Instituto Superior de Engenharia do Porto

Segurança da Informação na Escola Pública

Rute Conceição Vieira Pereira

Dissertação para obtenção do Grau de Mestre em Engenharia Informática, Área de Especialização em Arquiteturas, Sistemas e Redes

Orientador: Doutor António Cardoso da Costa

Júri:

Presidente:

Doutor João Jorge Pereira, Instituto Superior de Engenharia do Porto

Vogais:

Doutor António Cardoso da Costa, Instituto Superior de Engenharia do Porto

Doutor Nuno Magalhães Pereira, Instituto Superior de Engenharia do Porto

Porto, Outubro de 2012

Resumo

A função da escola é promover a aprendizagem nos jovens e estimular o acesso ao conhecimento. A utilização das TI proporciona um acesso mais rápido ao conhecimento mas, sem os mecanismos necessários, pode originar perdas e comprometer a segurança da informação.

A ausência de legislação e de regulamentação que ajude na manutenção da rede informática da escola, coloca-as numa posição muito vulnerável, obrigando-as a agir individualmente de modo a suprimir esta carência. A solução passa não só pela consciencialização dos utilizadores para a necessidade de segurança, mas também pela criação de mecanismos que permitam acrescentar segurança à rede e à própria informação.

Os projetos desenvolvidos pelo programa *Safer Internet* e pela ISECOM atuam junto da comunidade escolar, sensibilizando os utilizadores para a necessidade de segurança na Internet e nas comunicações.

Por sua vez, a adoção de práticas seguras é um processo mais demorado mas exequível através da implementação de uma política de segurança da informação adaptada à realidade da escola, de acordo com a norma ISO 27001.

Da recolha de opinião aos intervenientes do sistema resultaram dois documentos com a política de segurança da informação, um direcionado às escolas e outro aos utilizadores. Crê-se que a adoção destas recomendações pelas escolas pode trazer benefícios ao nível da segurança da informação.

Palavras-chave: Escola; Tecnologias da informação; Política; Segurança da Informação.

Abstract

The school mission is to promote learning and access to knowledge to young people. Using the Information Technologies can provide faster access to knowledge, but without the necessary mechanisms it can also lead to loss and compromise the information security.

The absence of laws and regulations that help maintaining the schools network and allow them to work can be harmful, because it forces them to act individually in order to remove this necessity. The solution not only requires the users' awareness of the security needs, but it also demands the creation of mechanisms that can add security to the network and to the information itself.

The projects which were developed by the Safer Internet Programme and by the ISECOM are working along with the school community, making users aware of the need of the Internet and the importance of communication security.

Although being a long process, the adoption of safe practices is also achievable through the implementation of an information security policy adapted to the school reality, according to ISO 27001.

By collecting opinion from the system stakeholders, it was possible to create two documents with a information security policy, one directed to schools and the other addressed to users. It is believed that the adoption of these recommendations by schools can allow benefits in terms of information security.

Keywords: School; Information Technologies; Policy; Information Security.

Agradecimentos

Gostaria de agradecer ao meu orientador, Doutor António Costa, não só pela sua orientação científica, mas sobretudo pela disponibilidade com que me acompanhou ao longo desta fase de investigação. Aos meus colegas de curso, em especial à Ana Cerqueira e ao Pedro Costa, pelo contributo na execução dos trabalhos e por tantas vezes terem conseguido motivar-me nos momentos de maior pressão. À minha família, por perceberem as minhas constantes ausências ao longo destes dois anos de dedicação ao mestrado. E por último, agradeço a oportunidade que me foi dada de concretizar este sonho, é com grande prazer que me torno diplomada numa instituição de mérito como o ISEP.

Índice

Lista de Figuras

Acrónimos e Símbolos

Lista de Acrónimos

APAV	Associação Portuguesa de Apoio à Vítima
CD	*Compact Disc*
CE	Comissão Europeia
CSE	Catálogo de Software do Estado
CTA	*Certified Trust Analyst*
DGE	Direção Geral da Educação do Ministério da Educação
DGIDC-CRIE	Direção Geral de Inovação e Desenvolvimento Curricular- Equipa de Computadores, Redes e Internet na Escola
DOS	*Denial Of Service*
eNACSO	*European NGO Alliance for Child Safety Online*
FCCN	*Fundação Cientifica para a Computação Nacional*
FCT	Fundação para a Ciência e Tecnologia
FDTI	*Fundação para a Divulgação das Tecnologias da Informação*
HTTPS	*HyperText Transfer Protocol Secure*
ICSEDB	*International Child Sexual Exploitation Image Database*
ICT	*Information and Communication Technology*
IEC	*International Electrotechnical Commission*
IMs	*Instant Messaging*
INHOPE	*Internet Hotlines All Over the World*
IPDJ	Instituto Português do Desporto e Juventude
ISECOM	*Institute for Security and Open Methodologies*
ISMS	*Information Security Management System*
ISO	*International Organization for Standardization*
ISP	*Internet Service Provider*

ITIL	*Information Technology Infrastructure Library*
MAC	*Media Access Control*
MP3	MPEG-1/2 Audio Layer 3
NIDS	*Network Intrusion Detection System*
ONG	Organização Não Governamental
OPSA	*Professional Security Analyst*
OPSE	*Professional Security Expert*
OPST	*Professional Security Tester*
OSSTMM	*Open Source Security Testing Methodology*
OWSE	*Wireless Security Expert*
POG	*European Online Grooming Project*
PTE	Plano Tecnológico da Educação
ROI	*Return On Investment*
SAI	*Security Awareness Instructor*
SGSI	Sistema de Gestão de Segurança da Informação
SIP-BENCH II	*Safer Internet Programme Benchmarking*
SPAM	*spiced ham*
SSID	*Service Set Identifier*
TI	Tecnologias da Informação
TIC	Tecnologias da Informação e Comunicação
USB	*Universal Serial Bus*
VPN	*Virtual Private Network*
WEP	*Wired Equivalent Privacy*
Wi-Fi	*Wireless Fidelity*
WPA	*Wi-Fi Protected Access*
WPA2	*Wi-Fi Protected Access II*

1 Introdução

Este estudo visa aprofundar o nível de segurança da informação nas escolas públicas em Portugal. Inicialmente será feita uma abordagem da evolução tecnológica nas escolas para que depois se possa formular o problema: qual o nível de segurança da informação nas escolas?

O interesse nesta problemática surgiu por estar inserida neste mercado de trabalho e por, ao longo destes últimos anos, observar uma estagnação no que diz respeito à disponibilização de recursos humanos e financeiros que tentem assegurar um nível razoável de segurança.

A ausência de mecanismos de proteção da informação deve-se ao facto de a própria escola ainda não reconhecer o valor que a informação representa no exercício das suas funções.

1.1 Enquadramento temático

A questão da segurança nas redes informáticas é uma problemática atual e em constante desenvolvimento. Ao longo da dissertação serão apresentadas várias soluções que implementam segurança nos recursos, no entanto é necessário o envolvimento e a atribuição de responsabilidades a todos os intervenientes.

Os projetos da ISECOM e do programa *Safer Internet* ajudam a criar comportamentos seguros nos utilizadores através da consciencialização para as necessidades de segurança. São disponibilizados materiais e exercícios práticos que podem ser aplicados durante as aulas, estimulando o desenvolvimento do pensamento crítico nos alunos. Mas estas iniciativas apenas ajudam a tornar os utilizadores mais conscientes para a necessidade de segurança, contudo a rede continua exposta aos mais diversos perigos.

A solução passa por implementar um sistema de gestão de segurança da informação que seja capaz de diminuir os riscos associados à utilização das TI. As ferramentas de gestão ITIL e Cobit são uma alternativa para implementar um sistema caracterizado pelas melhores

práticas, no entanto parece um pouco desajustado para a realidade que as escolas públicas enfrentam no nosso país.

A Norma ISO 27001 é o standard para a segurança da informação e pode ser implementada por qualquer organização que pretenda garantir elevados níveis de segurança através da proteção da informação. Serão apresentados os principais componentes da norma e de que forma as escolas podem inseri-la no seu quotidiano. A certificação no *Esafety School* é outra alternativa que as escolas devem considerar, sendo apresentada uma breve descrição sobre este projeto.

1.2 Objetivos

De modo a oferecer uma solução adequada à realidade das escolas foi feito um estudo através da aplicação de um questionário a professores. Os dados provenientes deste estudo serão apresentados e considerados para a solução a implementar. A realidade dos alunos foi também considerada, tendo sido analisado o relatório do projeto *EUKidsOnline* com o objetivo de conhecer os perigos que os jovens enfrentam ao utilizarem a Internet e as novas tecnologias.

Após analisar estes resultados, é apresentada uma proposta de implementação de uma política de segurança da informação através de um modelo de gestão e de um conjunto de recomendações direcionadas aos alunos.

A metodologia seguida responde aos requisitos da ISO 27001 para implementar um sistema de gestão da segurança da informação e na seleção de controlos de segurança da ISO 27002.

1.3 Organização da tese

Este documento está organizado em 8 capítulos:

- O capítulo 1 é a introdução, onde se pretende fornecer uma ideia geral da dissertação;
- No capítulo 2 são apresentados tópicos fundamentais de segurança que serão utilizados ao longo do trabalho;
- O capítulo 3 pretende contextualizar sobre o estado geral da segurança da informação nas escolas, sendo feita uma análise à legislação, por fim apresentamos projetos que interagem com as escolas na promoção da segurança da informação;
- No capítulo 4 é feita a análise do problema, tendo em conta a recolha de informação dos intervenientes do sistema;
- No capítulo 5 são apresentadas algumas soluções de gestão da segurança da informação;

- Já no capítulo 6 é feita a proposta de solução para os problemas de segurança da informação detetados nas escolas;
- No capítulo 7 são apresentadas as conclusões e no capítulo 8 as referências consultadas.

2 Tópicos de segurança

Antes de iniciarmos o desenvolvimento do trabalho, serão apresentados alguns conceitos chave de segurança que serão amplamente utilizados ao longo da dissertação.

A **segurança da informação** consiste na preservação dos dados iniciais, incluindo os mecanismos que garantam a sua proteção e assegurem as características da segurança da informação - a disponibilidade, a integridade, a confidencialidade e a autenticidade, entre outras.

- A **disponibilidade** garante que a informação está disponível para a pessoa certa, no momento em que ela precisar, prevenindo a perturbação. A disponibilidade pode ser garantida através da implementação de mecanismos de redundância e de salvaguarda da informação.

- A **integridade** consiste em prevenir a alteração não autorizada de dados, mantendo as características que o proprietário da informação estabeleceu. Pode ser obtida através de mecanismos de deteção de intrusão e controlos de acesso.

