intrusão aos recursos internos de TI da organização, nomeadamente sistemas de *firewalls* e de detecção e proteção contra intrusões em rede. Assim, a segurança do perímetro externo não está acautelada. É ainda evidente a falta de proteção e detecção contra intrusões ao nível dos servidores críticos da organização contra tráfego e atividades indesejadas.

Recomendação
Introduzir uma solução de detecção/proteção contra intrusões ao nível dos serviços críticos.

Identificação, Autenticação, Autorização

O processo de gestão de identidades suportado na arquitetura baseia-se na utilização de um serviço de diretório centralizado e na atribuição de perfis de acesso com tempo de vida limitado. Este posicionamento é adequado numa primeira fase.

A inexistência de um processo automatizado de gestão de identidades que permita definir formalmente os procedimentos para requisição, criação, ativação, suspensão e cancelamento de contas de utilizador no sistema automatizado é umas das debilidades apontadas neste ponto.

Segurança nos Acessos Remotos e Acessos Sem Fios

Nos últimos anos a mobilidade que surgiu com a introdução de novos dispositivos no IPL gerou outra classe de riscos de segurança. A proliferação do uso de dispositivos móveis fez com que o perímetro da rede do IPL protegido com *firewalls* tradicionais tivesse "desaparecido" e sido estendido até ao terminal sendo que o controlo destes dispositivos na maioria dos casos não pertence ao IPL.

A rede sem fios, tornou-se na principal porta de entrada de ameaças internas no IPL. Os PDAs, telefones "inteligentes" e os *tablets*, utilizam sistemas operativos e aplicações que incluem vulnerabilidades que podem ser exploradas de forma semelhante aos computadores portáteis.

Por todas estes motivos é necessário verificar a conformidade dos postos de trabalho que acedem à infraestrutura de comunicações do IPL face às políticas de segurança pretendidas pelo IPL, por exemplo em termos de deteção e remoção de *software* malicioso.

Recomendação
Introdução de uma solução de controlo de admissão à rede, pelo menos, para acessos remotos e acessos via redes sem fios, que permita verificar a conformidade da estação de trabalho em relação às políticas de segurança do IPL.

Monitorização de Segurança

A efetividade do nível de segurança disponibilizado quer pelos mecanismos quer pelos procedimentos, deve ser monitorizada centralmente para se detectar comportamentos anómalos ou desvios face à implementação das políticas pretendidas. A arquitetura não contempla mecanismos centralizados capazes de assegurar a monitorização de tráfego e eventos de forma centralizada e garantir a aderência aos níveis de segurança preconizados para a organização.

Recomendação
Aplicar uma solução de monitorização capaz de normalizar, agregar, classificar e analisar eventos de segurança oriundos dos distintos equipamentos que constituem a infraestrutura TI do IPL.

4.2.3 - Gestão de Segurança

O processo gestão de segurança possui uma importância extrema em qualquer infraestrutura TI. Neste ponto será avaliada a forma de estabelecer e gerir a política de segurança na organização, o processo de monitorização da segurança e de que maneira se audita o cumprimento das regulamentações definidas.

Gestão Centralizada da Infraestrutura

A infraestrutura de TI possui mecanismos adequados aos procedimentos de gestão, nomeadamente a disponibilização de segmentos de rede dedicados para a gestão. No entanto, dada a multiplicidade e dispersão de equipamentos, em particular no que concerne aos equipamentos de acesso sem fios (AP), deve-se assegurar que os mesmos possam ser configurados e geridos a partir de uma plataforma central de forma a minimizar erros de configurações e ajudar na rápida introdução de novas políticas de segurança.

Recomendações
Aplicar solução de gestão de gestão centralizada para equipamentos de acesso *wireless*.

Identificação de Requisitos, Definição de Política e Procedimentos de Segurança

O planeamento, implementação, gestão e atualização da arquitetura de segurança requer a identificação e consolidação dos requisitos de segurança de TI da organização e a definição formal das normas e procedimentos de segurança de TI pretendidos, uma política de segurança. O IPL não possui política de segurança em funcionamento com os objetivos de segurança pretendidos para proteção dos recursos da organização.

Recomendações
Ponderar a formalização da política de segurança do IPL, definindo-se objetivos de segurança pretendidos para proteção dos recursos da organização.

Organização da Segurança

Apesar de existir definida uma organização de segurança no IPL com referência a pessoas, funções e responsabilidades, com a função de implementar e gerir a segurança de TI, não existem políticas de segurança definidas.

4.2.4 - Manutenção dos Níveis de Serviço

Em qualquer organização é essencial que os níveis de serviço se mantenham dentro dos parâmetros estabelecidos como aceitáveis. Na avaliação de segurança, a manutenção dos níveis de serviço da infraestrutura preocupa-se com todos os instrumentos existentes para o cumprimento deste nível.

Definição, Implementação de Configurações Mínimas de Segurança

A definição e implementação controlada de configurações mínimas de segurança em recursos de TI, de acordo com as políticas da organização e indicações dos fabricantes, é uma medida importante na mitigação de riscos de segurança permitindo a análise de desvios e a correção atempada de falhas de segurança identificadas pelos fabricantes. A infraestrutura do IPL não possui mecanismos que o permitam fazer.

Recomendações
Ponderar a implementação de uma solução de análise e controlo de configurações de segurança nos equipamentos.

Gestão de Incidentes, Configurações e Alterações de Segurança

Qualquer infraestrutura deve assegurar que as alterações efetuadas sobre os recursos de TI, ou incidentes que ocorram sobre esses mesmos recursos, estão enquadrados por um plano de ação que permita lidar com estes eventos, mantendo o nível de segurança preconizado para a organização. O IPL não possui um processo desta natureza que seja capaz de, entre outras situações, lidar eficientemente com situações inesperadas, como é o caso de incidentes ou desastres.

Recomendações
Avaliar se a equipa que suporta o *front-office* está na posse de informação que lhe permita gerir incidentes e acompanhar situações de desastre de acordo com os objetivos do IPL.

4.2.5 - Análise de Vulnerabilidades

Estando a maioria das informações baseadas em tecnologia, é imperativo que as vulnerabilidades inerentes à infraestrutura tecnológica sejam geridas.

É essencial fazer análise de vulnerabilidades em qualquer infraestrutura para que a gestão e manutenção dos riscos advindos de tais vulnerabilidades sejam efetivos.

Prevenção, detecção e remoção de *software* malicioso e Controlo de Acesso a Conteúdos na Internet

Nos postos de trabalho não controlados diretamente pelo IPL não é garantido o controlo de postura ao nível do posto de trabalho. Sendo que não se consegue impedir a entrada de vírus, *worms, spywares* ou outras aplicações maliciosas.

Análise de Vulnerabilidades

Não é ainda garantida a detecção atempada de vulnerabilidades nos ativos de TI nem a mitigação antecipada de riscos de segurança.

Recomendações
Implementação de solução de análise de vulnerabilidades automática para testar as configurações de equipamentos de comunicação e servidores críticos.

Proteção de informação confidencial

Não existe processo de classificação da informação de carácter confidencial por parte do IPL, assim como mecanismos de encriptação de dados e armazenamento seguro de informação.

Recomendações
Avaliar a necessidade de introdução de mecanismos de armazenamento seguro de informação capaz de proceder à encriptação e assinatura de dados.

4.3 - Análise de Segurança e Visibilidade de Aplicações

Com objetivo de perceber as ameaças de segurança e debilidades existentes no IPL, foi elaborado um relatório de análise de risco e visibilidade de aplicações. Este relatório inicia com um resumo das principais descobertas, apresentando uma visão global da apreciação de risco aplicacional. Além disso, é feito uma análise de todo o tráfego, riscos e ameaças existentes, sendo exibida uma imagem de como a rede está a ser utilizada por parte dos utilizadores do IPL. O relatório termina com um resumo e um conjunto de ações recomendadas para os problemas encontrados.

Da análise, salta à vista: a quantidade de aplicações não corporativas que são usadas veemente no IPL, algumas prejudicando a produtividade dos funcionários da organização; número de aplicações usadas para disfarçar atividade e passar mecanismos de segurança implementados; os riscos de perda de dados confidenciais essenciais à organização e a possibilidade de

violação dos direitos de autor e o consumo exagerado de largura de banda e tempo em aplicações de entretenimento.

Os dados apresentados neste relatório dizem respeito a um período de análise de uma semana.

4.3.1 - Metodologia de Análise

A análise de visibilidade de aplicações e riscos, foi elaborada recorrendo ao uso de um *firewall* de nova geração do fabricante PALO ALTO no ambiente de produção que compõe a infraestrutura rede do IPL. A utilização das tecnologias, *App-ID*[30], *User-ID*[31] *e Content-ID*[32] deste fabricante, permitiu ter acesso a dados de visibilidade de aplicações, utilizadores e conteúdos que navegavam pela rede do IPL, tendo sido descobertas informações curiosas, sendo algumas desconhecidas dos responsáveis pela gestão da infraestrutura.

Uma das principais preocupações na elaboração da análise foi o impacto provocado na infraestrutura de rede com a introdução de novos mecanismos de segurança estranhos ao sistema. A necessidade de realizar testes de segurança, não poderia criar entropias e prejudicar o normal funcionamento da rede que suporta toda a atividade do IPL e o seu negócio.

Devido a tal preocupação, procedeu-se à colocação do NGFW com os seus interfaces em modo TAP[33], garantindo assim que o equipamento apenas observava e adquiria dados sem conseguir controlar/atuar sobre o tráfego que por ele circulava.

A escolha do local para colocação dos sensores do equipamento foi outro dos desafios. Sendo que, a incapacidade para realizar testes em todas as zonas existentes, levou a que fosse eleito o segmento de acesso à Internet e o segmento interno que conecta a Escola Superior de Tecnologia de Leiria caracterizada pela sua dimensão, e, por ser uma escola de índole tecnológica. Além disso, é responsável por albergar a DMZ com as principais aplicações do IPL. O segmento de acesso à Internet permite a visibilidade de todo o tráfego que circula de e para a Internet de todos os Campus do IPL.

[30] Tecnologia de identificação de aplicações.
[31] Tecnologia que permite ter visibilidade da atividade dos utilizadores.
[32] Combinação em tempo real de mecanismos de prevenção de ameaças com base de dados de URL.
[33] Apenas observa os dados e recolhe informações. Este tipo de interface não consegue controlar o tráfego.

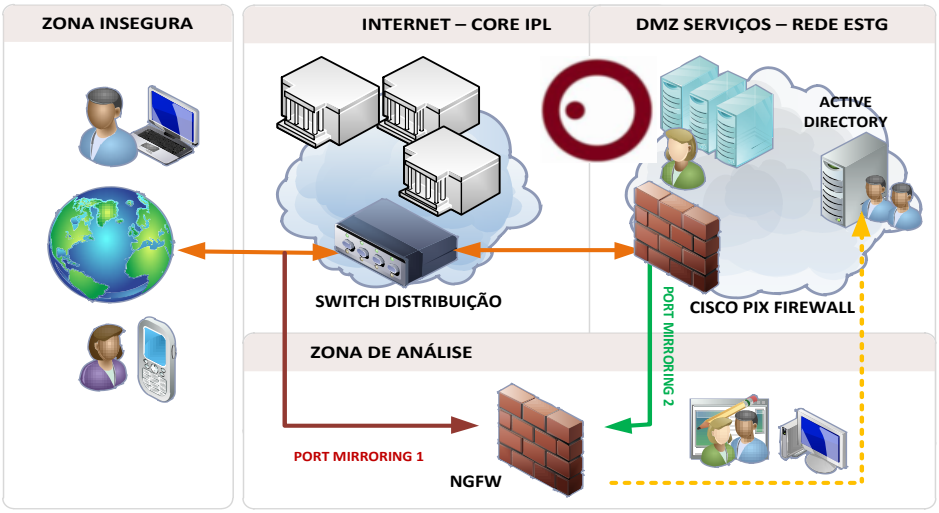

Figura 26 – Arquitetura de análise de risco de aplicações

Na Figura 26, é possível verificar a arquitetura de testes. O NGFW foi colocado em duas zonas diferenciadas, recebendo uma cópia de todo o tráfego que circula tanto no sentido de entrada como saída nas zonas elegidas. O envio da cópia do tráfego foi feito recorrendo a tecnologia *Port Mirroring*[34]. Todo o tráfego foi analisado posteriormente com as ferramentas de relatório e análise de tráfego e aplicações existentes no NGFW.

No relatório de análise são referidas, por diversas vezes, categorias e subcategorias de aplicações. A composição destes grupos de aplicações surgiu depois de um estudo aos centros de pesquisa[35] de aplicações e ameaças que os fabricantes Check Point, Fortinet e Palo Alto disponibilizam *online*. Cada fabricante agrupa as aplicações recorrendo aos seus critérios, sendo que, existem semelhanças na definição de algumas categorias. A Palo Alto apresenta um critério (Tabela 20) de organização mais simples e ajustado às necessidades do IPL utilizando subcategorias para cada categoria, simplificando assim a compreensão dos dados obtidos.

Categorias	Subcategorias
Business	Autentication services, Database, ERP, General Management, Office Programs, Software updates, Storage/backup
General Internet	File sharing, Internet utilities (web-browsing, toolbars,etc)
Collaboration	Email, Instant messaging, Internet conferencing, Social networking, Social business, VoIP/video, Web posting
Media	Audio streaming, Gaming, Photo/vídeo
Networking	Encrypted tunnel, Infrastructure, IP protocolo, Proxy, Remote access, Routing

Tabela 20 – Categorias e subcategorias de classificação de aplicações

[34] Tecnologia que permite "espelhar" o tráfego numa porta.
[35] Check Point - http://appwiki.checkpoint.com/appwikisdb/public.htm ; Fortinet - http://www.fortiguard.com/; Palo Alto - http://apps.paloaltonetworks.com/applipedia/

No que diz respeito à classificação das aplicações, o critério adotado seguiu a mesma linha de pensamento do usado na classificação das categorias, ou seja seguir os critérios dos fabricantes. As aplicações são classificadas com base nas seguintes características comportamentais:

- Capacidade de transferir ficheiros de uma rede para outra;
- Capacidade para propagar *malware;*
- Consumir 1 Mbps ou mais (acima do uso normal);
- Evitar a deteção usando um porto ou protocolo para algo diferente do seu propósito;
- Excessiva utilização;
- Com vulnerabilidades conhecidas;
- Passível de mau uso ou facilmente configuradas para expor mais do que o pretendido;
- Capacidade para criar túneis para outras aplicações.