- A **confidencialidade** garante que existe o nível adequado de secretismo em cada nó de processamento, prevenindo as fugas de informação. Pode ser obtida através de comunicações seguras e encriptação de dados (guardados e transmitidos).

- A **autenticidade** é obtida quando o sistema tem condições para verificar a identidade dos atores e entidades do sistema.

Segundo a ISO 27001 um **Ativo** é qualquer coisa que tenha valor para a organização, por isso a **Informação** é um ativo tão importante no seio da empresa como qualquer outro, devendo ser usados mecanismos para a proteger.

Alguns fatores podem alterar as características da segurança, tais como as ameaças, as vulnerabilidades, o risco e os ataques.

- A **ameaça** pode ser qualquer evento que provoque um impacto negativo sobre a confidencialidade, integridade ou disponibilidade da informação ou do sistema, causando prejuízos nos ativos da empresa. As ameaças podem ser naturais (causadas pela natureza) ou intencionais (vírus de computador, espionagem, fraude, vandalismo, etc.).

- **Vulnerabilidade** é uma falha, um erro na aplicação, que origina uma violação da política de segurança e que pode ser explorada propositadamente. As vulnerabilidades do sistema podem ser de diversos tipos, tais como condições físicas, humanas, hardware, software, meios de armazenamento e meios de comunicação.

- O **risco** está relacionado com a possibilidade de uma ameaça corromper a informação, através da exploração de uma vulnerabilidade que o sistema possui. Para se poder determinar o risco, é necessário identificar as vulnerabilidades.

- Um **ataque** consiste na exploração de uma falha no sistema informático, normalmente com a intenção de o prejudicar.

2.1 Exemplos de ataques à segurança

Um **vírus** é um programa que tem como finalidade infetar o computador e corromper o sistema operativo. Os vírus costumam agregar-se a um programa instalado no computador e têm como característica a rápida replicação.

O **cavalo de troia** ou trojan é um programa malicioso (malware) no computador com a função de o destruir. Difere do vírus no sentido em que este não se replica, tendo como função invadir o computador do utilizador para roubar informação, como por exemplo senhas de acesso.

O **SPAM** diz respeito à receção de correio eletrónico não solicitado, por norma é enviado a um grande número de pessoas e costuma abordar temas socialmente relevantes. O SPAM é usado habitualmente como veículo para lançar ataques à segurança.

Esquemas fraudulentos são praticados, na maioria da vezes, por email, sendo o principal alvo os utilizadores que utilizam sites de instituições financeiras. O atacante recorre a listas de endereços de correio eletrónico para enviar SPAM em grande escala, com ficheiros executáveis anexados às mensagens e serviços de hosting gratuitos. O utilizador envia mensagens de correio eletrónico a outros utilizadores, fazendo-se passar por bancos ou outras instituições financeiras, solicitando dados pessoais como número de conta, número de cartão bancário e palavras passe. A vítima, não reconhecendo que está a ser alvo de um esquema fraudulento, envia estes dados e a partir daí muitos outros crimes podem ocorrer.

O **Cyberbullying é** um fenómeno em constante desenvolvimento e refere-se ao ato de ameaçar ou humilhar uma criança e/ou adolescente através do recurso às tecnologias da informação (email, redes sociais, telemóvel, etc.). O cyberbullying consiste em:

- ameaçar e perseguir a vítima,
- roubar a identidade e palavras passe,
- criar páginas de perfil falsas,
- usar blogues de forma abusiva,
- enviar imagens quer por email, quer por telemóvel,
- utilizar sítios de votação com o objetivo de incomodar e humilhar a vítima,
- fazer inscrições em sites utilizando os dados da vítima.

O **phishing** é outro tipo de ataque frequente, tem como objetivo o roubo de identidade dos utilizadores, mas também pode infetar o computador com vírus e/ou levar os utilizadores a participar em esquemas fraudulentos.

Neste tipo de ataque são utilizados vários métodos que levem o utilizador a revelar dados pessoais e confidenciais (número de cartão de crédito, informação sobre contas bancárias, palavras passe, etc.) Para o conseguir, os atacantes fazem-se passar por entidades fidedignas tais como o banco, o ISP, um serviço de pagamento ou mesmo organismos do governo, e ameaçam o utilizador, por exemplo, com o cancelamento de conta, no caso de não atualizar os dados que estão a ser solicitados.

No momento em que o utilizador segue a hiperligação para outra página, aparentemente inofensiva, passa a ser alvo de phishing. O atacante consegue filtrar os dados que o utilizador digita para que posteriormente possa roubar a identidade, debitar contas em nome do utilizador ou cometer outro tipo de crime.

O **roubo de identidade** consiste em obter de forma ilegal dados pessoais de outro utilizador, como o nome e palavra passe, informações bancárias, número de cartão de crédito, de forma a usurpar a identidade.

Engenharia social é o conjunto de técnicas usadas pelos atacantes com o objetivo de persuadir o utilizador a divulgar informações pessoais, a executar programas maliciosos, etc.

3 Segurança da informação nas escolas

O nível de tecnologia associado às escolas públicas de Portugal era, até há pouco tempo, bastante obsoleto. Sob a legislação do antigo Governo, em 2007, foi levado a cabo o maior programa de modernização tecnológica das escolas portuguesas, o PTE.

Com a finalidade de melhorar as competências TIC em alunos e professores e preparar as gerações futuras para os desafios da sociedade do conhecimento, o PTE contribuiu para o enriquecimento da infraestrutura tecnológica das escolas através da cedência de conteúdos e serviços em linha. Esta restruturação tecnológica colocou-nos entre os 5 países com escolas tecnologicamente mais modernizadas, a nível europeu [PTE, 2009].

Para além de promover a ligação à Internet em banda larga de alta velocidade, o programa tentou diminuir o número de alunos por computador com ligação à Internet e, por fim, aumentar o número de docentes com certificação TIC.

De referir que com este programa as escolas passaram a ter:

- 2 alunos por computador nas salas de informática;
- 1 computador para o professor em cada sala de aula;
- 1 vídeo projetor por sala de aula;
- 1 quadro interativo por cada 3 salas de aula.

O projeto “Internet na sala de aula”, do programa PTE, foi criado com vista a disponibilizar acesso à Internet em todas as salas de aula e em todos os espaços escolares através de uma infraestrutura de redes locais estruturadas e certificadas. O Ministério da Educação forneceu os componentes ativos de rede e todo o sistema de cablagem estruturada (cabos, bastidores, calhas, etc), bem como o serviço de instalação e de configuração inicial dos equipamentos.

3.1 Formulação do problema

Houve uma grande preocupação da parte do anterior Governo em equipar as escolas com equipamentos que permitissem, a alunos e professores, acesso às novas Tecnologias da Informação e Comunicação, dentro e fora da sala de aula. Os professores passaram a ter na sala de aula um computador e um vídeo projetor para lecionar os conteúdos. Já os alunos passaram a ter acesso a estes equipamentos nas salas de informática e na biblioteca para realizar trabalhos, mas também para fazer outro tipo de pesquisas.

Antes de este programa ser levado a cabo, muitas escolas funcionavam de forma muito primitiva, existindo situações caricatas, como por exemplo professores que tinham a seu cargo disciplinas de informática mas em que as mesmas só podiam ser ensinadas na teoria devido à inexistência de equipamento. Esta reestruturação veio facilitar, por um lado, o trabalho do professor, dando-lhe a possibilidade de fazer o seu trabalho tendo meios disponíveis para lecionar devidamente os conteúdos e promover a interação na sala de aula. Por outro lado, os alunos passaram a ter à sua disposição meios que facilitam a aprendizagem.

Estas crianças e jovens passaram a ter acesso, nas escolas, a computadores e Internet, uma realidade a que muitos só têm acesso dentro da própria escola. A escola passou a ter a missão de formar os seus alunos, utilizando técnicas que fomentem a utilização das TIC e estimulem a literacia digital.

3.2 Contexto

Uma vez resolvido o problema da falta de equipamento, surge agora uma nova questão: como gerir estes recursos?

Na prática, nas escolas públicas o acesso aos computadores é feito da seguinte forma. Os computadores estão disponíveis nas salas de aula, biblioteca, ludoteca e clubes. Para aceder ao sistema é necessário autenticação, havendo duas contas: alunos e professor[1]. O perfil de utilizador é partilhado por todos os utilizadores que fazem parte do mesmo grupo (aluno ou professor), sendo o nome e a palavra passe comum. Esta configuração faz com que todos os utilizadores tenham acesso à informação guardada no computador, por exemplo, ficheiros, histórico da web, palavras passe para aceder a sítios Web, ficheiros na reciclagem, etc.

Por norma os programas antivírus estão desatualizados e não existem restrições para o armazenamento de ficheiros. É muito fácil para um aluno fazer a propagação de vírus, eliminar um ficheiro que outro aluno acabou de criar e que por lapso não gravou, utilizar ficheiros e dados de outro utilizador, entre outras possibilidades.

[1] Nesta pesquisa não será considerado a vertente administrativa, ou seja o acesso dos funcionários da secretaria

Estas características, aliadas à falta de competências na área da segurança que os alunos manifestam, tornam o sistema ainda mais vulnerável e comprometem os princípios da segurança da informação: a confidencialidade, a integridade, a disponibilidade e a autenticidade.

A título de exemplo passamos a explicar de que forma é que estes princípios relacionados com a segurança da informação podem ser violados.

Confidencialidade: É impossível garantir a confidencialidade da comunicação/informação num sistema com estas características. Um utilizador pode ter acesso aos ficheiros descarregados por outro utilizador e que ficaram armazenados nos ficheiros temporários do computador, ou nos itens eliminados na pasta da reciclagem; é também frequente encontrar janelas de sistemas de comunicação instantânea abertas com conversas entre utilizadores, etc.

Integridade: estes sistemas não garantem a integridade da informação, pois muitas vezes alunos e professores, por distração, guardam os ficheiros no computador, estando estes disponíveis para quem queira poder usufruir deles. Torna-se fácil alterar informação de outrem e fazer dela o que bem entender.

Disponibilidade: Qualquer pessoa tem acesso aos ficheiros guardados no computador, se por acaso um utilizador se tiver esquecido de gravar um documento, quando voltar ao computador para o fazer, corre o risco de o mesmo já não estar disponível. A facilidade com que um vírus se pode propagar neste tipo de sistema também pode colocar em causa a disponibilidade da informação e do próprio sistema. A disponibilidade fica ainda mais comprometida por não se realizarem outras cópias à informação.

Autenticidade: ao não ser exigido um login para cada utilizador que queira aceder ao sistema, a garantia de autenticidade não existe, pois não há forma de comprovar quem está a aceder ao sistema. Ao utilizar a Internet é frequente o pedido de autenticação em vários sítios Web, ficando muitas vezes estes dados armazenados no computador. Muitos sítios Web perguntam ao utilizador se pretende que o browser memorize o utilizador e a palavra passe, ou se quer manter a sessão iniciada, sendo que os utilizadores respondem frequentemente que sim. Isto dá origem a que muitas vezes, ao abrir uma página de um servidor de email ou de uma rede social, esta seja aberta com a conta de outro utilizador que esteve com sessão iniciada. Nestas situações, todos os princípios da segurança podem ser violados.

Para evitar estas falhas, a escola deve gerir a segurança através de atividades adequadas, que começam por uma avaliação do risco e devem resultar numa política de informação e procedimentos de segurança da informação.

3.3 Análise da legislação

Neste ponto pretende-se analisar a legislação produzida que regulamenta a segurança da informação e a rede local da escola. Após pesquisa da legislação disponível no sítio Web do Ministério da Educação, rapidamente se chegou à conclusão que a legislação produzida apenas contempla o programa PTE nas escolas, o ensino das TIC e a atribuição de certificações a professores [Min-edu, 2010].

No entanto, analisando a legislação com mais pormenor, foram recolhidos elementos importantes e que podem ajudar a compreender o estado atual de segurança da informação.

O PTE ficou aprovado pela Resolução de Ministros nº 137/2007, em que o Governo se propôs a contribuir para a escola do futuro, através da criação de condições de ensino e de aprendizagem, apoiando a utilização das Tecnologias da Informação e Comunicação nos processos de ensino e aprendizagem, bem como a gestão e segurança escolar.

Os equipamentos, oriundos do programa PTE, foram distribuídos pelas escolas, tal como se pode verificar na Resolução do Conselho de Ministros n.º 118/2009, em que ficou autorizada a entrega de 250 000 computadores portáteis, bem como a instalação de serviços conexos.

A Portaria n.º 732/2008 determina a aquisição, por parte do Ministério de Educação, de bens e serviços que assegurem nas escolas públicas (2º e 3º ciclo e secundárias) a instalação, manutenção, suporte e gestão de redes locais.

Já a Resolução do Conselho de Ministros n.º 35/2009 determina a atribuição de verbas para a celebração de acordos que permitam a construção do Sistema de Informação da Educação, nomeadamente para serviços de consultoria e desenvolvimento de tecnologias da informação e de serviços de suporte técnico e gestão operacional.

Foi ainda analisado o *manual de utilização, manutenção e segurança nas escolas*, documento emitido pelo Ministério da Educação, com um breve capítulo dedicado aos equipamentos audiovisuais e informáticos, mas não contemplando qualquer aspeto relacionado com a segurança informática. Apenas emana diretrizes sobre o controlo e verificação de cabos, fichas, instalações elétricas, questões climatéricas, etc. [Min-edu, 2003]

Visando consultar um documento de apoio à gestão da rede informática, foi encontrado um outro manual, emitido pelo Ministério da Educação, o *Manual de Cópias de Segurança*, que alerta para a necessidade de realizar backups dos documentos informatizados [Ramos, 2011].

Uma vez que este ministério tem uma linha de apoio, foi efetuado um contacto no sentido de apurar se existe legislação relativa à gestão e configuração das redes locais das escolas. A informação transmitida correspondeu àquilo que já se previa, isto é, não existe legislação produzida sobre esta matéria. Quando há verbas disponíveis, muitas vezes a própria escola recorre a empresas externas que possam assegurar a manutenção do equipamento.

O PTE equipou as escolas com equipamento tecnológico (computadores, vídeo projetores, quadros interativos), equipamento ativo e passivo de rede e disponibilizou verbas para assegurar a instalação e a configuração inicial dos equipamentos. Criou as condições necessárias para que cada escola tenha uma rede local funcional, no entanto a sua manutenção fica a cargo da própria escola. Para cumprir os requisitos mínimos de segurança, é necessário gerir a rede e implementar mecanismos de autenticação, criação de diferentes controlos de acesso, separação de redes distintas, etc.

Como as escolas não têm pessoal técnico que possa assegurar os requisitos de segurança que uma rede desta dimensão exige, supõe-se que cada escola recorra a uma empresa que assegure a manutenção do sistema. Esta despesa deve ser suportada pela própria escola, que através das fontes de receita próprias (verbas do refeitório, reprografia, aluguer de equipamento, etc.) deve financiar a manutenção destes serviços. [Min-edu, 2008]

Raramente isto acontece, as verbas que sobram são muito reduzidas e servem para cumprir outras prioridades identificadas pelos órgãos de gestão, que passam por:

- aquisição de livros pela biblioteca,
- compra de livros e dicionários para que os diferentes departamentos possam acompanhar as reformas curriculares,
- aquisição de material necessário para o desenvolvimentos da atividade da escola, etc.

As questões relacionadas com a manutenção e segurança da rede informática muito raramente são encaradas como uma prioridade pela gestão da escola.

Para colmatar esta lacuna, as escolas atribuem estas funções aos professores de informática para que durante as horas que têm de trabalho na escola tentem efetuar as tarefas de gestão de equipamento. As escolas podem ainda nomear um professor, diretor de instalações, com a função de coordenar a gestão informática do equipamento, e podem ainda designar uma equipa técnica de professores de informática com horas dedicadas ao gabinete e que tenham como funções:

- verificar o material,
- inventariar o hardware que está disponível,
- assegurar a sua manutenção e reparação de material,
- verificar o software que está instalado nas máquinas,
- dar apoio a utilizadores, etc.

Atualmente, poucas são as escolas que atribuem horas aos professores de informática para gestão do equipamento. Esta manutenção é necessária e a longo prazo representa uma mais-valia para a escola, pois com uma configuração apropriada e uma manutenção regular o equipamento tem uma durabilidade maior e consegue-se adicionar segurança na utilização dos recursos.

Existe ainda pouca sensibilidade por parte da gestão das escolas para esta problemática. As escolas são dirigidas por professores que podem ser de qualquer área curricular e que muitas vezes desconhecem os perigos da inexistência de uma política de segurança da informação.

3.3.1 O Futuro das TIC na Administração Pública

Os organismos públicos são dotados de autonomia para a aquisição e gestão das suas infraestruturas tecnológicas, tendo liberdade para adquirir e contratar comunicações, bem como para criar departamentos para a gestão e manutenção das TIC [Vasconcelos, 2011]. A Agência para a Modernização Administrativa I.P. disponibiliza as despesas que cada ministério teve com as TIC durante o ano 2010, a saber:

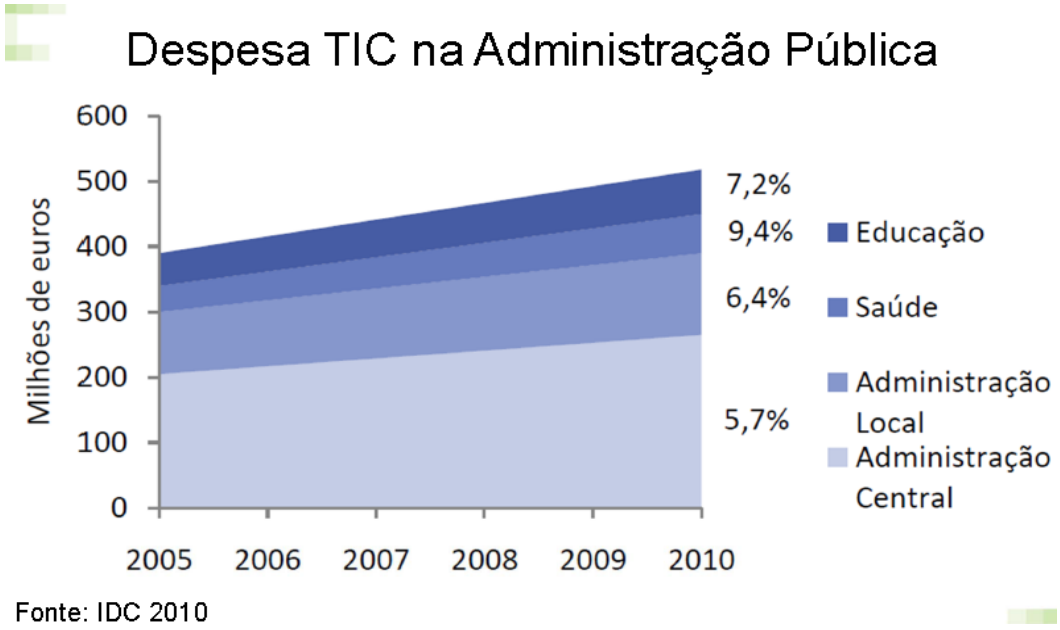

Figura 1 - Despesa com as TIC na Administração Pública, durante o ano de 2010

Observando o gráfico da figura 1, pode-se concluir que o Ministério da Educação foi o que apresentou uma despesa mais elevada com as TIC no ano de 2010: cerca de 520 milhões de euros. De realçar ainda que todos os ministérios tiveram um acréscimo nesta rubrica, até 2010.

Numa altura em que a redução de despesas faz parte das medidas estratégicas do Governo, também as TIC são alvo deste ajustamento. As medidas apresentadas em 2012 para racionalizar despesa, no âmbito das TIC, são: [DRE, 2012]

- Racionalizar a função informática sectorial - consiste em centralizar as funções de informática num único organismo por ministério, de modo a proporcionar uma melhor articulação com as políticas da sociedade de informação;
- Avaliar projetos TIC - Consiste em avaliar previamente custo/benefício antes de um investimento;

- Catalogar, uniformizar e partilhar software - ao ser criado um Catálogo de Software do Estado (CSE) é possível disponibilizar e reutilizar software desenvolvido pelo Estado;
- Adotar software aberto nos sistemas de informação do Estado - sempre que o software apresente maturidade e um benefício em termos de custo, deve-se apoiar a utilização de software aberto na administração pública.
- Racionalizar comunicações e interoperabilidade através da utilização da plataforma de interoperabilidade desenvolvida pela AMA.
- Racionalizar centros de dados através da implementação de soluções de cloud computing.