4.3.2 - Riscos Introduzidos por Aplicações de Risco Elevado

Os potenciais riscos que podem advir do uso de determinadas aplicações que navegam nas redes podem ser determinados pelas características comportamentais das aplicações de alto risco (classificadas de 4 ou 5 numa escala de 1 a 5).

Cada uma das características comportamentais das aplicações pode introduzir risco na organização. Aplicações de transferência de ficheiros podem levar a perda de dados confidenciais; aplicações com a capacidade de evitar a deteção ou aplicações de túneis podem levar a riscos de conformidade; aumento de largura de banda implica o aumento de custos operacionais; aplicações propensas a *malware* ou que apresentam diversas vulnerabilidades podem representar riscos na continuidade do negócio da organização.

A identificação dos riscos inerentes às aplicações é o primeiro passo para a gestão eficaz dos riscos da organização.

Na Figura 27 apresenta-se um resumo do cálculo de risco do IPL com base no top das aplicações de risco elevado. O Apêndice A possui a descrição completa do risco.

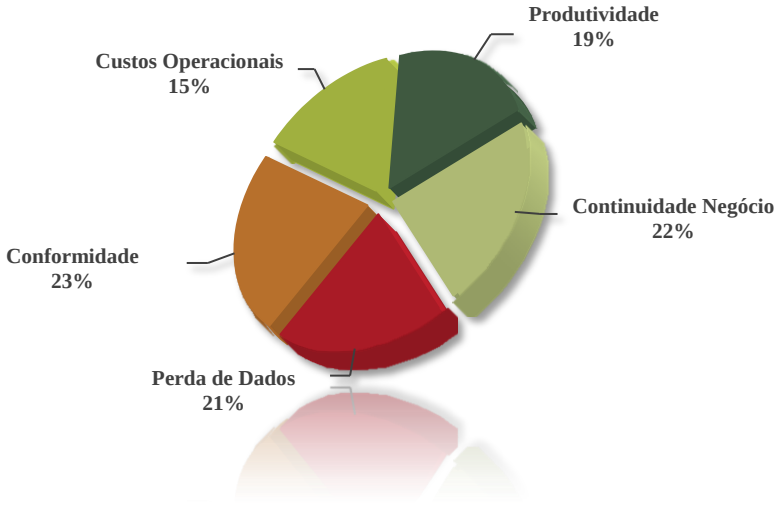

Figura 27 - Top das aplicações de alto risco

Na análise da Figura 27 constata-se que existe equidade na distribuição dos diferentes tipos de riscos provenientes de aplicações com risco elevado. O IPL encontra-se exposto, de forma considerável, a riscos de continuidade de negócio, perda de dados e conformidade.

4.3.3 - Top das Aplicações de Risco em Uso

A capacidade de utilizar mecanismos de segurança que permitam visualizar as aplicações que circulam na rede agrupando-as por categoria, subcategoria e tecnologia, é bastante profícua quando se discute o valor do negócio da organização e os potenciais riscos que as aplicações possuem para os utilizadores ou grupos de utilizadores.

Abaixo segue a lista das aplicações de risco elevado (classificação 4 ou 5) que, por serem consideradas relevantes ou apresentarem resultados surpreendentes, são alvo de um estudo mais aprofundado. Os dados encontram-se agrupados por categoria, subcategoria e por bytes consumidos. Todas as aplicações de risco elevado visíveis na rede do IPL encontram-se no Apêndice A para consulta.

RISCO	APLICAÇÕES	CATEGORIA	SUBCATEGORIA	TECNOLOGIA	BYTES	SESSÕES
5	google-docs	business-systems	office-programs	browser-based	3,579,407,837	58,939
5	Smtp	collaboration	email	client-server	69,279,075,864	1,758,261
5	Skype	collaboration	voip-video	peer-to-peer	47,139,429,216	168,687
5	Fileserve	general-internet	file-sharing	browser-based	214,062,638,751	38,622
5	Bittorrent	general-internet	file-sharing	peer-to-peer	136,116,957,326	1,180,640
5	Filesonic	general-internet	file-sharing	browser-based	119,524,903,477	46,196
5	ftp	general-internet	file-sharing	client-server	27,841,753,171	39,547
5	Hotfile	general-internet	file-sharing	browser-based	20,735,633,362	7,97
5	Emule	general-internet	file-sharing	peer-to-peer	8,480,824,430	422,95
5	msn-file-transfer	general-internet	file-sharing	peer-to-peer	1,619,724,625	2,255
5	qq-file-transfer	general-internet	file-sharing	client-server	167,691,585	655
5	Rss	general-internet	internet-utility	client-server	3,749,070,660	144,251
5	http-audio	Media	audio-streaming	browser-based	163,069,180,090	84,43
5	Youtube	Media	photo-video	browser-based	1,536,454,169,431	242,565
5	http-video	Media	photo-video	browser-based	114,272,840,208	34,076
5	Vimeo	Media	photo-video	browser-based	41,167,729,084	24,693
5	asf-streaming	Media	photo-video	browser-based	37,548,298,808	2,946
5	Freenet	networking	encrypted-tunnel	peer-to-peer	801,603,349	35,841
5	Hamachi	networking	encrypted-tunnel	peer-to-peer	225,758,087	1,306
5	http-proxy	networking	proxy	browser-based	9,033,255,783	344,43
5	Logmein	networking	remote-access	client-server	933,645,859	7,499
5	Vnc	networking	remote-access	client-server	778,176,180	19
5	vnc-http	networking	remote-access	browser-based	149,488	4

Tabela 21 - Aplicações descobertas com risco elevado 5

Ao observar a Tabela 21, sobressai o número de aplicações que são caracterizadas pelo **excessivo consumo de largura de banda**. No caso particular do IPL, os valores da aplicação ***youtube*** são surpreendentes, revelando consumos na ordem dos 1.3 ***terabytes*** relativos apenas uma semana de análise. A subcategoria "partilha de ficheiros" revela valores exagerados de tráfego consumido.

RISCO	APLICAÇÕES	CATEGORIA	SUBCATEGORIA	TECNOLOGIA	BYTES	SESSÕES
4	ms-update	business-systems	software-update	client-server	74,635,069,965	162,132
4	adobe-update	business-systems	software-update	client-server	59,968,807,902	13,467
4	Gmail	Collaboration	Email	browser-based	52,170,596,767	459,209
4	Hotmail	Collaboration	Email	browser-based	25,342,560,585	341,01
4	ms-exchange	Collaboration	Email	client-server	16,403,872,960	42,135
4	pop3	Collaboration	Email	client-server	3,155,565,694	371,081
4	Imap	Collaboration	Email	client-server	782,864,800	94,462
4	qq-mail	Collaboration	Email	browser-based	90,852,901	6,065
4	mail.ru	Collaboration	Email	browser-based	4,294,310	21
4	msn	Collaboration	instant-messaging	client-server	6,542,267,779	306,142
4	Aim	Collaboration	instant-messaging	client-server	1,548,302,574	1,770,827
4	google-talk	Collaboration	instant-messaging	client-server	442,996,473	19,13
4	Qq	Collaboration	instant-messaging	client-server	264,552,985	39,139
4	Facebook	Collaboration	social-networking	browser-based	39,913,816,998	1,507,163
4	Vkontakte	Collaboration	social-networking	browser-based	4,056,229,882	44,446
4	facebook-posting	Collaboration	social-networking	browser-based	3,514,507,820	45,422
4	facebook-apps	Collaboration	social-networking	browser-based	780,718,080	38,356
4	Myspace	Collaboration	social-networking	browser-based	313,271,347	7,927
4	msn-voice	Collaboration	voip-video	peer-to-peer	18,389,699,265	55,582
4	Sip	Collaboration	voip-video	peer-to-peer	369,359,344	41,915
4	Megaupload	general-internet	file-sharing	browser-based	818,722,280,108	35,175
4	Dropbox	general-internet	file-sharing	browser-based	231,525,962,875	637,37
4	Mediafire	general-internet	file-sharing	browser-based	42,223,018,290	10,137
4	Rapidshare	general-internet	file-sharing	browser-based	19,904,075,144	4,877
4	Sugarsync	general-internet	file-sharing	client-server	13,153,515,127	2,264
4	4shared	general-internet	file-sharing	browser-based	10,622,837,987	12,133
4	easy-share	general-internet	file-sharing	browser-based	9,548,543,535	789
4	qq-download	general-internet	file-sharing	peer-to-peer	7,001,042,479	559,001
4	Itunes	Media	audio-streaming	client-server	22,439,500,511	18,525
4	Rtmp	Media	photo-video	browser-based	228,719,620,271	26,455
4	Ppstream	Media	photo-video	peer-to-peer	157,601,979,229	2,824,029
4	Rtmpe	Media	photo-video	browser-based	33,760,313,621	3,77
4	Rtmpt	Media	photo-video	browser-based	20,543,377,245	2,020,359
4	Qvod	Media	photo-video	peer-to-peer	10,347,021,181	119,004
4	Dailymotion	Media	photo-video	browser-based	6,923,488,627	7,561
4	Qqlive	Media	photo-video	peer-to-peer	6,092,184,138	363,803
4	Ssl	Networking	encrypted-tunnel	browser-based	299,954,000,194	5,862,341
4	Ssh	Networking	encrypted-tunnel	client-server	15,870,767,807	475,783
4	Tor	Networking	encrypted-tunnel	client-server	8,543,619,566	1,139
4	Dns	Networking	Infrastructure	network-protocol	10,594,823,845	32,342,894

Tabela 22 - Aplicações descobertas com risco elevado 4

Nas aplicações com **risco elevado 4 (**Tabela 22**)**, é evidente a presença de aplicações da subcategoria "transferência de ficheiros" que além de serem caracterizadas pelo excessivo consumo de largura de banda, são evasivas, apresentam vulnerabilidades e são usadas frequentemente. Outro dado curioso é a existência de aplicações que são populares na China como é o caso do *qq, Qqlive, qq-download*, mostrando assim que a população Chinesa do IPL já possui algum peso. Aplicações de origem Russa também se encontram presentes (*vkontakte e mail.ru*).

Principais observações sobre as 193 aplicações descobertas de risco elevado (apêndice a)

Na generalidade e analisando todas as aplicações detectadas de risco elevado, o quadro do IPL poderá ser pintado da seguinte forma:

1. **Ocultação de Atividade**
   Foram detectadas aplicações de *Proxy* (13) e acesso remoto (6). Em adição, aplicações que não são VPN mas que utilizam túneis encriptados. Utilizadores experientes de IT recorrem com uma frequência cada vez maior a este tipo de aplicações com a intenção de ocultar/disfarçar a sua atividade e o que estão a fazer. Esta atividade pode expor o IPL a riscos de perda de dados e que exista atividade que não esteja em conformidade com a política de segurança.

2. **Transferência de Ficheiros/ Perda de Dados/ Violação de direitos de autor**
   Detectadas diversas aplicações P2P (36) e aplicações de partilha de ficheiros via *web* (24). Estas aplicações expõem o IPL a perda de dados, possíveis violações de privacidade e podem significar um veículo de ameaça.

3. **Comunicações pessoais**
   Foi encontrada uma variedade de aplicações que normalmente são usadas para comunicações pessoais, onde estão incluídas as de mensagens instantâneas (15), *webmail* (13) e conferência através de VoIP/vídeo (7). Este tipo de aplicações expõe o IPL a possíveis perdas de produtividade e risco de continuidade de negócio.

4. ***Bandwith hogging***
   Foram detectadas aplicações que são conhecidas por consumo excessivo de largura de banda incluindo fotos/vídeo (32), áudio (5) e redes sociais (13). Este tipo de aplicações, além de representarem redução drástica na produtividade dos funcionários, consome excessiva largura de banda.

4.3.4 - Características das Aplicações que Determinam Risco

Com o conhecimento das aplicações que percorrem a rede, as suas características individuais e quem as utiliza, os administradores ficam habilitados a decidir como tratar o tráfego das aplicações através de políticas de segurança associadas. Note-se que muitas aplicações transportam múltiplas características comportamentais.

Definições das Características Comportamentais das Aplicações:

- **Propensas a uso indevido,** usadas para propósitos prejudiciais ou facilmente configuradas para expor mais do que o pretendido. Inclui aplicações tipo *BiTorrent* ou *AppleJuice;*
- **Túneis ou outras aplicações,** possuem a capacidade de transportar outras aplicações e das "esconder". Inclui SSH, SSL, Hopster, TOR e RTSP;
- **Conhecidas pelas vulnerabilidades,** aplicações que possuem vulnerabilidades conhecidas. Tipicamente *exploits*;
- **Transferência de ficheiros,** capacidade para transferir ficheiros de uma rede para outra. Incluem FTP e P2P, aplicações de partilha de ficheiros *online* tais como *MegaUpload* e *YouSendIt*;
- **Usadas por *malware*,** utilizadas por propagar *malware*, iniciar um ataque ou propagar dados. Estas aplicações incluem colaboração (correio electrónico, IM) e categorias gerais de internet (partilha de ficheiros, …);
- **Consumo de largura de banda**, aplicações que consomem 1Mbps ou mais. Incluem aplicações de P2P como *Xunlei* e *DirectConnect* assim como aplicações de vídeo/áudio, atualizações de *software* e outras aplicações;
- **Evasivas,** usam uma porta ou um protocolo para outro fim, com objetivo de ludibriar mecanismos de segurança.