De acordo com o exposto, concluímos que seria vantajoso que o Ministério da Educação, à semelhança de outros ministérios, tivesse um organismo onde estivessem centralizadas competências de regulamentação e de apoio no âmbito das novas Tecnologias da Informação. Como exemplo, podemos referir o Instituto de Informática do Ministério das Finanças, cujas competências passam por definir estratégias e políticas no âmbito das Tecnologias da Informação e Comunicação. Achamos oportuno transcrever a declaração de missão[2] deste instituto:

"O Instituto de Informática tem por missão apoiar a definição das políticas e estratégias das tecnologias de informação e comunicação (TIC) do Ministério das Finanças e da Administração Pública (MFAP) e garantir o planeamento, concepção, execução e avaliação das iniciativas de informatização e actualização tecnológica dos respectivos serviços e organismos, assegurando uma gestão eficaz e racional dos recursos disponíveis." [inst-informática, 2007]

As escolas veriam muitos dos seus problemas de gestão informática resolvidos se fosse criado um organismo, pelo Ministério de Educação, com funções de planeamento e definição de políticas de segurança da informação. Para além de definir regras e procedimentos a implementar, este organismo deveria usar uma correta articulação com as escolas e promover palestras de sensibilização dos utilizadores para esta temática.

3.4 Programas de apoio às escolas

Esta massificação, na utilização das TIC, veio modificar profundamente a forma como as pessoas aprendem, trabalham e pesquisam informação. Desde o aparecimento da Internet têm sido estudadas as mais variadas formas que possam fazer frente aos ataques à segurança através da criação de mecanismos eficazes de prevenção de ataques.

[2] http://www.inst-informatica.pt/o-instituto

Por um lado, as escolas, nestes últimos anos, foram equipadas com equipamento tecnológico (computadores, etc), por outro lado a FCCN garante a ligação à Internet nas instituições de ensino público e superior. A escola passa a ser um meio privilegiado para a disseminação dos mais variados perigos, pois alia uma rede interna insegura às possibilidades de ataque existentes na Internet.

A questão da segurança na Internet, sobretudo no que concerne aos mais jovens, tem sido amplamente discutida, tendo já surgido programas que tentam consciencializar as pessoas para a necessidade de implementar mecanismos online mais seguros.

Atenta a este problema, a **Comissão Europeia** lançou em 1999 o *Safer Internet Programme*, que tem como foco a dinamização de projetos nos Estados Membros no âmbito da promoção de uma utilização mais segura da Internet pelos mais jovens.

A **ISECOM** é uma organização internacional sem fins lucrativos, com projetos dedicados a metodologias de utilização Open Source e à segurança, que tem como missão "*Make sense of security*" promovendo a segurança através de certificações, programas de treino e suporte a projetos.

Os projetos levados a cabo, no que diz respeito à segurança online, pela ISECOM e pela Comissão Europeia serão brevemente descritos.

3.4.1 Projetos ISECOM

O *Institute for Security and Open Methodologies*, criado em 2001 e presente nos EUA e em Espanha, representa uma comunidade colaborativa com milhares de membros voluntários em todo o mundo. Consciente dos problemas adjacentes à falta de segurança nos recursos informáticos, a equipa ISECOM tem em curso vários projetos de apoio a escolas, professores, alunos e quaisquer interessados neste tema. [ISECOM, 2012]

Figura 2 - Símbolo ISECOM

Os projetos levados a cabo pela equipa ISECOM, que se apresentam de seguida, são:

A. OSSTMM (Open Source Security Testing Methodology Manual)

Standard em metodologia e testes de segurança que consiste em verificar factos e em medir o nível de segurança do sistema. O teste à segurança é feito com base nas decisões tomadas por cada organização, sendo implementada uma metodologia formal que comprova se as ferramentas usadas realmente protegem o sistema, através de testes de penetração e exploração de vulnerabilidades. Especialmente direcionado a auditores, consultores e

profissionais de segurança, tem a vantagem de ser gratuito, no entanto o facto de estar em constante desenvolvimento faz com que não haja uma versão final.

A ISECOM promove certificações em profissionais em que as competências são validadas através do programa de treino e do exame final. As certificações disponíveis são:

- Professional Security Tester (OPST) - certificação para auditores de rede e para profissionais responsáveis por realizar testes de segurança (em aplicações locais e aplicações web) e testes de intrusão na intranet.
- Professional Security Analyst (OPSA) - certificação destinada a analistas de segurança da informação (analisam dados de segurança de rede, avaliam a segurança e tomam decisões em áreas críticas da gestão).
- Wireless Security Expert (OWSE) - certificação para auditores de segurança em comunicação wireless, através do protocolo 802.11.
- Certified Trust Analyst (CTA) - certifica o profissional e a organização que demonstra ter a capacidade de tomar decisões rápidas com base em evidências e gestão do risco.
- Professional Security Expert (OPSE) - certificação oficial em OSSTMM, oferece uma metodologia completa sobre a realização de testes de segurança de fora para dentro da rede.
- Security Awareness Instructor (SAI) - esta certificação habilita o profissional para o ensino de "Hacker High School" ou "smarter safer better". Assegura que o profissional possui determinadas competências tais como conhecimento, ética e responsabilidade no ensino de segurança.

B. Bad People Project

O projeto ***Bad People*** pretende desenvolver nos mais jovens a consciência de segurança na Web e a necessidade de criação de regras. Neste projeto são incentivadas crianças, de qualquer parte do mundo, a colaborar através do envio de um desenho que demonstre qual a imagem que têm das pessoas más e assustadoras. Os desenhos devem ser submetidos no sítio Web da *ISECOM.*

C. Hacker High School

Atualmente, os jovens estão expostos a um grande número de comunicações, faltando-lhes muitas vezes o conhecimento de como evitar fraudes, roubo de identidades e outros tipos de ataques praticados através da Internet [HHS, 2012]. O projeto **Hacker High School** tem como principal finalidade promover a segurança através do desenvolvimento do pensamento crítico nos jovens, levando-os a pensar como um Hacker.

O HHS disponibiliza suportes materiais a professores e alunos com recomendações sobre privacidade na Web e em chats, informação sobre malware (vírus e trojans), dicas sobre como reconhecer problemas no computador, etc. As fichas de trabalho estão disponíveis no sítio Web do HHS e qualquer utilizador pode descarregá-las, no entanto para ter acesso ao laboratório de testes e a um instrutor é necessário obter licença.

Todos os trabalhos do HHS são desenvolvidos para fins não comerciais e destinam-se a apoiar a formação de alunos dos vários tipos de ensino:

- As escolas têm licença livre para uso de recursos e acesso total ao laboratório HHS;
- Para o ensino individual de HHS, fora das escolas, é possível obter a licença por 150USD. Válida por um ano, a licença dá acesso aos recursos e ao laboratório;
- Para uso pessoal: apenas é possível ter a licença gratuita nos materiais, sendo o acesso aos laboratórios proibido por questões de segurança.

D. Safer Better

A equipa ISECOM organiza diversos seminários gratuitos que visam promover a segurança através da demonstração, com exemplos práticos, das desvantagens decorrentes da ausência da segurança nas escolas, no trabalho e na vida. Têm a finalidade de educar, informar e causar impacto nos participantes, tentando passar uma mensagem forte e recorrendo às técnicas de aprendizagem dos programas. Os seminários podem ser feitos em escolas, universidades, clubes ou comunidades e têm duas variantes: seminários académicos e seminários dirigidos à comunidade em geral.

3.4.2 Safer Internet Programme

O programa *Safer Internet*, desenvolvido pela Comissão Europeia e presente em todos os Estados Membros, assenta na promoção de vários projetos com o objetivo de proteger crianças e jovens dos perigos da Internet. Para alcançar este objetivo, o programa definiu uma política robusta que consiste essencialmente em tornar a Internet um local mais seguro para os jovens, ativando vários mecanismos que permitem lutar contra conteúdos e condutas ilegais. O programa financia a criação de plataformas seguras para os mais jovens (portal **Insafe** e o portal **Inhope)**, patrocina o evento anual (o *safer internet day)* e organiza o *safer internet fórum*. [EC, 2012a]

Os projetos levados a cabo pelo programa *Safer Internet* passam, entre outros, pela criação de ***Safer Internet Centres***. Presentes em 30 países Europeus, os Centros de Internet Segura têm a finalidade de produzir informação sobre segurança na utilização da Internet, facultando material a crianças, professores e pais.

Para garantir que a política de **luta contra conteúdos ilegais** é levada a cabo, cada centro possui uma linha de apoio que os utilizadores devem contactar para denunciar conteúdo ilegal.

Com o objetivo de prevenir abusos sexuais a menores, existe uma cooperação com a INTERPOL, nomeadamente ao nível do acesso à Base de Dados Internacional de Imagens de Crianças Abusadas Sexualmente (ICSEBD). A base de dados pode ser acedida por investigadores credenciados, independentemente da sua localização geográfica, os quais podem contribuir na identificação das vítimas e na redução de investigações redundantes, o que contribui para uma partilha de informação mais eficaz.

O programa financia projetos de benchmarking, que permitem a criação de **ferramentas de filtragem e etiquetas de conteúdo**, como é o caso do SIP-BENCH II. Pais e professores passam a ter acesso a uma panóplia de ferramentas de controlo que permitem limitar o acesso a conteúdos online não apropriados.

Outra medida consiste em **providenciar o conhecimento** através do financiamento de dois projetos com a finalidade de criar uma base de conhecimento que identifique riscos e perigos online para crianças.

- *EU Kids Online* é um projeto disponível em 21 países que visa conhecer padrões de utilização das crianças europeias, identificando riscos e quantificando a segurança online.
- O POG (European Online Grooming Project) tem como finalidade compreender o comportamento de pessoas que tentam aliciar jovens através da utilização das TI.

O **envolvimento da sociedade civil** é fundamental para que o programa responda adequadamente aos desafios e é assegurado através da recolha de opinião dos diversos intervenientes. A sociedade civil é representada pelos jovens que integram os Centros de Internet Segura de cada país.

Foi ainda criada a **eNACSO** (European NGO Alliance for Child Safety Online), uma ONG que tem como missão defender os direitos das crianças em matéria de segurança na Internet, em toda a União Europeia.

Por último, o programa disponibiliza 2 portais referentes aos projetos em questão:

O **INHOPE** permite ao utilizador fazer anonimamente o reporte de conteúdos ilegais na Internet como é o caso de material de abuso sexual infantil. Cada país tem o seu próprio portal INHOPE que em Portugal corresponde à Linha Alerta.

Figura 3 - Projeto INHOPE

Insafe é a rede europeia que financia a criação de centros que promovem a segurança no uso da Internet e na utilização de dispositivos móveis, em todos os Estados Membros. O portal Insafe providencia um acesso rápido aos serviços da rede e aos centros disponíveis em cada país (Insafe, INHOPE e o painel de jovens). [EC, 2012b]

Figura 4 - Projeto Insafe

Por exemplo ao escolher **Portugal** é-nos devolvida a indicação, e respetivas hiperligações, dos Centros de Internet Segura a atuar no nosso país, sendo estes:

- SeguraNet: direcionado à comunidade escolar;
- Internet segura: direcionado ao público em geral;
- Inhope Hotline: linha alerta utilizada para reportar conteúdos ilegais.

A. Coalition

A 1 de Dezembro de 2011, em Bruxelas, foi criada uma ***Coalition***, uma aliança entre a CE e 28 empresas em que estão incluídas várias empresas ligadas à tecnologia (Google, Apple e Facebook) com o objetivo comum de tornar a Internet um local mais seguro para as crianças. As empresas que formam a *Coalition* assumiriam o compromisso de, ao longo de 2012, agirem em 5 domínios [EC, 2011]:

- Criação de ferramentas simples e robustas para que os utilizadores possam reportar contactos e conteúdos perigosos,
- Permitir configurações privadas apropriadas à idade,
- Classificação do conteúdo mais eficaz,
- Possibilitar mais disponibilidade e controlo paternal,
- Mitigar material de abuso infantil.

Na declaração de missão da *Coalition*, cujo título é "*A Better Place for Kids*", é possível verificar quais os propósitos desta coligação, podendo-se resumir ao próprio título- tornar a Internet um local mais seguro para as crianças. As empresas que formam esta *Coalition* comprometem-se a lutar por este objetivo, trabalhando em conjunto, mas tomando iniciativas individuais que proporcionem o progresso nesta área e ajudem a alcançar os 5 domínios identificados. Financiado pelo Programa *Safer Internet*, a *Coalition* apela à colaboração dos pais, familiares, professores, educadores e toda a sociedade para alcançar as metas identificadas com maior eficácia.

Uma vez que seria demasiado exaustivo enunciar quais as empresas e que medidas levaram a cabo no âmbito do seu envolvimento na *Coalition*, a título de exemplo serão apresentados o Google e o Facebook. De referir que todas elas disponibilizam no seu sítio Web informação relativa a segurança na Internet, tipos de ataques mais comuns e que medidas as pessoas podem tomar de forma a evitar este tipo de ataques.

O Facebook identifica a sua integração na *Coalition* como a sua mais recente iniciativa de participação na Europa, tendo sido assinado o *European Safer Social Networking Principles* e criadas ferramentas de tecnologias da informação e comunicação bem como serviços que ajudem a promover a utilização segura dos serviços online, disponibilizando ligações para os seguintes recursos: [Facebook, 2012]

- Padrões de comunidade do Facebook: Aqui o utilizador tem acesso aos padrões aceitáveis de liberdade de expressão definidos pelo Facebook. O Facebook identifica como principal prioridade a segurança. No caso de esta ser ameaçada sob alguma forma para além da remoção conteúdos, é formalizada uma comunicação às autoridades. O Facebook considera como fora do padrão estabelecido:

  - A violência, as ameaças e condições que coloquem em causa a integridade e a segurança pública,
  - Ameaças de automutilação,
  - Bullying e assédio,
  - Conteúdo que incentive o ódio,
  - Conteúdo gráfico para fins de prazer sádico,
  - Nudez e pornografia,
  - Identidade e privacidade - é proibida a criação de perfis falsos e a divulgação de informação que seja falsa. Também não é permitido revelar informação privada de outra pessoa,
  - Propriedade intelectual - respeitar direitos de autor, marcas comerciais e direitos legais,
  - Phishing e spam.

- Centro de segurança familiar: nesta página é fornecida informação, ferramentas e recursos que ajudem a implementar segurança no Facebook. Tem ainda informação direcionada a pais, professores e adolescentes.

- Denunciar abuso ou violações da política: nesta página é fornecida informação sobre o tipo de ferramentas que o Facebook disponibiliza para os utilizadores denunciarem conteúdos. A forma mais rápida é clicar em “denunciar” em qualquer publicação.

- Informação de definições de privacidade: ensina a implementar privacidade na conta do Facebook, através das publicações, identificações e adição de localização.

O **Google** compromete-se a acompanhar e estimular o desenvolvimento da Web organizando campanhas de alfabetização digital, a mais recente foi a "Bom Saber" organizada em parceria com outras organizações. Disponibiliza ainda a ferramenta *SafeSearch Lock* que dá a possibilidade aos pais de bloquear conteúdo ofensivo e por fim, os *Safety Center* (centros de segurança) disponíveis no youtube permitem reportar ilegalidades de uma forma mais célere. [Google, 2012]

B. SeguraNet

O projeto SeguraNet foi criado em 2004 pela DGIDC-CRIE do Ministério da Educação com a finalidade de promover uma utilização mais segura da Internet junto dos estudantes do ensino básico e do ensino secundário.

Este projeto, direcionado à comunidade escolar (alunos, pais, escolas e encarregados de educação) disponibiliza informações adaptadas a cada tipo de utilizador. No sítio Web é possível ter acesso a material didático e os professores são incentivados a participar nas inúmeras atividades promovidas pela SeguraNet, ao longo de todo o ano letivo.

O painel de Jovens é um dos projetos seguraNet e tem como objetivo escutar a opinião dos jovens, saber como a tecnologia e a Internet são usadas, quais os problemas que surgem e como estes conseguem ser ultrapassados. O objetivo é que a opinião dos jovens seja ouvida e levada em conta aquando o momento de tomada de decisão e programação de novas ações. No painel nacional estão 40 jovens de 4 escolas:

- Escola Básica Integrada Quinta de Marrocos;,
- Colégio St. Peters Schooll,
- Escola Básica de S. Julião da Barra,
- Agrupamento de Escolas de Vagos.

Para além das reuniões realizadas nas escolas, 3 por ano letivo, é esperada a intervenção dos alunos através da plataforma moodle no envio de sugestões.

De modo a quantificar e avaliar os saberes adquiridos pelos alunos em matéria de segurança, a SeguraNet define **metas de aprendizagem** que servem como referencial de objetivos e devem ser verificáveis em todos os níveis de ensino. [Costa, 2010]

As metas estão definidas por grau escolar:

- No final do pré-escolar espera-se que a criança respeite as regras a adotar face aos equipamentos e ferramentas digitais, responsabilizando-se pela sua utilização, como por exemplo ligar e desligar o computador.
- No final do 1º ciclo, para além de saber manusear o equipamento com o devido cuidado, o aluno deve saber o que são os direitos de autor e como os respeitar, bem como as regras de etiqueta on-line (Netiqueta).
- Ao concluir o 2º ciclo o aluno já deve conhecer procedimentos de segurança tais como instalar um antivírus e um firewall, respeitar os direitos de autor e saber utilizar ambientes digitais de acordo com as normas.
- No final do 3º ciclo o aluno já deve reconhecer a existência dos diversos perigos, adotando comportamentos seguros e de boa conduta na WEB.

C. Internet Segura

Fruto do programa LigarPortugal resultou a orientação estratégica "Assegurar a Segurança e a Privacidade no Uso da Internet". Para conseguir cumprir esta estratégia é necessário "garantir que todos, e em particular as famílias, dispõem de instrumentos para protecção de riscos que possam ocorrer no uso da Internet e têm informação sobre como os utilizar".[MCTES, 2005]

Para poder realizar esta orientação nasceu o projeto Internet Segura, em 2007, através de um consórcio coordenado pela FCT **(**Fundação para a Ciência e Tecnologia), onde estão envolvidas a DGE (Direção Geral da Educação do Ministério da Educação) a FCCN (Fundação para a Computação Científica Nacional), o IPDJ (Instituto Português do Desporto e Juventude) e a Microsoft Portugal. [Internetsegura, 2012a]

O projeto **Internet Segura** surgiu como resposta à necessidade de implementar estratégias que possam minimizar os riscos associados à utilização das novas tecnologias da informação, promovendo uma utilização segura da Internet junto da população em geral. [InternetSegura,2012a]

A par das iniciativas europeias, os objetivos estratégicos da Internet Segura são o combate aos conteúdos ilegais, minimizar o efeito que estes conteúdos possam ter nos cidadãos, promover a utilização segura da Internet e, por fim, consciencializar através do fornecimento de informação aos cidadãos dos perigos da ausência de segurança na Internet.

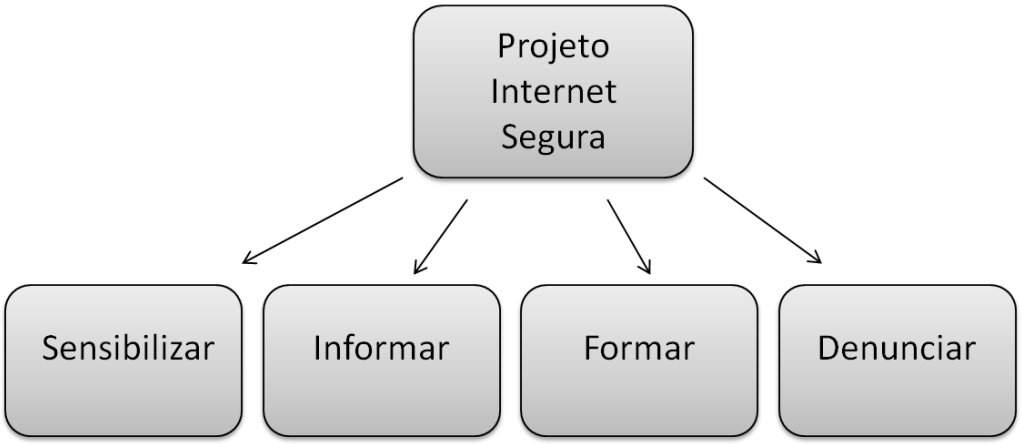

Figura 5 - Linhas de atuação do projeto Internet Segura

De acordo com o que podemos observar na figura 5, as linhas de atuação do projeto Internet Segura são:

- **Sensibilizar** a população para a necessidade de segurança na informática,
- **Informar** sobre os perigos decorrentes da utilização da Internet e de que forma as pessoas se podem proteger,
- **Formar** os cidadãos em geral,
- **Denunciar** através da disponibilização de uma linha de atendimento para onde devem ser feitas as denúncias de conteúdos ilegais na Internet.