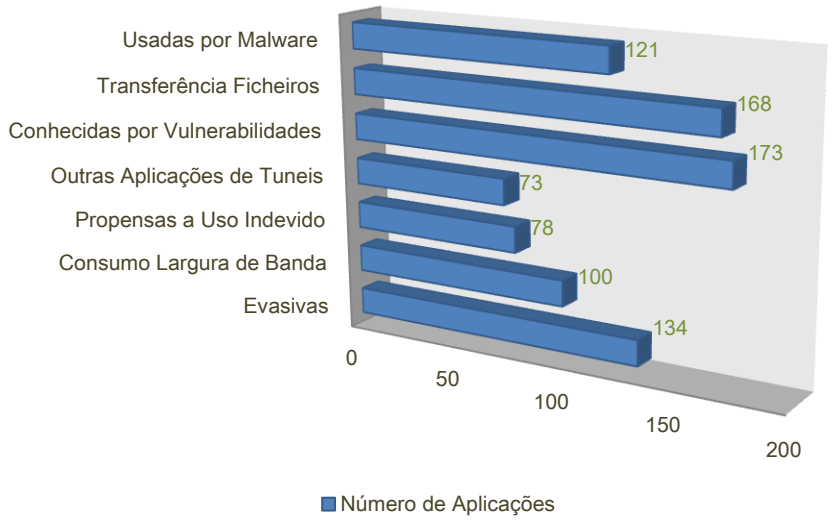

Figura 28 - Características comportamentais das aplicações de alto risco detectadas

4.3.5 - Top das Aplicações que Percorrem a Rede

O top de aplicações com base no consumo de largura de banda é constituído por 35 aplicações diferenciadas, classificadas por categoria e subcategoria, é apresentado na Tabela 23.

Risco	Aplicações	Categoria	Subcategoria	Tecnologia	Bytes	Sessões
3	Snmp	business-systems	management	client-server	32,801,800,439	2,927,978
4	ms-update	business-systems	software-update	client-server	74,635,069,965	162,132
4	adobe-update	business-systems	software-update	client-server	59,968,807,902	13,467
2	360-safeguard	business-systems	software-update	client-server	29,896,633,728	656,185
3	ms-ds-smb	business-systems	storage-backup	client-server	212,412,900,804	364,733
3	rsync	business-systems	storage-backup	client-server	115,834,742,337	150
5	smtp	Collaboration	email	client-server	69,279,075,864	1,758,261
4	gmail	Collaboration	email	browser-based	52,170,596,767	459,209
4	hotmail	Collaboration	email	browser-based	25,342,560,585	341,01
4	facebook	Collaboration	social-networking	browser-based	39,913,816,998	1,507,163
5	skype	Collaboration	voip-video	peer-to-peer	47,139,429,216	168,687
4	megaupload	general-internet	file-sharing	browser-based	818,722,280,108	35,175
4	dropbox	general-internet	file-sharing	browser-based	231,525,962,875	637,37
5	fileserve	general-internet	file-sharing	browser-based	214,062,638,751	38,622
5	bittorrent	general-internet	file-sharing	peer-to-peer	136,116,957,326	1,180,640
5	filesonic	general-internet	file-sharing	browser-based	119,524,903,477	46,196
4	mediafire	general-internet	file-sharing	browser-based	42,223,018,290	10,137
3	netload	general-internet	file-sharing	browser-based	41,162,941,180	700
5	ftp	general-internet	file-sharing	client-server	27,841,753,171	39,547
4	web-browsing	general-internet	internet-utility	browser-based	2,021,951,096,562	46,259,483
4	flash	general-internet	internet-utility	browser-based	295,627,915,602	865,729
5	http-audio	Media	audio-streaming	browser-based	163,069,180,090	84,43
4	itunes	Media	audio-streaming	client-server	22,439,500,511	18,525
3	steam	Media	gaming	client-server	25,364,373,551	15,429
2	zynga-games	Media	gaming	browser-based	22,075,427,369	326,186
5	youtube	Media	photo-video	browser-based	1,536,454,169,431	242,565
4	rtmp	Media	photo-video	browser-based	228,719,620,271	26,455
4	ppstream	Media	photo-video	peer-to-peer	157,601,979,229	2,824,029
5	http-video	Media	photo-video	browser-based	114,272,840,208	34,076
5	vimeo	Media	photo-video	browser-based	41,167,729,084	24,693
5	asf-streaming	Media	photo-video	browser-based	37,548,298,808	2,946
4	rtmpe	Media	photo-video	browser-based	33,760,313,621	3,77
3	megavideo	Media	photo-video	browser-based	24,095,375,210	5,206
4	ssl	Networking	encrypted-tunnel	browser-based	299,954,000,194	5,862,341
3	hotspot-shield	Networking	encrypted-tunnel	client-server	22,531,065,996	475

Tabela 23 - Top de aplicações que consumem largura de banda

*Foram detetadas cerca de **600** aplicações na rede do IPL, sendo que, da observação das **35** mais usadas conclui-se que o tipo mais comum de aplicações são foto-vídeo e partilha de ficheiros.*

4.3.5.1 - Subcategoria das Aplicações

O agrupamento por categoria das aplicações detetadas (Tabela 24), com a classificação por consumo de largura de banda, permite saber onde o uso da aplicação é mais intensivo e qual a categoria que possui maior impacto na largura de banda. Estes dados além de auxiliarem na priorização das aplicações tornam o processo mais eficaz.

Subcategoria	Num. Aplicações	Bytes	Sessões
internet-utility	31	2,390,065,807,021	61,609,414
photo-video	59	2,290,919,946,131	5,901,351
file-sharing	64	1,754,820,037,196	4,639,944
encrypted-tunnel	14	364,293,085,534	6,378,798
storage-backup	7	329,004,921,603	365,752
audio-streaming	17	197,118,866,795	112,768
software-update	14	176,764,976,003	940,31
email	23	172,259,656,823	3,269,618
voip-video	21	70,721,021,969	2,762,841
social-networking	41	65,448,909,371	2,553,297
management	15	54,676,771,683	3,204,314
gaming	24	50,971,347,523	454,684
instant-messaging	44	32,153,176,325	3,205,283
social-business	3	14,665,445,548	141,914
infrastructure	18	12,295,249,331	32,992,175
proxy	13	9,214,925,137	349,438
general-business	14	8,350,000,090	1,784,535
remote-access	11	5,945,538,351	46,025
office-programs	7	3,846,017,541	70,571
auth-service	6	1,731,749,033	222,997
database	8	1,511,343,154	186,829
routing	14	1,388,837,941	23,76
web-posting	5	407,586,663	9,753
ip-protocol	116	44,349,381	104,093
internet-conferencing	8	11,426,686	116
erp-crm	3	4,175,623	2,226

Tabela 24 - Subcategorias de todas as aplicações encontradas

As subcategorias das aplicações que consomem maior largura de banda são: internet-utility, photo-video e file-sharing.

4.3.6 - Aplicações que Utilizam HTTP

Foi realizada a análise do top 25 de aplicações (Tabela 25), com base no consumo de largura de banda e que, de algum meio, utilizam HTTP. Muitas das aplicações organizacionais são baseadas em HTTP como forma de aumentar a velocidade de desenvolvimento e simplificar o acesso. No entanto existem aplicações que o utilizam para contornar a segurança. Saber dentro de uma organização quais são as aplicações que utilizam HTTP é um ponto crucial para elaborar uma política de habilitação de aplicações.

Risco	Aplicações HTTP	Tecnologia	Bytes	Sessões
4	web-browsing	browser-based	2,021,951,096,562	46,259,483
5	youtube	browser-based	1,536,454,169,431	242,565
4	megaupload	browser-based	818,722,280,108	35,175
4	flash	browser-based	295,627,915,602	865,729
4	dropbox	browser-based	231,525,962,875	637,37
5	fileserve	browser-based	214,062,638,751	38,622
5	http-audio	browser-based	163,069,180,090	84,43
4	ppstream	peer-to-peer	157,601,979,229	2,824,029
5	bittorrent	peer-to-peer	136,116,957,326	1,180,640
5	filesonic	browser-based	119,524,903,477	46,196
5	http-video	browser-based	114,272,840,208	34,076
4	ms-update	client-server	74,635,069,965	162,132
4	adobe-update	client-server	59,968,807,902	13,467
4	gmail	browser-based	52,170,596,767	459,209
4	mediafire	browser-based	42,223,018,290	10,137
5	vimeo	browser-based	41,167,729,084	24,693
3	netload	browser-based	41,162,941,180	700
4	facebook	browser-based	39,913,816,998	1,507,163
5	asf-streaming	browser-based	37,548,298,808	2,946
2	360-safeguard-update	client-server	29,896,633,728	656,185
3	steam	client-server	25,364,373,551	15,429
4	hotmail	browser-based	25,342,560,585	341,01
3	megavideo	browser-based	24,095,375,210	5,206
3	hotspot-shield	client-server	22,531,065,996	475
4	itunes	client-server	22,439,500,511	18,525

Tabela 25 - Top de aplicações HTTP identificadas

Na análise dos dados recolhidos e analisando o top 25 de 370 aplicações suportadas por HTTP detetadas no IPL, pode-se concluir que circulam pela rede do IPL um misto de aplicações de trabalho e não relacionadas com trabalho, baseadas de uma forma ou de outra em HTTP.

4.3.7 - Principais Categorias de URLs

Outro aspecto a considerar sobre a visibilidade do tráfego das aplicações é a identificação e o posterior controlo dos *websites* que são visitados pelos utilizadores. A filtragem de URL, combinada com o controlo de aplicações e prevenção de ameaças pode melhorar drasticamente a segurança da rede e aumentar a produtividade na organização.

	Categoria URL	Contagem
1	social-networking	7,297,895
2	search-engines	3,938,177
3	educational-institutions	3,664,837
4	unknown	3,535,538
5	computer-and-internet-	2,886,153
6	business-and-economy	1,878,774
7	internet-portals	1,750,468
8	news-and-media	1,529,551
9	online-personal-storage	1,311,222
10	web-advertisements	1,162,480
11	content-delivery-networks	932,805
12	games	884,529
13	personal-sites-and-blogs	847,276
14	streaming-media	703,308
15	parked-domains	674,385
16	shopping	630,231
17	web-based-email	601,208
18	sports	582,481
19	internet-communications	524,332
20	private-ip-addresses	350,41
21	entertainment-and-arts	319,544
22	travel	315,724
23	shareware-and-freeware	297,48
24	reference-and-research	268,514
25	society	259,128

Tabela 26 - Top categorias de URL visitadas

O top 25 de categorias de URLs mais visitadas apresentado na Tabela 26, é constituído por uma maioria de URLs relacionados com atividade extra trabalho. A categoria "redes sociais" surge destacada somando mais visitas que as duas categorias posteriores.

4.3.8 - Principais Ameaças Presentes na Rede

O aumento de visibilidade no tráfego que flui através da rede, além de identificar o par protocolo/porta das aplicações, ajuda a melhorar a prevenção de ameaças através da determinação exata das aplicações, que poderão ser responsáveis pela sua transmissão. Este aumento de visibilidade na identificação de aplicações, significa que o motor de prevenção de

ameaças existente nos NGFW ou UTMs poderá reduzir rapidamente o número de potenciais ameaças e aumentar o desempenho na deteção.

Nome da Ameaça	Tipo	Gravidade	Incidentes
MSSQL Login failed for user 'sa' execution	vulnerability	medium	168,12
Win32.Conficker.C p2p	spyware phone home	critical	32,619
Generic2 User-Agent Traffic	spyware phone home	medium	7,828
HTTP SQL Injection Attempt	vulnerability	medium	4,989
Alueron Command and Control Traffic	spyware phone home	critical	1,849
ClamAV libclamav PE File Handling Integer Overflow Vulnerability	vulnerability	high	807
ShopperReports Track/Upgrade/Report activities	spyware phone home	medium	472
Buzus.Gen Command and Control Traffic	spyware phone home	critical	417
PHP Remote File Include Vulnerability	vulnerability	medium	315
Bot: Gozi Phone phone activity	spyware phone home	critical	266
Trend Micro OfficeScan Server cgiRecvFile Buffer Overflow	vulnerability	critical	199
Squid HTTP Version Number Parsing Denial of Service	vulnerability	medium	152
Download_Accelerator_Plus DAP ads	spyware phone home	low	116
AutoIt.Gen Backdoor Traffic	spyware phone home	high	115
Microsoft Agent ActiveX Control Buffer Overflow Vulnerability	vulnerability	high	107
Microsoft SQL Server Stack Overflow Vulnerability	vulnerability	critical	96
Hiloti.Gen Command and Control Traffic	spyware phone home	high	90
ShopperReports Services requests	spyware phone home	medium	74
Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	Vulnerability	critical	70
Macdefender Command and Control Traffic	spyware phone home	critical	54
HTTP SQL Injection Attempt	Vulnerability	medium	43
Microsoft ASP.NET Path Validation Security Bypass Vulnerability	Vulnerability	medium	41
Virus/Win32.mabezatgen.a	Vírus	medium	40
SCN_Toolbar Hijacks IE auto searches and error pages	spyware phone home	medium	36
HTTP SQL Injection Attempt	vulnerability	medium	34

Tabela 27 - Principais ameaças identificadas, ordenadas pelo número de incidentes

Das 111 ameaças detetadas, a distribuição da criticidade é feita da seguinte forma: Ameaças criticas 18%; Ameaças elevadas 19% e 23% de ameaças médias. As restantes ameaças possuem classificação de baixa ou então são apenas de informação.

4.3.9 - Utilização de Aplicações por Categoria e Tecnologia

O consumo de recursos (sessões e bytes) das aplicações com base na tecnologia subjacente e sua subcategoria são mostrados nos gráficos abaixo. Esta informação complementa a granularidade dos dados sobre as aplicações e ameaças, de forma a apresentar uma síntese mais completa dos tipos de aplicações com base na subcategoria e na tecnologia subjacente em uso.

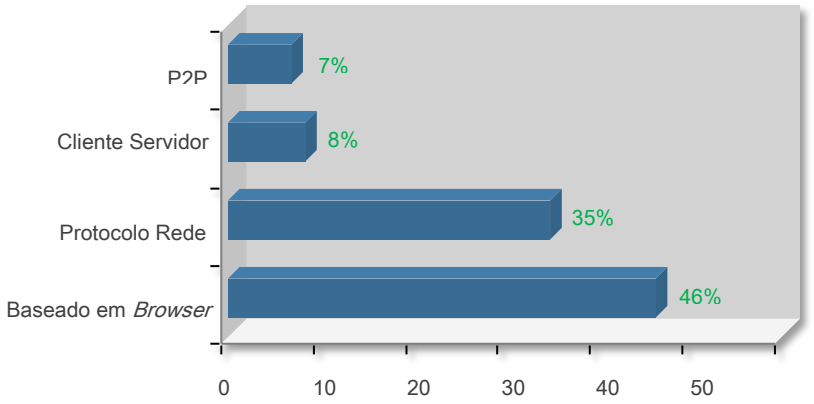

Figura 29 - Consumo de sessões em percentagem por tecnologia (aplicações)

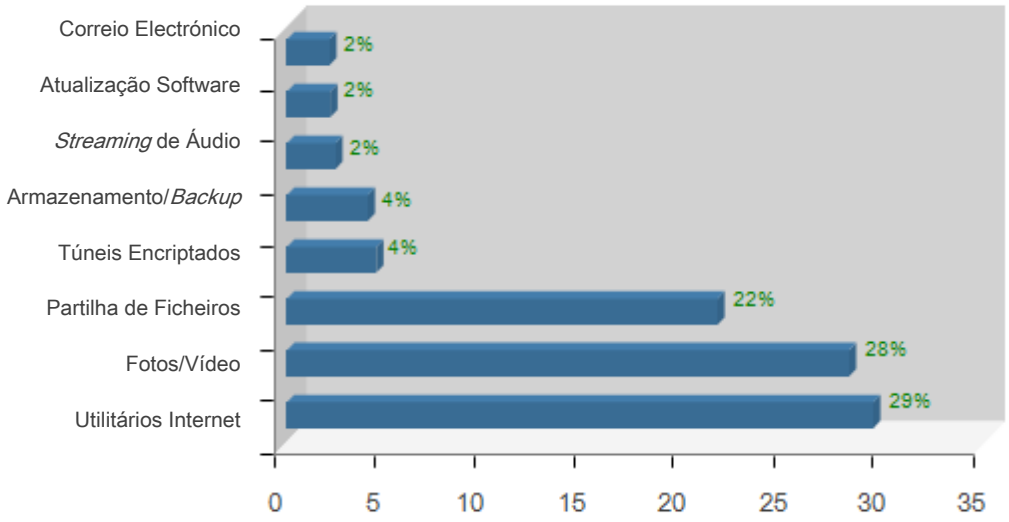

Figura 30 - Consumo de bytes em percentagem por tecnologia (aplicações)

Com os dados recolhidos, é possível observar (Figura 29) que as aplicações baseadas em *browser*, são responsáveis pelo consumo de 46% das sessões existentes no IPL. No que diz respeito às aplicações por categoria (Figura 30), a categoria de utilitários internet (internet-utility) absorve cerca de 29% da largura de banda.

4.3.10 - Ameaças Encontradas

Durante a análise ao ambiente de rede do IPL, caracterizado como de relativamente aberto e sem a presença de mecanismos que permitam "ver" que aplicações percorrem a rede, o que expõe a organização a um largo conjunto de riscos de segurança, foram descobertos os seguintes:

- **Aplicações para ocultação de atividade -** Detetada elevada atividade deste tipo de aplicações na rede do IPL. Utilizadores experientes estão a esconder a sua atividade e a fazer *bypass* aos mecanismos de segurança implementados;
- **P2P e aplicações *online* de transferência de ficheiros -** Da análise, salta à vista a utilização intensiva na rede do IPL de diversas aplicações desta categoria. Os riscos de segurança inerentes à sua utilização são a perda de dados e violação de direitos de autor. O consumo avultado de largura de banda que este tipo de aplicações regista é outro dos problemas detetados, prejudicando claramente a utilização da rede de dados para fins académicos;
- **Entretenimento e redes sociais -** Aplicações que são usadas para entretenimento e socialização (meios de comunicação, rede, áudio social) foram encontradas na rede. Essas aplicações apresentam o desafio de como equilibrar o uso deste tipo de aplicações sem ameaçar a produtividade, a exposição a ameaças, conformidade e os riscos de perda de dados. Na maioria dos casos a sua utilização não é efetuada em contexto de trabalho, excepto em utilizadores que têm a seu cargo a tarefa de gestão das redes sociais da Instituição;
- ***Webmail*, Mensageiros e VoIP –** Diversos exemplos deste tipo de aplicações foram encontrados na rede. Muitos desses aplicativos podem facilmente contornar *firewalls* e funcionar como vectores de ameaça, além de permitirem a perda de dados.

4.3.11 - Recomendações

Com base nos resultados obtidos do relatório de análise de segurança surgem algumas recomendações com objetivo de minimizar os riscos encontrados e aumentar o desempenho da rede do IPL.

1. **Implementar políticas de uso apropriado para aplicações e navegação *web***

   Como a maioria das instituições, o IPL carece de uma política refinada para reger o uso de aplicações. Com o crescimento das aplicações controladas pelo utilizador, a sua tendência é possuírem características evasivas e as ameaças tirarem partido destas, sendo recomendado a criação de políticas de uso apropriado por aplicação ou categoria de aplicações.

2. **Reconhecer as áreas de alto risco (P2P, Partilha/transferência de ficheiros *online,..)***

   Os riscos associados a estes aplicativos podem apresentar problemas para o IPL, assim como aos funcionários que utilizam estas aplicações para contornar os mecanismos de segurança tradicionais. Sem entender, categorizar e mitigar o risco nessas áreas, o IPL expõe-se a possível transferência de dados não autorizados, bem como às ameaças associadas ao nível de aplicação.

3. **Implementar políticas ditando uso de aplicações de acesso remoto e *Proxies***

   Estas aplicações são muitas vezes utilizadas pelos funcionários para ocultação de atividade ilícita ou para acesso remoto a máquinas e sistemas externos. Possuem a

particularidade de permitir ultrapassar as barreiras de segurança tradicionais, de possuírem diversas ameaças associadas e de diminuírem a produtividade dos funcionários. Com objetivo de salvaguardar os seus interesses, o IPL deve implementar políticas ditando o uso deste tipo de aplicações e em que condições. Uma das opções possíveis é ditar quais grupos podem usar um determinado *proxy* ou aplicação de acesso remoto, bloqueando os restantes.

4. **Controlar as redes sociais e aplicações de entretenimento**

   As redes sociais são uma das maiores causas de perda de produtividade nas organizações. O seu controlo é um assunto que deve ser olhado com cuidado e preocupação, sendo que as medidas a aplicar poderão ser consideradas de abusivas por parte de alguns utilizadores e funcionar como factor desmotivador noutros. A definição de horários específicos de permissão para utilização deste tipo de ferramentas ou a aplicação de regras de QoS nestas aplicações poderão ser algumas opções viáveis.

5. **Procurar Visibilidade e Controle de Aplicativos**

   A única forma de reduzir o risco nas aplicações é, em primeiro lugar, ter visibilidade do tráfego de aplicações existente na rede para em seguida o compreender e posteriormente ser capaz de criar e impor políticas que o rejam. Para combater os problemas de segurança no IPL será necessário proceder a criação de políticas de utilização de aplicações, e à instalação de um NGFW com objetivo de assegurar a visibilidade, o tráfego de aplicações e garantir que a rede está sendo usada de acordo com as prioridades da organização.

Esta página foi intencionalmente deixada em branco

5 - Proposta de Arquitetura de Segurança

O ambiente de rede nas universidades apresenta um conjunto ímpar de desafios de segurança. Por norma, uma universidade é constituída por dezenas de departamentos, milhares de funcionários e dezenas de milhares de alunos. A sua infraestrutura pode ser formada por milhares de dispositivos sem qualquer tipo de proteção, ou então, com mecanismos de segurança desapropriados.

A rápida proliferação de *botnets*, a sofisticação dos ataques, o crescimento alarmante do crime organizado e espionagem através da internet, o roubo de dados e identidade, são algumas das novas formas de ameaças que despontaram nos últimos anos e ao qual as ferramentas de segurança tradicionais não conseguem dar resposta.

Se noutros tipos de organizações este género de ameaças são bastante problemáticas, representando uma variável de risco bastante elevada para o seu negócio, nos meios académicos a sua criticidade é superior. Este aumento deve-se à relação balanceada entre ataques com origem externa e origem interna.

Se a uma rede de grande dimensão, inserida num ambiente aberto e com características peculiares juntarmos a combinação dos novos desafios de segurança com as diversas origens de ameaças, temos com certeza um desafio de segurança complexo, ambicioso e em constante mutação.

Neste capítulo, será apresentada a proposta arquitetura de segurança para o IPL, tendo em conta os novos desafios, as necessidades do IPL, a análise e recomendações de segurança efetuada no capítulo anterior à arquitetura e mecanismos de segurança em funcionamento.

A arquitetura foi desenhada tendo a segurança como elemento integrado com objetivo de garantir a confidencialidade, integridade e disponibilidade dos dados e recursos dos sistemas.

Adicionalmente à apresentação da arquitetura serão enumerados alguns cuidados a ter na sua implementação e apresentado um plano de ação para a sua implementação.

5.1 - Arquitetura de Segurança

O modelo proposto de arquitetura de segurança foi estudado e desenhado tendo por base as melhores práticas de segurança. A arquitetura Cisco SAFE, assim como as suas recomendações, tiveram um papel preponderante neste processo.

Um dos principais desafios foi o de abandonar a arquitetura descentralizada analisada no capítulo anterior, e desenhar uma que conseguisse responder à arquitetura de gestão centralizada que o IPL possui. Este desafio foi ainda acompanhado da necessidade de unificar os mecanismos de segurança e simultaneamente aumentar a visibilidade e o controlo de toda a infraestrutura. Aqui existiu a preocupação de seguir as seis ações de segurança recomendadas na *framework* SCF da cisco, que são:

Visibilidade

1. Identificar e classificar utilizadores, serviços, tráfego e dispositivos;
2. Monitorizar o desempenho, comportamentos, padrões de uso, eventos e sua conformidade com a política;
3. Recolher, analisar e correlacionar eventos do sistema;

Controlo

4. Dispositivos, serviços, servidores, aplicações e infraestrutura;
5. Isolar utilizadores, sistemas e serviços, quando necessário;
6. Impor controlos de acessos e políticas de segurança e mitigar os eventos de segurança.

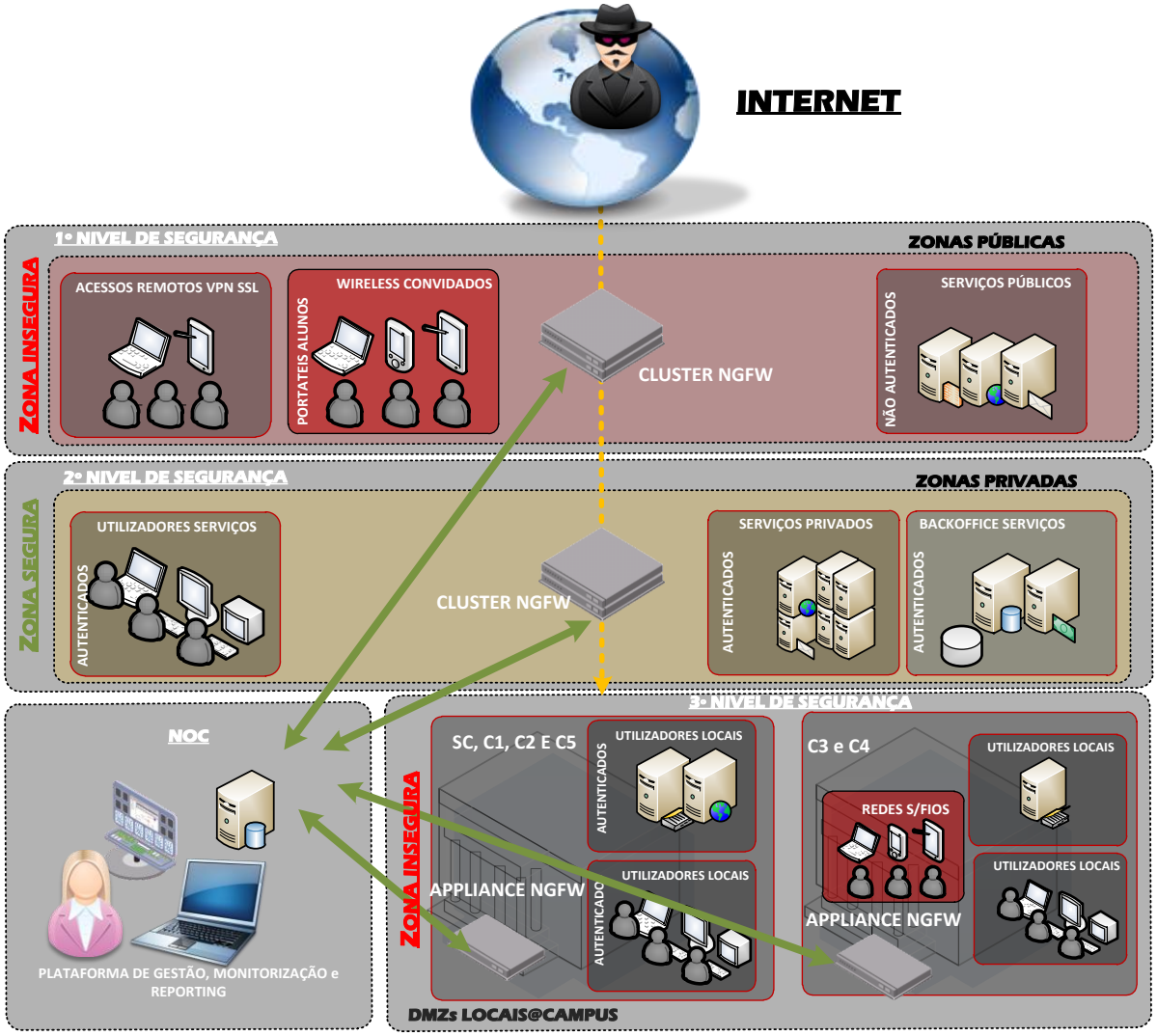

Figura 31 – Arquitetura de segurança proposta

Na Figura 31 encontra-se representada a proposta de arquitetura de segurança tendo em conta todos os desafios e necessidades. A arquitetura inclui 3 zonas de segurança com objetivo de responder aos diferentes perfis e características dos elementos que a compõem. A tecnologia escolhida para a implementação assenta em 2 clusters de *firewalls* da próxima geração (NGFWs) para os primeiros níveis de segurança e elementos individuais para as restantes zonas. Cada NGFW da arquitetura terá um conjunto de proteções que serão analisadas posteriormente. Esta tecnologia revela-se o grande elemento da arquitetura de segurança, passando por ela o controlo e visibilidade de todasa infraestrutura.

A arquitetura será analisada e descrita nos próximos itens tendo em conta as seguintes características:

- Zonas de segurança;
- Redundância;
- Desempenho;
- Mobilidade;
- Utilizadores remotos;
- Módulos e proteções;
- Funcionamento;
- Infraestrutura e Controlo de Acessos.