Entre os vários apoios e projetos desenvolvidos pela equipa **Internet Segura**, destacamos a **Linha Alerta**. Esta corresponde ao centro INHOPE em Portugal, operacionalizada pela FDTI, presta apoio telefónico a crianças, professores, pais e encarregados de educação no sentido de promover a segurança na Internet. A linha Alerta formou uma parceria com a APAV, sendo um projeto combinado - linha de denúncia e de consciencialização. Este serviço tem como missão o bloqueio de conteúdos ilegais na Internet e a acusação criminal dos seus autores. Para que isto aconteça é feita a comunicação às autoridades policiais portuguesas e é também feita uma comunicação ao ISP para que os conteúdos sejam automaticamente removidos. A linha alerta compreende como conteúdos ilegais:

- Pornografia infantil
- Apologia do racismo
- Apologia da violência

3.5 Conclusão

Ao longo deste capítulo contextualizou-se a problemática da ausência de mecanismos de segurança da informação nas escolas, após a modernização tecnológica na educação ocorrida nos anos mais recentes.

As escolas passaram a ter equipamento que facilita um acesso rápido ao conhecimento tornando-se agora urgente a criação de mecanismos que implementem segurança na rede. A ausência de regulamentação na área da segurança da informação talvez seja o principal motivo para o estado atual de (falta) de segurança nas escolas.

Os projetos desenvolvidos pela ISECOM e pelo programa da Comissão Europeia na área da segurança da informação disponibilizam material teórico e promovem projetos ativos junto das crianças, pais, professores e escolas. Os professores podem utilizar as fichas de trabalho nas aulas de segurança e desenvolver exercícios práticos através do acesso ao laboratório (caso ISECOM) e da participação em testes e atividades (SeguraNet).

Concluímos que uma correta articulação entre as escolas (e seus professores) e as equipas de trabalho (ISECOM, SeguraNet e SaferPlus) estimula a perceção e educação dos utilizadores em segurança da informação.

No entanto o verdadeiro problema continua a existir, o sistema informático da escola continua a ser vulnerável a um grande número de ameaças e não respeita os princípios básicos da segurança da informação, nomeadamente disponibilidade, integridade, confidencialidade e autenticidade.

Compete à escola a criação de manuais de utilização e de apoio ao utilizador que transmitam a política de segurança definida e estimulem a segurança na utilização dos recursos. Seria ainda vantajoso que as escolas começassem a apostar na promoção de palestras e workshops interativos sobre as consequências da falta de segurança da informação e na navegação na Web.

4 Análise do problema

A ausência de mecanismos que garantam a segurança da informação dentro da escola pública assume-se como o problema desta dissertação.

Ao longo deste trabalho aborda-se a segurança da informação e a segurança informática. Estes conceitos, embora interligados, representam objetos distintos. A segurança informática refere-se sobretudo à segurança dos equipamentos e da informação digital, já a segurança da informação contempla toda a informação que é vital para a organização e para o desenvolvimento do negócio, seja em formato digital ou em documento físico. [APCER,2012]

Como atualmente quase toda a documentação é produzida em formato digital, cada vez mais estes termos estão interligados, tornando-se urgente a adoção de medidas que permitam manter o valor original dos documentos, para que sempre que a organização necessite deles, no desenvolvimento das suas atividades, eles estejam disponíveis. Garantir que o documento é íntegro e que só tem acesso a ele quem realmente possui permissão para o aceder são outros requisitos fundamentais. Numa rede informática, onde as barreiras físicas muitas vezes não existem, vulnerabilidades podem ser exploradas de modo a quebrar barreiras lógicas e assim conseguir ter acesso aos mais variados recursos.

A informação continua a ser o bem mais valioso que qualquer organização possui, pois é ela que sustenta o negócio, ajuda no apoio à decisão e fundamenta as opções tomadas.

Decompôs-se o problema da segurança da informação para que seja mais fácil encontrar as devidas soluções:

- Na rede informática das escolas, não estão implementados mecanismos que permitam assegurar a segurança da informação: confidencialidade, disponibilidade, autenticidade e integridade;
- A configuração da rede informática torna-a bastante vulnerável a ataques externos;

- Esta incipiente configuração na rede faz com que ocorram falhas no sistema, o que pode fazer com que software e hardware fiquem mais rapidamente alterados;
- Alunos possuem poucos conhecimentos sobre utilização dos recursos digitais;
- Ausência de segurança na navegação na Internet: os alunos conseguem aceder a todo o tipo de recursos através dos computadores da escola;
- Professores com poucos instrumentos de apoio para promover aulas interativas com recurso à Internet;
- Inexistência de uma política de segurança, devidamente documentada, para apoio de utilizadores;
- Pouco envolvimento das escolas na formação dos utilizadores.

4.1 Requisitos e critérios

O requisito principal é, sem dúvida, atribuir à informação a importância que ela merece no seio da organização. A partir do momento em que a informação é encarada como um recurso valioso a ser salvaguardado, devem ser tomadas iniciativas que melhorem a segurança da informação interna da escola e também a formação dos recursos humanos.

A segurança deve ser analisada em duas vertentes:

- A segurança da informação, através da implementação de mecanismos que acrescentem segurança à informação, criação de políticas, etc.
- A segurança no acesso aos equipamentos e às salas onde estes se encontram, através da criação de regras, atribuição de responsabilidades, etc.

Na rede interna de uma escola circula informação muito variada e a sua importância depende de quem a criou e com que finalidade. Deve-se proceder a uma análise do carater da informação, fazendo sempre que possível uma divisão física e lógica mediante o tipo de utilizador que a produziu.

- A informação com carater de gestão e administrativo, como é o caso dos documentos gerados pela secretaria, devem ser salvaguardados de acessos indevidos;
- Também a documentação que é produzida pelos professores, como é o caso de documentação de gestão de alunos e as atas resultantes de reuniões, devem ter um nível de proteção adequado;
- A documentação produzida pelos alunos possui um valor menos significativo em termos legais.

Importa caracterizar a informação que cada organização produz no decorrer das suas atividades, pois só assim se conseguem perceber quais os fluxos de informação. Depois de analisar a informação que circula dentro de uma escola é importante identificar prioridades para que se comece a agir, em primeiro lugar, na informação que foi identificada como vital para o desenvolvimento das atividades da organização.

Para implementar um plano de ação adequado, convém ainda perceber quais os hábitos que os utilizadores têm na sua interação com o sistema.

4.2 Definição da recolha de informação

Para efetuar uma recolha de informação mais precisa, foi elaborado um questionário no GoogleDocs e distribuído a um universo de 50 professores, sem distinção de grupo disciplinar e nível de ensino, dos quais foram respondidos 19. O questionário é anónimo, não havendo nada que identifique nem caracterize quem o respondeu. Optou-se por um questionário de resposta rápida, com poucas questões, de modo a conseguir obter o máximo de respostas possível num intervalo de tempo curto.

Foi feita uma outra recolha de informação, usando os dados do relatório do projeto europeu "EUKIDS Online", que visa retratar o comportamento dos jovens perante certos perigos online. O relatório com o título «*Towards a better internet for children*», financiado pelo programa *Safer Internet*, analisa o êxito das estratégias implementadas pela *Coalition* para proteger os jovens dos perigos online. O principal objetivo deste relatório é promover uma navegação mais segura na Internet, melhorando o conhecimento das crianças bem como a experiência dos pais. Este relatório tem por base a aplicação de inquéritos a 25000 crianças (entre os 9 e os 16 anos) e a um dos seus pais, tendo sido realizado em 2010 e aplicado em 25 países europeus (entre estes Portugal).

4.3 Estudo de resultados

Serão analisados dois tipos de resultados: o proveniente dos questionários aplicados aos professores e os resultados extraídos do relatório do projeto europeu EU Kids Online. O inquérito aos jovens investigou alguns riscos eminentes, como bullying, pornografia, receção de mensagens de cariz sexual, contacto com pessoas desconhecidas, encontros com pessoas que se conhece na Internet, abuso de dados pessoais e acesso a conteúdos nocivos. [Livingstone et al., 2012]

4.3.1 Análise dos questionários

Os resultados provenientes dos questionários aplicados aos professores serão apresentados sob a forma de gráficos, tornando mais fácil a análise das respostas. Essencialmente o questionário permite perceber a opinião dos professores em relação ao sistema informático que utilizam na escola em termos de segurança, quais as suas principais preocupações e que cuidados têm na interação diária com o sistema.

Como podemos observar na figura 6, apenas 26% dos inquiridos considera seguro o sistema que utiliza na escola. É importante que os utilizadores tenham noção das fragilidades que o sistema apresenta para que tomem alguns cuidados na sua utilização.

Figura 6 - Gráfico representativo da questão nº1 do questionário

No entanto dos inquiridos apenas 32% tem conhecimento sobre quantos perfis/contas de utilizador têm os computadores da escola, de acordo com a figura 7. Este resultado demonstra desconhecimento num aspeto da segurança que é tão importante - a autenticação - e que pode comprometer os restantes aspetos da segurança.

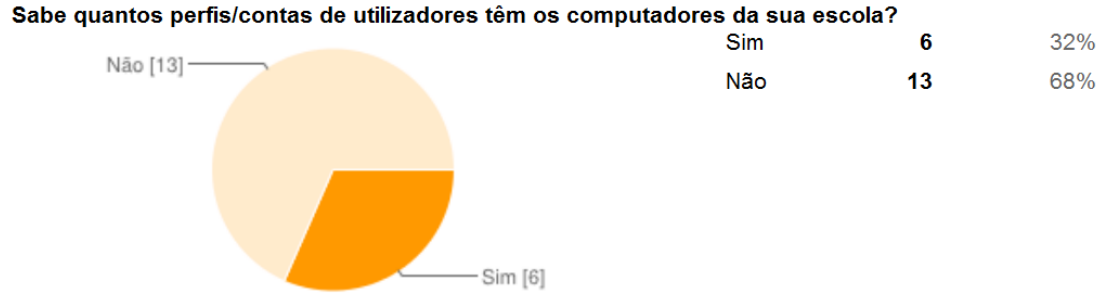

Figura 7 - Gráfico representativo da questão nº2 do questionário

Por outro lado, como podemos observar na Figura 8, grande parte dos inquiridos (58%) afirma não se sentir confortável ao partilhar a mesma conta de utilizador com os restantes professores da escola. Os restantes 42% parecem não se importar com esta ausência de privacidade.

Ainda na mesmo segmento, tal como se pode observar na figura 9, 47% dos inquiridos considera correto que a palavra passe para iniciar sessão, nos computadores da escola, seja partilhada pela maioria da comunidade escolar.

É importante que os professores percebam que o facto de partilharem a mesma conta de utilizador e consequentemente a mesma palavra passe com outros professores implica um cuidado redobrado na utilização dos computadores.

Num sistema com estas características é importante que o utilizador tenha sempre a atenção de guardar os documentos que criou ou que descarregou num suporte próprio, de apagar os ficheiros que criou para que outros utilizadores não tenham acesso a eles, etc. Como os computadores são partilhados por todos os utilizadores, se por acaso o autor do ficheiro não o apagar, qualquer outra pessoa que vá utilizar o computador pode abrir o ficheiro, alterá-lo, utilizá-lo, etc.