5.1.1 - Zonas de Segurança

Foram definidas 3 zonas de segurança (zona Internet, zona Intranet e zona Local). O princípio para a sua definição foi o de criar 3 níveis que representassem as necessidades da infraestrutura de TI, recorrendo aos conceitos de segurança de abordagem modular, segmentação e defesa em profundidade.

Estas zonas têm como objetivo albergar diferentes subzonas (DMZs) com perfis e necessidades distintas, respondendo aos desafios de segurança definidos e tendo em conta os diferentes tipos de utilizadores, serviços existentes, diversidade de dispositivos, mobilidade e novas ameaças.

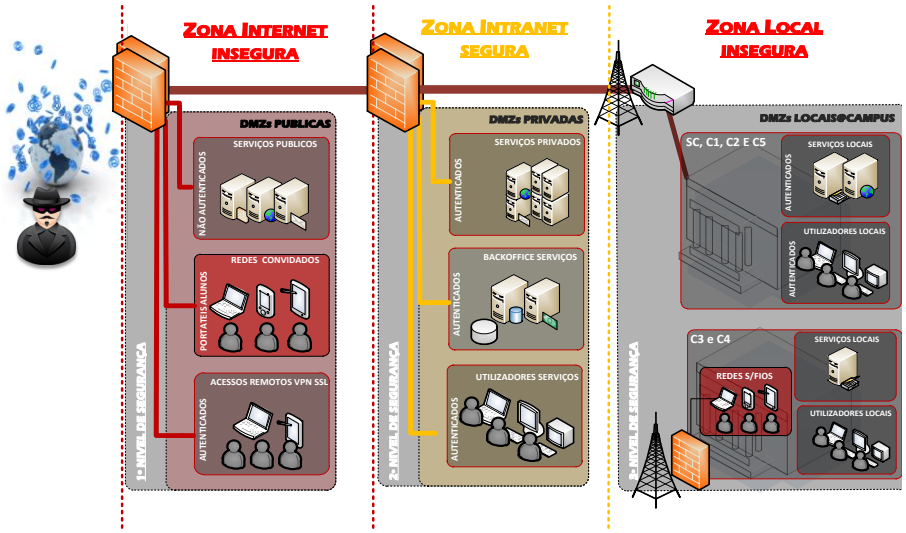

Figura 32 – Zonas de segurança

A flexibilidade que a arquitetura na Figura 32 apresenta, permite que dentro de cada zona/nível de segurança possa existir uma desmultiplicação, sendo possível aumentar o número de subzonas, se assim for necessário. Por questões de segurança e desempenho, optou-se por alojar os diferentes níveis de segurança em equipamentos exclusivos para o efeito, reforçando a segurança ao garantir a existência de 3 níveis de segurança físicos diferenciados.

Zona Internet

A zona Internet representa a primeira barreira de segurança, sendo caracterizada pelo elevado risco e insegurança a que se encontra exposta. A sua finalidade é a de alojar os serviços e utilizadores que pelas suas particularidades/características possuem uma maior exposição ao risco ou que de alguma forma representam ameaças.

Esta zona foi subdividida em 4 subzonas:

1. **Serviços públicos** – Subzona que inclui todos os serviços públicos que se encontram diretamente expostos na internet como por exemplo: DNS, *proxy¸radius* de topo, *relay* de correio eletrónico;
2. **Rede sem fios para convidados**: Inclui todos os utilizadores que são identificados como convidados do IPL. Abrange utilizadores em *roaming* do projeto eduroam e participantes de eventos que necessitem de ter acesso apenas a recursos externos;
3. **Rede sem fios para alunos**: Inclui utilizadores do tipo aluno que pertençam aos campus de Leiria e que façam uso dos seus próprios dispositivos ou utilizem salas de projeto, onde a gestão dos dispositivos não seja da responsabilidade dos serviços informáticos do IPL. Nesta zona, os utilizadores terão acesso a recursos internos de forma limitada. Utilizadores desta zona terão que se autenticar na infraestrutura do IPL;
4. **Acessos remotos**: Zona com objetivo de albergar os utilizadores que necessitam de ligar remotamente ao IPL. Esta zona é destinada a utilizadores autenticados na infraestrutura do IPL e possibilitará acesso remoto controlado aos serviços internos disponibilizados pelo IPL. O tipo de acesso será dado em função do perfil e necessidade do utilizador.

Zona Intranet

A segunda barreira de segurança ao qual foi atribuído o nome de DMZs privadas é caracterizada por alojar subzonas de maior segurança e consequentemente com menor risco. Estas subzonas contêm todos os serviços de suporte à atividade do IPL, ou seja, os serviços Intranet.

Tal como na zona anterior, foram definidas subzonas que apesar de serem consideradas privadas, possuem características dispares e como tal necessitam de ser isoladas. Por exemplo, serviços como gestão documental, gestão académica e colaboração, entre outros, farão parte da mesma subzona. No que diz respeito ao *backoffice* aplicacional de suporte aos *frontends* de alguns serviços, como é o caso da base de dados académica, administrativa e

financeira, este será hospedado numa subzona criada para o efeito e caracterizada de restrita. Outras das preocupações, foi a de dotar os utilizadores (RH, académicos, aprovisionamento e contabilidade) do qual a sua atividade depende quase exclusivamente destas aplicações, de melhores condições de segurança e desempenho. Como consequência, foi criada uma subzona transversal a todo o IPL.

Apesar de não se encontrar representada na Figura 32, está contemplada uma subzona destinada aos serviços alojados em tecnologia virtualizada.

Zona Local

Por fim, a zona local que tem a finalidade de suportar todos os serviços locais e exclusivos ao campus e seus utilizadores. Conforme nas zonas anteriores, aqui também existem diferentes subzonas destinadas a distintos tipos de utilizadores do campus (em função do seu tipo, perfil e dispositivo usado) e aos seus serviços, como é o caso de servidores de domínio e correio eletrónico.

Todos os utilizadores que sejam autenticados na infraestrutura do IPL, e que usem dispositivos controlados pelos serviços informáticos, serão sempre colocados na zona que corresponde ao seu perfil no campus a que pertencem. A confiança nestes dispositivos permite recorrer a esta abordagem, que evita as barreiras de segurança estabelecidas nos níveis anteriores no acesso a recursos locais do campus.

Polos Remotos

Por questões de distância geográfica e que naturalmente implicam limitações na ligação de dados entre Leiria, Caldas e Peniche, não foi possível recorrer à mesma abordagem utilizada no desenho e definição da arquitetura de segurança para os campus residentes em Leiria. As condicionantes fizeram com que fossem tidos alguns cuidados, a fim de não prejudicar a ligação com tráfego escusado.

A opção tomada passou pela terminação de todas as diferentes redes nos equipamentos locais, ou seja, criação de zonas semelhantes às referidas na zona local.

Exceções

Para além das zonas definidas existem segmentos de rede destinados à gestão da infraestrutura de TI do IPL onde se incluem os equipamentos ativos (APs, *Switches*, *Routers*) e infraestrutura de VoIP por exemplo. Estas zonas não se encontram definidas na arquitetura de segurança mas estão contempladas, sendo garantido apenas o acesso aos utilizadores que possuam direitos de gestão ou se encontrem no NOC.

5.1.2 - Tecnologia

Quando se pensa em tecnologia de segurança, o primeiro termo que surge é o de *firewalls* como ferramenta fundamental na defesa dos computadores e serviços das organizações. Os *firewalls* tradicionais encontram-se obsoletos e desajustados para os desafios modernos, sendo

facilmente controlados pelas ameaças dos nossos dias. Como resposta à sua incapacidade, surgiram os NGFW.

A arquitetura definida para o IPL assenta na tecnologia dos NGFWs estudada no item 3.4 *Firewalls* da Próxima Geração.

.

5.1.3 - Redundância e Desempenho

Sendo as organizações cada vez mais dependentes de tecnologia, a performance e disponibilidade são fundamentais para o sucesso do negócio. Para garantir uma disponibilidade contínua dos sistemas, evitar os custos que advém da interrupção no funcionamento de qualquer sistema e tendo no horizonte o máximo desempenho que permita obter o máximo retorno do investimento efetuado, qualquer arquitetura deve ter como meta a alta disponibilidade.

No processo de definição da arquitetura, existiu uma preocupação em torná-la redundante e com níveis de desempenho elevados que respondessem às exigências do IPL. Ao analisar a arquitetura proposta (Figura 31) verifica-se que os primeiros níveis de segurança encontram-se suportados em *clusters* de duas máquinas cada. Esta opção, para além de garantir redundância em caso de avaria dos componentes que suportam arquitetura, permite ainda aumentar o seu desempenho através da utilização de *clusters* em modo ativo-ativo.

No caso das zonas locais, por questões de ordem financeira, a opção foi a de não utilizar *clusters* mas sim fazer o *bypass* aos equipamentos de segurança no caso de falha. Nesta situação o *bypass* permite que os equipamentos em *cluster* assumam o papel do equipamento em falha.

O *bypass* aos equipamentos será feito através da utilização de VRF (*Virtual Rounting and Forwarding)* nos equipamentos de core do fabricante Cisco.

5.1.4 - Mobilidade

O crescimento exponencial na utilização de dispositivos portáteis, assim como o uso de redes sem fio, fez com que aumentasse de forma considerável a mobilidade dos utilizadores e consequentemente as necessidades de segurança. Com esta "revolução", os dispositivos passíveis de mobilidade atingiram o estatuto de ferramentas indispensáveis no dia-a-dia, sendo em muitos casos essenciais na gestão de negócios.

Consequentemente, nos ambientes onde a mobilidade se encontra presente de forma acentuada, as vulnerabilidades dos sistemas e dados sensíveis tornam-se maiores existindo complexidade na gestão do utilizador móvel e na problemática intrínseca da segurança.

Um dos problemas na gestão de uma infraestrutura similar à do IPL diz respeito ao controlo e gestão de políticas/acessos de segurança dos utilizadores. Em virtude da mobilidade é essencial assegurar que, independente da localização ou dispositivo usado, os

direitos/restrições acompanhem o utilizador. Esta abordagem, para além de facilitar a gestão de segurança e tratar os utilizadores de forma particular, garante a proteção do perímetro de segurança, esteja o utilizador onde estiver.

Na arquitetura proposta e recorrendo à técnica de *captive portal*[36], é possível controlar todos os tipos de utilizadores dentro da infraestrutura. Este tipo de técnica garante que, independentemente do utilizador, dispositivo, tipo de rede (com fio ou sem fio) ou local da organização em que este tenta aceder à infraestrutura, que apenas lhe seja autorizado o acesso à rede e seus recursos, posteriormente ao processo de autenticação no *captive portal*. O *captive portal* recorre ao serviço de diretório existente para efetuar a validação dos utilizadores, assim como a atribuição das suas políticas de segurança.

Esta abordagem, apenas é utilizada em dispositivos que não se encontrem integrados no domínio IPLeiria.pt. Para os integrados, o processo de autorização de acesso à rede encontra-se integrado na autenticação do dispositivo no domínio.

5.1.5 - Utilizadores Remotos

O controlo e visibilidade de utilizadores móveis e remotos é uma das grandes falhas na maioria das arquiteturas. O desafio não é o de controlar este tipo de utilizadores mas sim disponibilizar uma solução que permita um controlo similar à fornecida localmente, sem que sejam constituídas políticas independentes para estes utilizadores. Existe um conjunto de opções disponíveis para o controlo de utilizadores remotos:

- ***Software* para clientes** – A distribuição e instalação deste tipo de soluções, por vezes, é problemática. Normalmente, quando sobrecarregado, reflete-se no desempenho dos clientes. O *software* funciona como cliente do NGFW;
- **Portais de entrada** – Serviços *Web* que disponibilizam, normalmente através da porta 80, o acesso a um conjunto limitado de serviços e contra medidas (filtragem URL e *malware*). São personalizáveis;
- **VPN** – Pode ser usado SSL ou IPSec. Necessita de um gateway.

Analisadas as opções destinadas a utilizadores remotos, a solução baseada em *software* cliente persistente oferece a melhor alternativa. Tal como na abordagem da VPN, o tráfego remoto é enviado através de um túnel seguro, com a diferença que a ligação é feita automaticamente com o NGFW, sem que seja necessária a intervenção do utilizador. A sessão do utilizador é protegida e controlada existindo a capacidade para identificação das aplicações.

A abordagem dos portais de entrada será a opção para os tipos de dispositivos que não sejam suportados pelo NGFW e necessitem de mobilidade e também para acessos remotos estáticos, ou seja, utilizadores que necessitem apenas de aceder pontualmente a um conjunto de serviços prontamente identificados. Este tipo de acesso facilitará o utilizador.

[36] Portal de autenticação de utilizadores usado para garantir apenas acesso à rede aos utilizadores autenticados.

5.1.6 - Módulos e Proteções

Nos dias de hoje, as organizações são confrontadas com desafios que "obrigam" a implementação de uma infraestrutura de segurança consistente, com a capacidade de garantir a conformidade dos seus negócios, a redução das interrupções dos seus serviços e que seja capaz de responder proativamente aos novos desafios de segurança.

Para além da definição da arquitetura e tecnologia que servirá de suporte à mesma, torna-se crucial definir diversas proteções a empregar na infraestrutura de segurança.

Na proposta de arquitetura do IPL foram definidos diferentes tipos de proteções e facilidades (Figura 33) com a missão de combater as ameaças e os riscos enumerados no capítulo anterior.

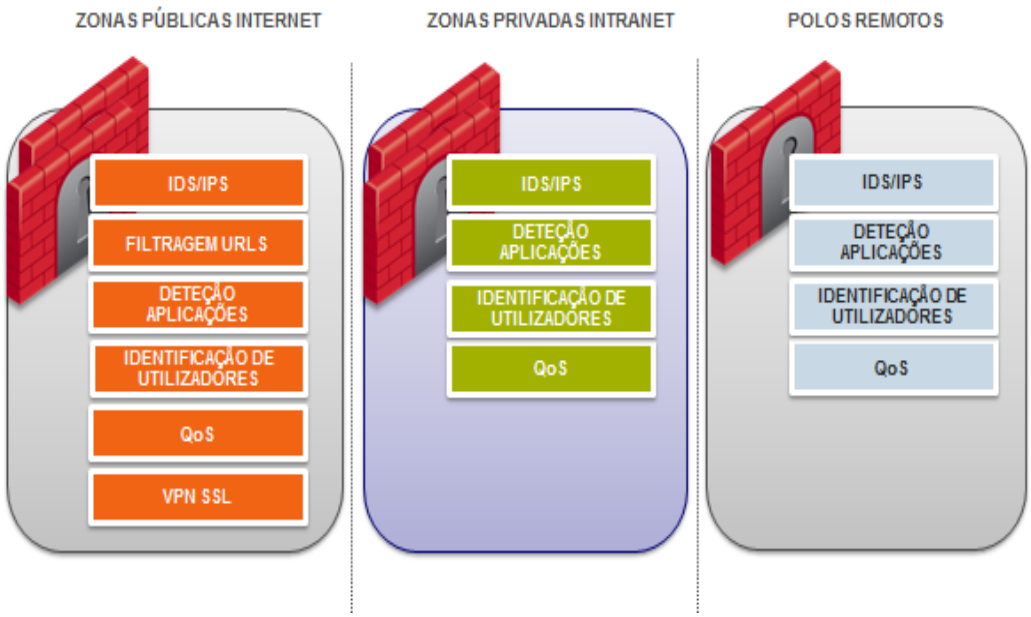

Figura 33 – Mecanismos de Proteção

A abordagem de não utilizar as mesmas proteções e facilidades em todas as zonas é justificada pela necessidade de ajustar as proteções às características das zonas e aos requisitos de segurança estabelecidos para cada. A estrutura e dinamismo que a proposta de arquitetura de segurança detém faz com que na maioria dos casos ocorra uma comunicação natural entre todas as zonas, o que garante a avaliação do tráfego pelos diferentes módulos de proteções distribuídos pelas zonas da arquitetura.

Na escolha das proteções, deve-se ter em conta o impacto da segurança no desempenho da infraestrutura. Atualmente, a segurança e o desempenho são características que precisam de andar de mãos dadas, uma vez que, uma rede com um alto desempenho e não segura é tão ineficiente quanto uma muito segura e com desempenho abaixo do esperado.

As proteções de segurança e o objetivo da sua utilização são os seguintes:

- **IDS/IPS** – Módulo de deteção e resposta a ataques de intrusão, responsável por detetar ataques em curso e responder de forma proativa, bloqueando automaticamente e instantaneamente o atacante. Este módulo foi colocado em todas as zonas com objetivo de parar os ataques o mais próximo da fonte;
- **Filtragem URLs** – Filtro de conteúdos Web, constituído por milhões de URLs distribuídos por diversas categorias. Esta funcionalidade garante o controlo das páginas de internet a fornecer aos elementos da organização, impedindo os utilizadores de visitar sítios com risco elevado e ameaças. Este módulo de segurança permite ainda aumentar a produtividade da organização. A filtragem de URLs apenas se aplica na zona intranet sendo justificável esta opção por tratar da zona de acesso à Internet;
- **Deteção de aplicações** – Responsável pela visibilidade e controlo de aplicações. Permite identificar, autorizar, bloquear ou limitar o uso de aplicações por utilizador ou grupo. Pode ser usada para educar e alertar os utilizadores sobre as aplicações e os seus riscos. A utilização desta funcionalidade permite aumentar a produtividade da organização, visibilidade e controlo da rede. Todas as zonas incluem esta proteção;
- **Identificação de utilizadores** – Para além da visibilidade e controlo de aplicações é necessário aumentar a visibilidade dos utilizadores. Este módulo mostra a atividade dos utilizadores e identifica-os. Dentro do IPL, a identificação dos utilizadores internos será feita recorrendo ao serviço de diretório. Todas as zonas incluem esta proteção.
- **QoS** – Responsável pela gestão de QoS e controlo de largura de banda. Optimiza o desempenho da rede através da priorização das aplicações críticas e utilizadores finais. De forma a garantir a qualidade na infraestrutura todas as zonas incluirão o módulo QoS.
- **VPN SSL** – Módulo responsável pela disponibilização de acesso via VPN através de uma página web. Este módulo será apenas aplicado na zona internet com intuito de permitir esta funcionalidade aos utilizadores remotos.

Na seleção das proteções foi ainda equacionada a implementação de mecanismos de DLP. Esta opção não foi tomada devido ao pouco estado de maturação que este tipo de tecnologia neste momento apresenta.

5.1.7 - Gestão, Registos e Relatórios

Nos últimos anos, o aparecimento de novos desafios de segurança teve como causa direta o aumento do número de equipamentos de rede. Este crescimento foi responsável pelo incremento proporcional no esforço de gestão destas soluções, exigindo enormes gastos de tempo e pessoal.

A difusão de vários sistemas de segurança e sistemas de optimização fez com que surgissem infraestruturas cada vez mais exigentes, com incontáveis interações entre dispositivos.

Numa infraestrutura de segurança de grande dimensão, constituída por diversos equipamentos distribuídos geograficamente, torna-se inquestionável a utilização de uma abordagem de gestão única, que ofereça uma resposta convincente para os requisitos das arquiteturas de segurança moderna. A infraestrutura poderá ser complexa, mas isto não representa que a sua gestão deixe de ser transparente e eficiente.

Na gestão moderna das arquiteturas de segurança, a rastreabilidade e a auditoria de controlo são dois conceitos essenciais. Se, através da rastreabilidade conseguimos recuperar todo o histórico de operações e processos efetuados na infraestrutura, já a auditoria de controlo permite preservar e recuperar as configurações.

Num estado inicial, os equipamentos de segurança apresentam bastantes analogias, com o passar dos tempos poderá existir uma disparidade entre eles em função da especificidade da zona a que pertencem ou das necessidades de segurança particulares.

A arquitetura proposta possibilitará a gestão central de todos os equipamentos através de uma única interface para a gestão das similaridades, convergência, segurança, auditoria e controlo.

Em qualquer infraestrutura, os registos são responsáveis pela informação sobre o seu funcionamento e eventos que ocorrem. Por vezes, esta informação é a única ferramenta que um administrador possui para descobrir as causas de um problema ou comportamentos anómalos. Para que estes registos tenham utilidade é necessário que os registos horários se encontrem sincronizados com um servidor NTP e que sejam tão detalhados quanto possível, tendo sempre o cuidado para não gerar dados em excesso.

No que diz respeito a infraestruturas de segurança de grande dimensão e com diversos mecanismos, torna-se obrigatório a existência de uma plataforma central de análise e auditoria de registos com a capacidade para analisar registos de todos os equipamentos, possuindo a habilidade para gerar relatórios acerca da rede, segurança e atividade dos utilizadores. A criação de relatórios deverá ser realizada de forma automática e periódica de acordo com as necessidades do administrador. O objetivo é economizar tempo e reduzir custos aproveitando a infraestrutura de segurança existente.

5.1.8 - Funcionamento

Como foi referido anteriormente, o sucesso nesta arquitetura passa em parte pelo elemento central da arquitetura, os NGFWs. Estes equipamentos vão ter a função de controlar o tráfego e toda a atividade dos locais onde se encontram localizados. Na maioria dos casos assumirão o controlo através do papel de *gateways* das diversas redes que se pretende controlar e segurar.

A comunicação entre as diferentes unidades que compõem o IPL será efetuada exclusivamente com o recurso a endereçamento privado, sendo que, cada organização será identificada pelo seu endereçamento. Ao contrário do passado, o endereçamento público migrará para os equipamentos que suportam a zona internet e será apenas utilizado na

comunicação de/para Internet. Aqui pretende-se suportar simultaneamente endereçamento IPv4 e IPv6.

A zona internet será também caracterizada por controlar o acesso dos dispositivos do IPL ao exterior. O acesso será efetuado recorrendo a NAT, exceto nos casos em que este mecanismo não possa ser utilizado.

O processo de autorização à rede será também controlado nos NFGWs e será efetuado da seguinte forma:

1. O utilizador liga o dispositivo na infraestrutura de rede do IPL (seja com ou sem fios);
2. Se o dispositivo se encontrar adicionado ao domínio, o processo de validação de segurança é feito de forma automática, se não, surgirá o *captive portal* que permitirá introduzir as credenciais do utilizador;
3. Se o processo de autenticação ocorreu com sucesso, o NGFW atribui as políticas de segurança ao utilizador e garante o acesso à rede, caso contrário, bloqueia o acesso do utilizador na infraestrutura.

Para além das funcionalidades descritas no item módulos e proteções da arquitetura, os equipamentos realizarão também a inspeção de todo o trafego SSL com exceção do classificado na categoria de finanças e saúde. Esta opção serve de resposta à abordagem dos utilizadores na utilização do trafego SSL para ocultarem as suas atividades.

A gestão de políticas numa infraestrutura de segurança baseada em NGFW permite que exista herança entre os diferentes equipamentos que a compõem. Imaginemos que o utilizador autenticado não possui políticas de segurança atribuídas, neste caso ele receberá as políticas configuradas por defeito nos equipamentos. Se na comunicação existir a passagem por mais que um NGFW, o utilizador poderá herdar as diferentes políticas configuradas por defeito nos equipamentos sobrepondo-se sempre as mais restritas.

5.2 - Implementação

Antes de partir para a fase de implementação e cumprimento do plano de ação que irá permitir a colocação em funcionamento da arquitetura de segurança, torna-se capital perceber algumas recomendações a ter em conta nesta fase e em especial no que diz respeito à implementação de mecanismos de segurança como é o caso dos NGFWs.

5.2.1 - Implantação de NGFW

Em diversos casos, verifica-se que as soluções técnicas são implementadas sem serem consideradas as implicações que estas possuem na organização e na sua estratégia de segurança. Para que este erro não aconteça, é necessário assegurar que as políticas da organização se encontram atualizadas e que as soluções a implementar permitem suportá-las.

Para que seja eficaz a implantação dos NGFW, é indispensável que sejam criadas políticas inteligentes, não devendo o departamento TI ser o único dono destas. Sem o apoio dos responsáveis das organizações, o seu sucesso poderá estar condenado. Uma vez aprovada a utilização das aplicações pela administração, o departamento de TI não mais terá o seu apoio para impedir a sua utilização.

O cumprimento das políticas possui melhores resultados se estas surgirem com base em políticas inteligentes desenvolvidas pelos seguintes interessados: TI, recursos humanos, gestão e utilizadores.

Muitas vezes, os responsáveis pela segurança baseiam os seus argumentos e tomadas de decisão com base na utilização que os utilizadores dão às aplicações *Web* 2.0, referindo por exemplo a conformidade do uso de aplicações de entretenimento durante o horário laboral. Este argumento poderá não ser válido, em virtude de possivelmente, não existir regulamentação interna para a utilização das aplicações *Web* 2.0. Tudo se resume à utilização da ferramenta certa no lugar certo. As aplicações *Web* 2.0 são consideradas o fruto proibido dentro das organizações, onde os responsáveis pela segurança o tentam impedir e os funcionários da organização o cobiçam.

O papel dos responsáveis pela segurança é o de educar os funcionários para as implicações no uso das ferramentas, participar no desenvolvimento da política de uso e posteriormente garantir a sua monitorização e cumprimento.

Se vão ser aplicados e executados controlos de aplicações, estes devem ser parte integrante da política de segurança . Como parte do processo de implementação de uma política de controlo de aplicações, deve ser feito um esforço concertado para aprender sobre as aplicações *Web* 2.0 e a sua proliferação dentro da organização. O que inclui perceber o funcionamento, o objetivo e a sua forma de agir.

5.2.2 - Controlo de Utilizadores

As organizações devem fornecer aos seus utilizadores, em especial aos funcionários, a política de uso de aplicações onde se encontram definidas as aplicações que são permitidas e proibidas e os seus termos de uso. Cada utilizador deverá ainda compreender e perceber o conteúdo da política e as consequências do seu incumprimento. Além de tudo isto, ficam ainda algumas questões por responder, incluindo:

Dado o número crescente de aplicações como saberá o utilizador quais as permitidas e proibidas?

Como é atualizada a lista das aplicações proibidas? Como se garante que os utilizadores sabem que a lista mudou?

O que constitui uma violação da política?

O desenvolvimento das políticas é muitas vezes um desafio entre o risco e a recompensa, onde existem diversas opiniões acerca do que deve ser permitido e proibido. O cerne desta questão centra-se no facto de, por vezes, os dois grupos (TI, RH) organizacionais mais presentes neste processo, serem normalmente "marginalizados" durante a adoção de novas tecnologias para a organização. A elaboração de uma política segura de utilização de aplicações torna-se assim uma tarefa ingrata quando a tecnologia já está escolhida e a mesma apresenta diversos problemas de segurança.

5.2.3 - Plano de migração

A migração é um dos fatos mais desafiadores para os elementos das equipas de TI, devido à complexidade que acompanha um processo desta natureza. Já por si, a simples ideia de substituir qualquer arquitetura de segurança ou tecnologia é bastante assustadora. Um dos maiores obstáculos responsáveis por este medo, deve-se à perda do conhecimento adquirido ao longo dos anos na arquitetura de segurança e tecnologia envolvida. Esta troca faz com que o administrador saia da sua zona de conforto, o que o deixa bastante incomodado.

No caso do IPL, a migração para além de significar a implementação de uma nova arquitetura de segurança, caracterizada pelo *refresh* tecnológico que introduz na organização, significa também a entrada em produção de novos mecanismos de segurança. Estas mudanças representam avanços tecnológicos consideráveis, que obrigam a alterações profundas na infraestrutura de rede, aumentando assim a probabilidade de existirem tempos de inatividade e impacto sobre os serviços que suportam o negócio do IPL.

Qualquer migração deve ser programada recorrendo a pequenas etapas, assegurando uma transição suave para a nova infraestrutura de segurança e uma maior probabilidade de sucesso. A fase de migração, na maioria das vezes, representa uma boa oportunidade para realizar uma auditoria, avaliação e validação da política de segurança. Em algumas situações, uma migração pode representar uma melhor compreensão e conhecimento da infraestrutura de segurança e resultar numa documentação bem-sucedida da mesma.

Em cada fase do processo de migração, as equipas envolvidas devem caracterizar completamente a fase em questão, perceber todas as *nuances* e avaliar diversos caminhos existentes antes de partir para a migração.