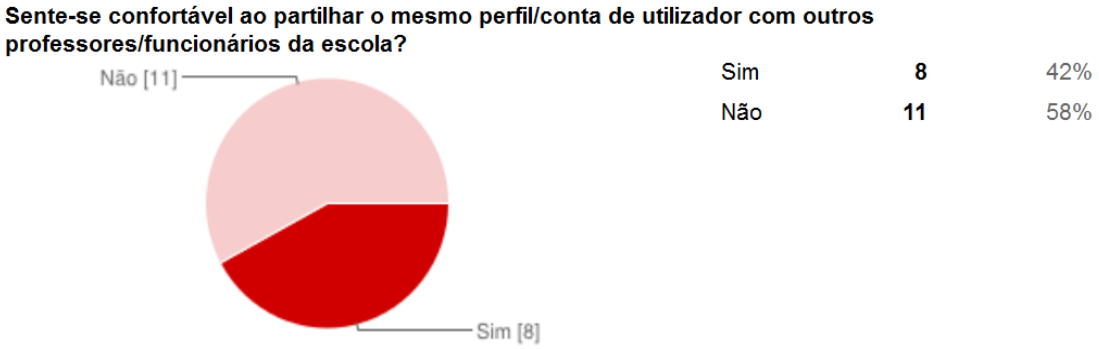

Figura 8 - Gráfico representativo da questão nº3 do questionário

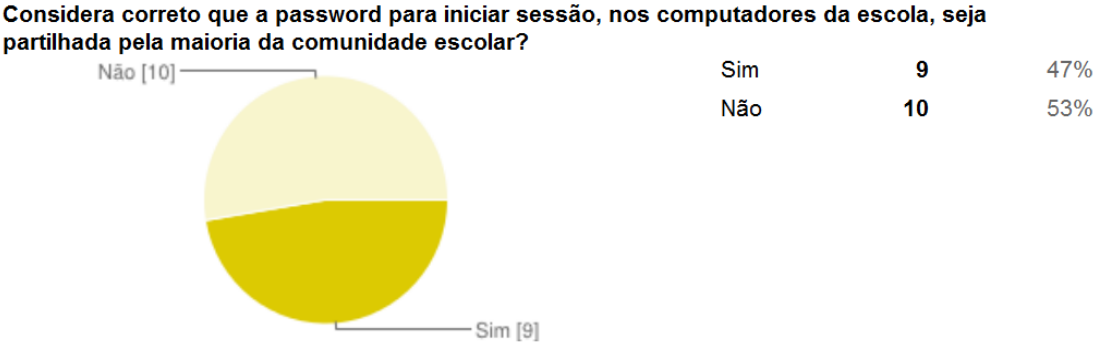

Figura 9 - Gráfico representativo da questão nº4 do questionário

As restantes perguntas do questionário visam abordar os hábitos que os professores têm na interação com o sistema de modo a não comprometerem a sua segurança.

Como podemos observar na Figura 10, 21% dos inquiridos afirma que quando acede a uma página onde é necessário autenticação permite que o browser memorize as suas credenciais

de acesso (password). Esta permissão pode trazer graves problemas de segurança, sobretudo quando é feito em computadores públicos, como é o caso dos computadores da escola. No caso de o utilizador confirmar que quer que o computador guarde o identificador e palavra passe, sempre que alguém aceda à página web em questão estarão memorizadas estas informações e qualquer outra pessoa pode entrar com as credenciais deste utilizador. É muito frequente ocorrer esta situação nos computadores da escola, por vezes dura até ao final do ano letivo ou até haver alguma alteração no computador.

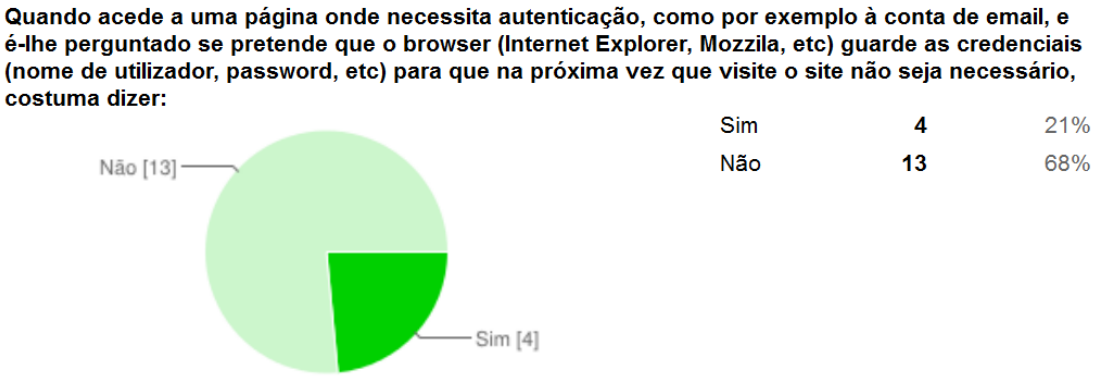

Figura 10 - Gráfico representativo da questão nº5 do questionário

As rotinas de privacidade no acesso à web são esquecidas ou desconhecidas pela grande parte dos utilizadores, como podemos verificar na figura 11, apenas 26% tem por hábito fazer a eliminação de cookies e do histórico da Web no browser e apenas 21 % afirma ter por hábito fazer a remoção definitiva dos ficheiros, através da utilização de um software de limpeza ou esvaziando a reciclagem (figura 12).

Isto quer dizer que estes utilizadores, ao acederem à Internet nos computadores da escola em que a conta é partilhada, não têm o cuidado de eliminar os ficheiros definitivamente, podendo outros utilizadores ter acesso a eles. Também facilmente se pode consultar o histórico da Web e ver que sites um utilizador consultou.

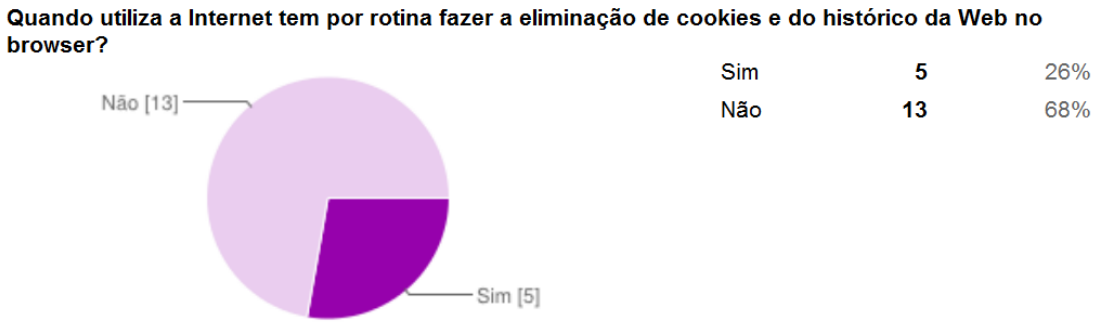

Figura 11 - Gráfico representativo da questão nº6 do questionário

A eliminação de cookies, em computadores públicos e partilhados por muitas pessoas, é também uma rotina de segurança muito importante.

Qualquer utilizador pode instalar um software de sniffing no computador e assim consegue ter acesso a nomes de utilizador e palavras passe armazenadas no computador. Com estes dados o atacante consegue ter acesso total às contas do utilizador.

Figura 12 - Gráfico representativo da questão nº7 do questionário

4.3.2 Análise do relatório EU Kids Online

O relatório tenta analisar qual o êxito das medidas implementadas pela *Coalition* para tornar a Internet um local mais seguro para os jovens. Tendo em conta a realidade que se pretende analisar, apresentar-se-ão os resultados que caracterizam o contexto português. Também serão apresentados alguns resultados com a média europeia para se tirarem algumas conclusões comparativas. [Livingstone et al., 2011]

- Disponibilização de ferramentas simples e robustas para reportar conteúdos maliciosos

Segundo o relatório, apenas 13% dos jovens inquiridos utilizaram as ferramentas que os sites disponibilizam para denunciar ilegalidades online, sendo em Portugal este número ainda menos significativo - 11%.

É importante que os jovens utilizadores com menos experiência sejam estimulados a usar estas ferramentas, devendo estas *"ser desenhadas de forma a serem fáceis de usar por utilizadores pouco experientes"*. [Livingstone et al., 2011]

- Definições privadas apropriadas à idade

É muito comum para os jovens que têm acesso à Internet criarem um perfil numa rede social. Numa amostra de jovens dos 9 aos 16 anos, 59% dos jovens europeus têm o seu perfil criado numa rede social. Destes, apenas 43% têm o seu perfil privado, permitindo apenas aos seus

amigos ter acesso às suas informações pessoais 28% têm semiprivado, ou seja os amigos dos amigos podem ter acesso às suas informações e 26% têm-no público.

A utilização de redes sociais pode trazer perigos, pelo que é importante que os jovens sejam devidamente informados dos perigos que correm ao ter o seu perfil público, devendo ser encorajados a torná-lo privado e a não divulgar informação privada, como o número de telefone e a morada.

Em Portugal,

- 78% dos jovens entre os 13 e os 16 anos
- 38% dos jovens entre os 9 e os 12 anos

} têm um perfil criado numa rede social,

- 25% das crianças têm o seu perfil público,
- 7% dos jovens confessou disponibilizar o seu número de telefone ou endereço nas redes sociais,
- 25% dos jovens exibe na rede social uma idade diferente da que têm.

➢ Classificação do conteúdo/ Mitigar material de abuso infantil

A criação de medidas que incentivem a implementação de uma política eficaz de classificação de conteúdos na Internet é muito importante tendo em conta os resultados obtidos - 12% dos jovens confessaram já ter visto na Internet algo que os incomodou.

Em Portugal:

- 14% dos jovens tiveram acesso a imagens sexuais em sites,
- 6% viram mensagens que incentivam o ódio e a descriminação por grupos,
- 8% tiveram contacto com sites que incitam a magreza excessiva (bulimia e anorexia),
- 5% viram imagens que incentivam a mutilação,
- 4% tiveram acesso a material sobre a experiência em drogas,
- 1% acedeu a material que incentiva o suicídio.

➢ Maior disponibilidade no controlo paternal

É muito importante que os pais controlem o acesso à Internet através da utilização de software de monitorização e filtragem de conteúdos. O relatório demonstra que as principais preocupações dos pais dizem respeito ao risco dos filhos serem contactados por estranhos (33%) ou que vejam material inapropriado (32%).