Fase1: Recolha de Informação

A primeira fase consiste em reunir todas as informações sobre a infraestrutura atual e a sua configuração. Esta informação é fundamental para o sucesso do processo de migração porque permite conhecer a infraestrutura em funcionamento e todas as suas particularidades. Para além do contexto de migração, a recolha de informação é sempre útil. As informações recolhidas incluem:

- Topologia da rede;
- Esquemas de endereçamento e configurações de interfaces;
- Aplicações e protocolos suportados;

- Configurações dos equipamentos e as políticas que implementam;
- Configuração das VPNs.

Devem ser feitas cópias de todas as informações e configurações de forma a preservar um quadro do estado atual da arquitetura. No final desta fase, o estado da arquitetura atual deve estar bem compreendida e representada.

Fase2: Desenho da Arquitetura Física e Lógica

Com base na informação recolhida e com o desenho da arquitetura pretendida, deve-se trabalhar no sentido de desenhar a arquitetura de segurança a implementar, elaborando esquemas físicos e lógicos para sua implementação. Nestes desenhos deve-se ter em conta a definição das diferentes zonas, assim como os seus elementos. Na implementação da arquitetura do IPL e tentado minimizar os tempos de indisponibilidade, o desenho vai ter em conta a coabitação das duas arquiteturas, permitindo assim uma migração sustentável.

Fase3: Planos de Migração

Em conjunto com todas as equipas dos serviços informáticos devem ser elaborados planos de migração que contemplem a migração de utilizadores, servidores e serviços. Os planos devem ser minuciosos.

Fase4: Migração e Adaptação de Políticas de Segurança

Os responsáveis pela migração devem analisar as políticas de segurança existentes de forma a planear a sua implementação na nova arquitetura e nos elementos que a compõem. A adaptação das políticas existentes e a criação de novas, que respondam aos novos desafios de segurança e à nova arquitetura, devem ser feitas nesta fase.

Fase5: Testes

Nesta fase deverão ser realizados todos os testes nos equipamentos que suportam a arquitetura. Os testes devem ser intensivos com objetivo de validar funcionalidades, aspetos operacionais da política de segurança, regras de NAT, políticas de encaminhamento e mecanismos de segurança. Além disso, devem simular cenários de *failover*, uma vez que pode ser difícil testar após a transição da arquitetura para produção.

Fase6: Implementação

A fase de implementação tem como objetivo a implementação da arquitetura com base na informação recolhida nas fases anteriores. Aqui será dado um cuidado especial na implementação da arquitetura em coabitação com a atual, sem que existam tempos de indisponibilidade.

Em virtude do esforço de implementação ser demasiado grande, o processo de implementação é dividido em diferentes fases. Cada fase é realizada em dias diferentes, tendo cada uma a sua própria janela de implementação.

Após a implementação da arquitetura em paralelo, toda a infraestrutura deverá ser configurada e preparada para os objetivos definidos. Posteriormente, procederá à migração gradual de utilizadores, servidores e serviços definidos nos planos fase 3. A fase de migração também será dividida em diferentes períodos devido à necessidade de realizar a migração faseada por campus do IPL.

Uma vez que a arquitetura é bastante complexa e introduz novas proteções e funcionalidades de segurança, a introdução destes mecanismos será feita de forma gradual com objetivo de não criar entropias e minimizar os pontos de falha.

Fase7: Documentação

A documentação, apesar de muitas vezes ser descurada pelos administradores de sistema, é uma medida bastante importante que permite uma rápida avaliação da situação de um sistema. A ideia passa por efetuar uma espécie de diário da infraestrutura de segurança onde se reúna, para além da informação descrita na fase 1, todas as configurações realizadas ao longo dos tempos e alterações na infraestrutura.

Esta página foi intencionalmente deixada em branco

6 - Conclusões

A segurança hoje em dia é um dos grandes desafios nas organizações, sendo uma preocupação constante para os seus responsáveis.

Os principais objetivos desta dissertação foram o de especificar e conceber uma arquitetura de segurança para o IPL que respondesse aos novos desafios de segurança de forma eficiente e eficaz, sem comprometer a usabilidade e o desempenho da infraestrutura de rede.

Para auxiliar na definição do modelo, foram estudados diversos temas e desafios referidos no capítulo 2 e 3. É evidente a contribuição dada no estudo das problemáticas resultantes do aparecimento de novos dispositivos que tiveram como consequência alterações no perímetro de segurança e das ameaças que surgiram com o aparecimento das aplicações *Web 2.0*. No capítulo 3, foram ainda abordados os NGFW que afinal de contas acabam por ser o coração da arquitetura proposta.

O processo de caracterização e análise da arquitetura existente efetuado no capítulo 4 foi determinante na definição dos requisitos que o modelo de arquitetura e os mecanismos a implementar deviam contemplar. Neste capítulo, foi possível concluir através da análise de risco das aplicações em funcionamento no IPL, que existem diversos problemas e ameaças na utilização que é dada à rede, de onde se destacam: ocultação de atividade por parte dos utilizadores; consumo excessivo de largura de banda; baixa produtividade e perda de informação confidencial.

O modelo de arquitetura foi definido no capítulo 5, tendo seguido as orientações base da arquitetura SAFE da cisco, dando especial atenção no aumento de visibilidade e controlo. A arquitetura proposta é constituída por 3 zonas de seguranças distribuídas por equipamentos NGFW. A primeira zona, considerada de zona pública, corresponde à DMZ Internet. A sua responsabilidade é a de alojar e proteger todos os serviços expostos diretamente na Internet ou os utilizadores que representem risco elevado. À segunda zona, batizada de zona privada, cabe-lhe a função de resguardar todos os serviços de suporte ao funcionamento do IPL (gestão documental, gestão académica, colaboração, virtualização,…). Nesta zona, para além dos serviços, serão alojados os utilizadores do qual o seu trabalho depende quase exclusivamente destas aplicações. Por fim, a DMZ local abriga todos os serviços exclusivos dos campus e os seus utilizadores.

Olhando para a arquitetura atual e para a proposta, contata-se que o objetivo foi cumprido na integra. O desenho escolhido, para além de responder às necessidades do IPL resultantes da centralização ocorrida em 2007.

A utilização dos NGFWs revela-se uma mais-valia conseguindo este dispositivo dar resposta a todas exigências e inclusive responder positivamente às ameaças e desafios previstos pela *checkpoint* para 2011.

No que diz respeito à gestão da infraestrutura constituída por diversos componentes distribuídos geograficamente, a utilização de uma abordagem de gestão única revelou-se uma mais-valia para a equipa responsável pela segurança.

6.1 - Trabalhos Futuros

A informação é um dos bens de maior valor das organizações, devendo ser corretamente utilizada e protegida de todas as ameaças e riscos. De forma a garantir a sua segurança, será necessário, no futuro, adoptar políticas e procedimentos, reduzindo assim os riscos de falhas, danos e/ou prejuízos que possam comprometer a imagem e os objetivos do IPL. A utilização de uma política de segurança adequada funcionará como uma declaração formal acerca do compromisso com a proteção da informação, devendo ser cumprida por todos seus utilizadores.

O desafio do futuro passará pela elaboração desta política, que deverá ter por base uma auditoria a todos os sistemas existentes com objetivo de detetar âmbitos e vulnerabilidades. O seu resultado deverá ser expresso num conjunto de documentos com três níveis hierárquicos distintos: Política de Segurança da Informação; Normas de Segurança da Informação e Procedimentos de Segurança.

"Educar para segurar"

Bibliografia

1. **Silva, Pedro, Carvalho, Hugo e Torres, Catarina.** Segurança dos Sistemas de Informação. s.l. : Centro Atlantico, 2003, pp. 12-15.

2. **Zorrinho, C.** *Gestão da Informação.* s.l. : Editorial Presença, 1991.

3. **Miller, HG e Murphy, RH.** *Secure cyberspace: Answering the Call for Intelligent Action.* s.l. : IT Profissional, 2009. pp. 60-63.

4. **Pfleeger, C.P e Pfleeger, S.L.** *Security in Computing.* 3rd Edition. s.l. : Prentice Hall, 2003.

5. **Parker, Donn.** Toward a New Framework for Information Security. [autor do livro] Michel Kabay e Seymour Bosworth. *The Computer Security Handbook.* 4º. New York : Wiley, 2002, 5.

6. **ISO.** *ISO/IEC 17799 - Information Technology - Code of practice for information security management.* s.l. : British Standard Institution, 2005.

7. —. *ISO/IEC 27002:2005 Information technology - Security techniques - Code of pratice for information security management.* 2005.

8. **Fenton, J.H e Wolfe, J.M.** *Organizing for Success: Some Human Resources Issues in Information Security.* [ed.] H.F. Tipton and M. Krause. 4 Edition. s.l. : Auerbach Publications, 2003. pp. 313-324. Vol. 4.

9. **Bekin, Saul.** *Endomarketing, Como Pratica-lo com sucesso.* s.l. : Prentice Hall Brasil, 2003.

10. **Cabeça, Vitor.** A Internet no lar. *Marktest.* [Online] GrupoMarktest, 2011. [Citação: 12 de 07 de 2011.] http://www.marktest.com/wap/a/n/id~16fa.aspx.

11. **Moore, D., Shannon, C. e Claffy, K.** *Code-Red: A case study on the spread and victims of an Internet worm.* Marseille : s.n., 2002. pp. 273-284.

12. **Tanenbaum, Andrew S.** *Computer Networks (fourth edition).* s.l. : Prentice Hall, 2003. 0-13-066102-3.

13. **Dowd, P.W. e McHenry, J.T.** *Network Security: It's Time to Take It Seriously.* s.l. : IEEE, 1998. pp. 24-28. Vol. 31.

14. **Kartalopoulos, Stamatios V.** *ICC '08. IEEE International Conference.* Beijing : s.n., 2008. pp. 1469 - 1473.

15. **RedHat.** Red Hat Enterprise Linux 3: Security Guide. *Docs Redhat.* [Online] [Citação: 13 de 07 de 2011.] http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/3/html/Security_Guide/ch-sgs-ov.html.

16. **Hamer, David, Sullivan, Geoff e Weierud, Frode.** *Enigma Variations: An Extended Family of Machines.* s.l. : Cryptologia.

17. Internet Usage Statistics The Interent Big Picture. *Internet World Stats.* [Online] [Citação: 17 de 08 de 2011.] http://www.internetworldstats.com/stats.htm.

18. **ISO.** *ISO/IEC 13335-1:2004 - Information technology - Security techniques – Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.* 2004.

19. **NIST.** NIST SP 800-30 – Risk Management Guide for Information Technology Systems . 2002.

20. **ITSEC.** *Information Technology Security Evaluation Criteria - Harmonized Criteria of France, Germany, the Netherlands, and the United Kingdom.* s.l. : Dept. of Trade and Industry, 1991.

21. **NIST.** NIST 800-100 - Information Security Handbook: A Guide for Managers. 2006.

22. **Whitman, Michael E. e Mattord, Herbert J.** *Management of Information Security.* 3º. s.l. : Delmar Cengage Learning, 2009.

23. **TZU, SUN.** *A Arte da Guerra.* s.l. : Jardim dos Livros, 2007.

24. **Adeyinka, O.** Internet Attack Methods and Internet Security Technology. s.l. : Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, 2008, pp. 77-82.

25. **Odom, Wendel.** CCNA Self-Study CCNA INTRO Exam Certification Guide. s.l. : Cisco Press, 2004, p. 627.

26. **Buecker, Axel, Andreas, Per e Paisley, Scott.** *Understanding IT Perimeter Security.* s.l. : IBM, 2008.

27. **Thomsett, R.** The Indiana Jones School of Risk Management. s.l. : American Programmer, 1992, Vol. 7, pp. 10-12.

28. **Cisco.** Cisco SAFE: A Security Reference Architecture. [Online] Cisco System, 2009. [Citação: 16 de 08 de 2011.] http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns954/white_paper_c11-527476.pdf.

29. —. *Cisco SAFE Reference Guide.* s.l. : Cisco Systems, 2010.

30. **PALOALTO.** Application Usage and Risk Report. *Paloalto Networks.* [Online] May de 2011. [Citação: 15 de 07 de 2011.] http://www.paloaltonetworks.com/literature/forms/aur-report.php.

31. —. The Application Usage and Risk Report - An Analysis of End User Application Trends in the Enterprise. *PaloAlto Networks.* [Online] 15 de 07 de 2010. http://www.paloaltonetworks.com/literature/whitepapers/App_Usage_Risk_Spring2010.pdf.

32. —. Academic Freedom and Application Chaos:A Delicate Balancing Act (2nd Edition, March 2011). *PaloAlto Networks.* [Online] March de 2011. [Citação: 19 de 08 de 2011.] http://www.paloaltonetworks.com/literature/higherEd_report.php.

33. Check Point reveal top security challenges for 2011. *Infosecurity Magazine.* [Online] 2011. [Citação: 27 de 08 de 2011.] http://www.infosecurity-magazine.com/view/17795/check-point-reveal-top-security-challenges-for-2011.

34. **Beznosova, Olga e Beznosov, Konstantin.** On the imbalance of the security problem space and its expected consequences. *Information Management & Computer Security.* 2007, Vol. 15, 5, pp. 420-431.

35. **Mayorkas, Alejandro e Mrozek, Thom.** Kevin mitnick sentenced to nearly four years in prison; computer hacker ordered to pay restitution to victim companies whose systems were compromised. *U.S. Department of Justice.* [Online] 1999. [Citação: 27 de Agosto de 2011.] http://www.justice.gov/criminal/cybercrime/mitnick.htm.

36. **Formyduval, W.** *Integrating static analysis and testing for firewall policies.* 2009. pp. 749-750.

.

Esta página foi intencionalmente deixada em branco

Anexo A

Neste apêndice serão apresentadas todas as aplicações de risco detetadas durante a fase de análise de risco de aplicações na rede do IPL.

Aplicações de Risco

Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
5	google-docs	business-systems	office-programs	browser-based	3,579,407,837	58,939
4	evernote	business-systems	office-programs	client-server	133,734,793	2,715
4	ms-groove	business-systems	office-programs	peer-to-peer	25,695,067	172
5	google-docs-enterprise	business-systems	office-programs	browser-based	383,445	31
4	ms-update	business-systems	software-update	client-server	74,635,069,965	162,132
4	adobe-update	business-systems	software-update	client-server	59,968,807,902	13,467
4	crashplan	business-systems	storage-backup	client-server	713,448,506	9
5	smtp	collaboration	Email	client-server	69,279,075,864	1,758,261
4	gmail	collaboration	Email	browser-based	52,170,596,767	459,209
4	hotmail	collaboration	Email	browser-based	25,342,560,585	341,01
4	ms-exchange	collaboration	Email	client-server	16,403,872,960	42,135
4	pop3	collaboration	Email	client-server	3,155,565,694	371,081
4	imap	collaboration	Email	client-server	782,864,800	94,462
5	horde	collaboration	Email	browser-based	268,928,745	16,279
4	outlook-web	collaboration	Email	browser-based	116,846,019	3,035
4	gmail-enterprise	collaboration	Email	browser-based	103,446,275	2,107
4	qq-mail	collaboration	Email	browser-based	90,852,901	6,065
4	squirrelmail	collaboration	Email	browser-based	24,916,846	738
4	roundcube	collaboration	Email	browser-based	11,551,326	41
4	mail.ru	collaboration	Email	browser-based	4,294,310	21
4	netease-mail	collaboration	Email	browser-based	1,337,769	95
4	fastmail	collaboration	Email	browser-based	803,662	43
4	twig	collaboration	Email	client-server	687,242	18
4	aim-mail	collaboration	Email	browser-based	240,891	28
4	secureserver-mail	collaboration	Email	browser-based	3,21	2
4	msn	collaboration	instant-messaging	client-server	6,542,267,779	306,142
4	aim	collaboration	instant-messaging	client-server	1,548,302,574	1,770,827
4	google-talk	collaboration	instant-messaging	client-server	442,996,473	19,13
4	qq	collaboration	instant-messaging	client-server	264,552,985	39,139
5	ebuddy	collaboration	instant-messaging	browser-based	192,282,164	29,488
4	yahoo-im	collaboration	instant-messaging	client-server	52,615,842	16,042
5	jabber	collaboration	instant-messaging	client-server	35,009,688	5,899
4	imo	collaboration	instant-messaging	browser-based	33,444,572	2,743
4	gadu-gadu	collaboration	instant-messaging	client-server	24,019,060	4,548
4	mibbit	collaboration	instant-messaging	browser-based	6,336,622	282
4	google-buzz	collaboration	instant-messaging	browser-based	2,941,526	9
4	icq	collaboration	instant-messaging	client-server	2,230,543	169
4	aim-express	collaboration	instant-messaging	browser-based	816,668	147
5	irc	collaboration	instant-messaging	client-server	58,546	18
4	simplite-msn	collaboration	instant-messaging	peer-to-peer	18,638	2
5	adobe-connect	collaboration	internet-conferencing	browser-based	94,064	2
4	facebook	collaboration	social-networking	browser-based	39,913,816,998	1,507,163
4	vkontakte	collaboration	social-networking	browser-based	4,056,229,882	44,446

4	facebook-posting	collaboration	social-networking	browser-based	3,514,507,820	45,422
4	facebook-apps	collaboration	social-networking	browser-based	780,718,080	38,356
5	netlog	collaboration	social-networking	browser-based	609,590,871	3,28
4	myspace	collaboration	social-networking	browser-based	313,271,347	7,927
4	sina-weibo	collaboration	social-networking	browser-based	168,759,453	22,792
4	odnoklassniki	collaboration	social-networking	browser-based	118,619,839	4,515
4	plaxo	collaboration	social-networking	browser-based	3,648,445	507
4	daum	collaboration	social-networking	browser-based	1,849,766	652
4	twitter-posting	collaboration	social-networking	browser-based	1,192,222	247
4	cyworld	collaboration	social-networking	browser-based	527,329	13
4	myspace-posting	collaboration	social-networking	browser-based	31,133	1
5	skype	collaboration	voip-video	peer-to-peer	47,139,429,216	168,687
4	msn-voice	collaboration	voip-video	peer-to-peer	18,389,699,265	55,582
4	sip	collaboration	voip-video	peer-to-peer	369,359,344	41,915
4	gtalk-voice	collaboration	voip-video	peer-to-peer	139,774,056	13
5	stickam	collaboration	voip-video	browser-based	1,671,716	32
4	yahoo-voice	collaboration	voip-video	peer-to-peer	1,362,786	399
4	h.323	collaboration	voip-video	client-server	7,82	4
4	megaupload	general-internet	file-sharing	browser-based	818,722,280,108	35,175
4	dropbox	general-internet	file-sharing	browser-based	231,525,962,875	637,37
5	fileserve	general-internet	file-sharing	browser-based	214,062,638,751	38,622
5	bittorrent	general-internet	file-sharing	peer-to-peer	136,116,957,326	1,180,640
5	filesonic	general-internet	file-sharing	browser-based	119,524,903,477	46,196
4	mediafire	general-internet	file-sharing	browser-based	42,223,018,290	10,137
5	ftp	general-internet	file-sharing	client-server	27,841,753,171	39,547
5	hotfile	general-internet	file-sharing	browser-based	20,735,633,362	7,97
4	rapidshare	general-internet	file-sharing	browser-based	19,904,075,144	4,877
4	sugarsync	general-internet	file-sharing	client-server	13,153,515,127	2,264
4	4shared	general-internet	file-sharing	browser-based	10,622,837,987	12,133
4	easy-share	general-internet	file-sharing	browser-based	9,548,543,535	789
5	emule	general-internet	file-sharing	peer-to-peer	8,480,824,430	422,95
4	qq-download	general-internet	file-sharing	peer-to-peer	7,001,042,479	559,001
4	sendspace	general-internet	file-sharing	browser-based	2,543,972,577	1,608
5	msn-file-transfer	general-internet	file-sharing	peer-to-peer	1,619,724,625	2,255
5	megashares	general-internet	file-sharing	browser-based	1,526,724,125	872
4	ifile.it	general-internet	file-sharing	browser-based	578,597,382	417
5	azureus	general-internet	file-sharing	peer-to-peer	499,238,155	837,191
4	yousendit	general-internet	file-sharing	browser-based	369,645,597	298
5	megashare	general-internet	file-sharing	browser-based	361,370,187	853
5	webdav	general-internet	file-sharing	browser-based	340,033,234	34,594
5	kugoo	general-internet	file-sharing	peer-to-peer	330,784,279	3,324
4	skydrive	general-internet	file-sharing	browser-based	291,505,928	2,141
5	filemail	general-internet	file-sharing	browser-based	252,921,271	10
4	docstoc	general-internet	file-sharing	browser-based	234,065,203	1,367
5	qq-file-transfer	general-internet	file-sharing	client-server	167,691,585	655
4	amazon-cloud-up	general-internet	file-sharing	browser-based	154,567,442	4
4	live-mesh	general-internet	file-sharing	client-server	152,983,484	3,264
5	flashget	general-internet	file-sharing	peer-to-peer	142,865,247	5,484
5	xunlei	general-internet	file-sharing	peer-to-peer	84,550,453	4,211
4	live-mesh-sync	general-internet	file-sharing	client-server	78,111,601	1,394
4	office-live	general-internet	file-sharing	client-server	36,088,350	7,139
5	imesh	general-internet	file-sharing	peer-to-peer	33,430,463	492
5	gnutella	general-internet	file-sharing	peer-to-peer	17,558,541	110,97

4	badongo	general-internet	file-sharing	browser-based	12,764,927	459
5	foxy	general-internet	file-sharing	peer-to-peer	9,465,683	8,128
4	clip2net	general-internet	file-sharing	client-server	5,573,994	62
5	ares	general-internet	file-sharing	peer-to-peer	3,784,477	14,621
4	adrive	general-internet	file-sharing	browser-based	3,244,034	95
5	gtalk-file-transfer	general-internet	file-sharing	peer-to-peer	3,143,854	4
4	aim-file-transfer	general-internet	file-sharing	peer-to-peer	2,632,084	3
4	ifolder	general-internet	file-sharing	client-server	2,280,126	174
5	manolito	general-internet	file-sharing	peer-to-peer	1,274,301	2,751
5	mydownloader	general-internet	file-sharing	browser-based	757,324	7
5	pando	general-internet	file-sharing	peer-to-peer	367,812	23
5	kazaa	general-internet	file-sharing	peer-to-peer	218,217	1
4	filedropper	general-internet	file-sharing	browser-based	187,287	13
5	transferbigfiles	general-internet	file-sharing	browser-based	146,587	7
5	neonet	general-internet	file-sharing	peer-to-peer	75,538	776
4	tftp	general-internet	file-sharing	client-server	6,356	3
4	instan-t-file-transfer	general-internet	file-sharing	client-server	5,514	4
5	direct-connect	general-internet	file-sharing	peer-to-peer	4,504	1
4	web-browsing	general-internet	internet-utility	browser-based	2,021,951,096,562	46,259,483
4	flash	general-internet	internet-utility	browser-based	295,627,915,602	865,729
4	web-crawler	general-internet	internet-utility	browser-based	18,308,159,039	311,51
4	apple-appstore	general-internet	internet-utility	client-server	11,465,856,847	8,101
4	mobile-me	general-internet	internet-utility	browser-based	6,236,206,338	7,147
5	rss	general-internet	internet-utility	client-server	3,749,070,660	144,251
4	atom	general-internet	internet-utility	client-server	2,693,023,895	37,252
4	google-desktop	general-internet	internet-utility	client-server	53,939,412	4,691
4	zamzar	general-internet	internet-utility	browser-based	8,655,544	42
5	http-audio	media	audio-streaming	browser-based	163,069,180,090	84,43
4	itunes	media	audio-streaming	client-server	22,439,500,511	18,525
4	spotify	media	audio-streaming	client-server	66,740,974	16
4	tagoo	media	audio-streaming	browser-based	464,795	13
4	pandora-tv	media	audio-streaming	browser-based	237,956	242
4	poker-stars	media	Gaming	browser-based	242,131,995	126
4	second-life	media	Gaming	client-server	32,798,268	85
4	party-poker	media	Gaming	browser-based	337,837	4
4	nintendo-wfc	media	Gaming	client-server	136,926	22
4	all-slots-casino	media	Gaming	client-server	64,524	6
4	zango	media	Gaming	browser-based	2,882	2
5	youtube	media	photo-video	browser-based	1,536,454,169,431	242,565
4	rtmp	media	photo-video	browser-based	228,719,620,271	26,455
4	ppstream	media	photo-video	peer-to-peer	157,601,979,229	2,824,029
5	http-video	media	photo-video	browser-based	114,272,840,208	34,076
5	vimeo	media	photo-video	browser-based	41,167,729,084	24,693
5	asf-streaming	media	photo-video	browser-based	37,548,298,808	2,946
4	rtmpe	media	photo-video	browser-based	33,760,313,621	3,77
4	rtmpt	media	photo-video	browser-based	20,543,377,245	2,020,359
4	qvod	media	photo-video	peer-to-peer	10,347,021,181	119,004
4	dailymotion	media	photo-video	browser-based	6,923,488,627	7,561
4	qqlive	media	photo-video	peer-to-peer	6,092,184,138	363,803
4	youtube-uploading	media	photo-video	browser-based	3,367,872,546	23
5	sopcast	media	photo-video	peer-to-peer	1,500,617,249	20,304
4	pplive	media	photo-video	peer-to-peer	1,324,358,021	36,085
4	tudou-speedup	media	photo-video	peer-to-peer	925,045,900	4,517

5	tudou	media	photo-video	browser-based	589,160,482	2,279
5	youku	media	photo-video	browser-based	445,673,627	699
4	youtube-safety-mode	media	photo-video	browser-based	411,649,468	43
4	limelight	media	photo-video	browser-based	308,430,738	2,511
4	justin.tv	media	photo-video	browser-based	126,194,165	364
4	mogulus	media	photo-video	browser-based	80,489,265	612
5	kino	media	photo-video	browser-based	53,366,442	505
4	uusee	media	photo-video	peer-to-peer	11,763,674	138
4	baofeng	media	photo-video	peer-to-peer	11,038,519	284
4	veetle	media	photo-video	browser-based	7,926,654	624
4	metacafe	media	photo-video	browser-based	4,891,240	435
4	sky-player	media	photo-video	client-server	1,067,489	20
4	socialtv	media	photo-video	browser-based	439,713	18
5	funshion	media	photo-video	client-server	211,072	19
5	libero-video	media	photo-video	browser-based	167,54	6
4	niconico-douga	media	photo-video	browser-based	109,603	3
4	yahoo-douga	media	photo-video	browser-based	40,363	1
4	ssl	networking	encrypted-tunnel	browser-based	299,954,000,194	5,862,341
4	ssh	networking	encrypted-tunnel	client-server	15,870,767,807	475,783
4	tor	networking	encrypted-tunnel	client-server	8,543,619,566	1,139
4	frozenway	networking	encrypted-tunnel	client-server	2,272,296,119	46
5	freenet	networking	encrypted-tunnel	peer-to-peer	801,603,349	35,841
5	hamachi	networking	encrypted-tunnel	peer-to-peer	225,758,087	1,306
4	dns	networking	Infrastructure	network-protocol	10,594,823,845	32,342,894
4	icmp	networking	ip-protocol	network-protocol	43,442,189	102,525
5	http-proxy	networking	Proxy	browser-based	9,033,255,783	344,43
4	dostupest	networking	Proxy	browser-based	104,743,734	1,402
4	your-freedom	networking	Proxy	client-server	41,540,276	2,467
5	phproxy	networking	Proxy	browser-based	17,398,098	133
5	cgiproxy	networking	Proxy	browser-based	9,611,302	126
5	glype-proxy	networking	Proxy	browser-based	3,944,517	64
5	coralcdn-user	networking	Proxy	browser-based	3,185,291	415
4	freegate	networking	Proxy	client-server	823,267	75
5	socks	networking	Proxy	network-protocol	159,194	309
4	vtunnel	networking	Proxy	browser-based	126,132	6
5	proxeasy	networking	Proxy	browser-based	110,488	7
5	http-tunnel	networking	Proxy	client-server	15,463	2
5	hopster	networking	Proxy	client-server	11,592	2
4	ms-rdp	networking	remote-access	client-server	2,698,994,959	13,39
5	logmein	networking	remote-access	client-server	933,645,859	7,499
5	vnc	networking	remote-access	client-server	778,176,180	19
4	pptp	networking	remote-access	network-protocol	1,168,786	153
5	vnc-http	networking	remote-access	browser-based	149,488	4
4	glide	networking	remote-access	browser-based	4,921	1

Anexo B

O apêndice B apresenta o fluxograma com todas atividades inerentes ao processo mitigação de risco.