De realçar que, dos 25 países, Portugal é o que apresenta uma percentagem mais elevada no que diz respeito à preocupação dos pais com o que os filhos fazem na Internet. Neste documento é possível observar que 61% dos pais portugueses preocupa-se com o facto de os filhos verem material inapropriado e 65% preocupa-se com o facto de poderem ser contactados por estranhos.

Dos pais inquiridos, na Europa, 33% afirma utilizar a filtragem de conteúdos na Internet de modo a limitar os conteúdos a que o filho pode aceder e apenas 27% afirma usar software de monitorização. Em Portugal, 29% dos pais afirma utilizar a filtragem e 28% faz a monitorização de conteúdos.

- Mediação no uso da Internet

No que diz respeito à mediação do uso da Internet, é pertinente referir o papel desempenhado pelos professores no contexto português. Serão apresentados os valores de Portugal em cada questão e no final da questão será apresentado entre parêntesis o valor da média europeia. [Simões, 2011]

- 28% dos pais disseram que o local onde obtêm informação e aconselhamento sobre utilização da Internet é na escola do filho (EU 27%),
- 65% dos pais responderam que o local onde desejariam obter mais informações sobre utilização da Internet é a escola do filho (EU 43%),
- 77% dos alunos portugueses confessaram que os professores ajudaram-nos quando estavam com dificuldade em encontrar algum conteúdo na Internet (EU 58%),
- 73% dos alunos portugueses disseram que os professores explicaram porque que alguns sites são bons e outros são maus (EU 58%),
- 68% dos alunos disseram que os professores sugerem medidas para utilizar a Internet de forma mais segura (EU 58%),
- 61% dos alunos disseram que os professores sugeriram maneiras para o aluno se relacionar na Internet (EU 48%),
- 51% dos jovens afirmou que os professores costumam falar com eles sobre o que devem fazer no caso de alguma coisa os incomodar na Internet (EU 40%) e 18% disseram que efetivamente os ajudaram quando alguma coisa os incomodou (EU 24%),
- 64% dos jovens afirmou que o professor estabelece regras sobre o que se pode fazer na Internet (EU 62%) ,
- 78% dos professores falaram com os alunos sobre o que fazem na Internet (EU 53%).

De realçar os valores de Portugal em relação à média europeia e também que os professores têm um papel bem mais proeminente na mediação do acesso à Internet em Portugal relativamente aos outros países.

A. Levantamento de problemas de segurança

De acordo com os dados extraídos do questionário e do relatório, serão apresentados alguns problemas de segurança relacionados com a utilização do sistema não só pelos mais jovens mas também pelos professores.

Com a aplicação deste questionário podemos concluir que, embora a maioria dos professores reconheça que o sistema informático que utilizam na escola apresenta graves falhas de segurança, não têm os cuidados para salvaguardar uma certa dose de privacidade. Embora a maior parte dos professores saiba que os computadores são partilhados por vários utilizadores, mesmo assim não têm hábitos que assegurem segurança tais como eliminar cookies e o histórico da Web no browser e eliminar os ficheiros de forma definitiva, através da utilização de um software de limpeza ou esvaziando a reciclagem. Isto nota falta de hábitos de segurança da informação, o que se deve em grande parte à falta de formação que os professores têm na área da segurança, à inexistência de ações de formação e sobretudo à inexistência de uma Direção nas escolas que se comprometa com uma questão tão importante, mas ao mesmo tempo colocada de parte.

Após analisar os resultados extraídos do relatório EU KIDS ONLINE, podem-se tirar algumas conclusões:

O questionário demostrou que os utilizadores com mais competências digitais são aqueles que utilizam a Internet com mais segurança, pois conseguem reconhecer perigos e adotar um comportamento correto perante eles. Por norma estes utilizadores conseguem manter a privacidade nas redes sociais, utilizam as ferramentas de reporte quando encontram algo que não lhes agrada e conseguem reconhecer material inapropriado.

O mesmo se passa em relação aos pais, sendo que os pais que têm mais conhecimento sobre Internet e que são utilizadores regulares são os que mais utilizam a filtragem e monitorização de conteúdos. É importante que os pais assumam o papel de mediadores no uso da Internet, através da realização de atividades conjuntas ou incentivando a criança a aprender sozinha, mas mantendo-se vigiada.

Uma correta classificação de conteúdos é também um importante incentivo para tornar a Internet um local mais seguro para os jovens. A classificação pode ser feita através da utilização de etiquetas e descrição de conteúdos. Se o material na Web estiver devidamente classificado, provavelmente não vão ocorrer tantas situações em que os jovens recebem material inapropriado para a sua idade, fruto de uma pesquisa mal realizada.

Importa ainda referir a expectativa dos pais e alunos sobre o papel dos professores e da própria escola no aconselhamento sobre o uso da Internet. Aos professores compete o acompanhamento dentro da sala de aula, mas também o aconselhamento aos encarregados de educação sobre como estes devem controlar o acesso dos filhos à Internet.

As escolas cada vez mais desempenham um papel pró-ativo no desenvolvimento destas questões. Ao promoverem a utilização da internet é incrementada a literacia digital, o que melhora as competências em segurança.

B. Identificação de padrões de problemas

Com a análise dos questionários foi possível detetar padrões de problemas:

- Utilizadores com poucas competências digitais

A pouca informação que os utilizadores mais novos têm sobre como devem utilizar a Internet e os recursos informáticos representa um grave problema, não só para as escolas mas para a sociedade em geral. As crianças são incentivadas a utilizar o computador desde o ensino primário, no entanto não lhes são transmitidos os princípios básicos de segurança, o que faz com que esta utilização se torne cada vez mais intuitiva e menos racional.

- Ausência da temática segurança nas componentes letivas

A disciplina de TIC é introduzida muito tardiamente no currículo escolar dos alunos. Atualmente, só no 8º ano é que os alunos têm oficialmente uma disciplina de informática, no entanto a própria disciplina de TIC não aborda a temática da segurança da informação.

- Fraco acompanhamento dos pais

Os pais nem sempre têm disponibilidade para acompanhar os filhos quando estes precisam de utilizar o computador e a Internet para realizar pesquisas, sendo que muitas vezes as crianças ficam sozinhas nas suas primeiras interações. Ao utilizarem de forma autónoma a Internet, as crianças ficam sujeitas a muitos perigos, que já foram mencionados anteriormente, possuindo poucos conhecimentos para lidar com eles.

- Ausência de hábitos de segurança da informação

Também a utilização por parte dos professores reflete falta de conhecimentos digitais e de práticas de segurança. Na maior parte das vezes os professores são “obrigados” a utilizar os computadores da escola para a realização e preparação das atividades letivas, como é o caso das planificações anuais das disciplinas que lecionam, as atas resultantes das várias reuniões, o lançamento de faltas dos alunos, a comunicação aos encarregados de educação, os relatórios das atividades que desenvolvem, a avaliação de desempenho, etc.

Como a maior parte dos professores não tem a devida formação na utilização de recursos informáticos, isto verifica-se sobretudo nos professores com mais idade, sendo compreensível que cometam descuidos que podem causar graves problemas de segurança.

Nos questionários aplicados pode-se verificar que, embora a maior parte dos inquiridos considere que o sistema que utilizam não é seguro, também não tomam medidas para que o mesmo se torne mais seguro, como é o caso dos que responderam que não costumam fazer a

eliminação de cookies e do histórico de navegação nem tampouco a eliminação definitiva dos ficheiros criados.

- Rede da escola vulnerável

Por outro lado e como já foi referido anteriormente, o problema deve-se à configuração das redes instaladas nas escolas públicas, que por si só já são um incentivo para as mais variadas falhas de segurança.

C. Deteção de casos críticos

Com este estudo detetaram-se os seguintes casos críticos:

- Pouca importância atribuída pela Direção da escola à gestão e manutenção da rede informática.
- Inexistência de um documento com a política de gestão da informação da escola que sirva para definir boas práticas e para apoiar utilizadores com menos experiência.
- Os utilizadores do sistema devem ter responsabilidades atribuídas e devem ser responsabilizados pelos seus atos.
- A comunidade escolar não está devidamente consciencializada para a necessidade de segurança na utilização da internet e do sistema informático. É importante que os utilizadores saibam agir com segurança.
- Os utilizadores manifestam competências digitais básicas. Deve-se apostar na formação dos utilizadores sobre segurança na utilização de dispositivos de modo a estimular comportamentos corretos.
- A escola desempenha um papel pouco ativo na formação dos seus utilizadores, devendo promover ações informativas direcionadas a professores, alunos e encarregados de educação.

5 Estudo de soluções

Com o objetivo de encontrar soluções, foram estudadas algumas opções que contribuem para a segurança da informação dentro de uma organização.

A organização que pretenda garantir um nível adequado de segurança de informação deve implementar um ISMS (Information Security Management System), em português um SGSI (Sistema de Gestão de Segurança da Informação). Existem várias opções para implementar um sistema de gestão da segurança da informação conforme as características da organização e o nível de proteção que se pretende implantar.

Independentemente do modelo de SGSI que se pretenda implementar, ele refere-se sempre ao conjunto de políticas de gestão de segurança da informação e à identificação dos riscos associados às TI. Na prática, descreve o conjunto de políticas, processos e sistemas implementados por uma organização com o objetivo de diminuir os riscos associados à gestão da segurança da informação.

Como qualquer outro processo de gestão, a manutenção do SGSI requer eficiência e eficácia ao longo de todo o processo, não devendo ser encarado como um modelo rígido, mas antes adaptar-se às necessidades da empresa e ao ambiente externo. Este sistema de gestão pode ser implementado em qualquer tipo de organização, independentemente da dimensão, ramo a que se dedica, etc. Existem vários modelos para implementar um sistema de gestão da segurança da informação, o mais conhecido e aconselhado é a certificação da ISO 27001, mas também pode ser implementado através das frameworks de gestão Cobit e ITIL.

5.1 Ferramentas de gestão

O **ITIL** e o **Cobit,** embora implementem algumas soluções relacionadas com a segurança da informação, visam sobretudo gerir as Tecnologias da Informação dentro da empresa, ajudando no apoio à decisão e na criação de uma "IT Governance".

"IT Governance" é um componente de gestão que conduz as TI até à gestão de topo, ajudando a prever resultados com menor margem de erro e aumentando a eficácia dentro da organização. Para que seja tirado o máximo partido das TI é necessária uma alteração profunda na forma como estas são encaradas no seio da organização, só assim sendo possível trazer inovação para a empresa. Pode-se definir "IT Governance" como o conjunto de relações e processos que dirige a organização de modo a atingir os objetivos, sendo acrescentando valor ao negócio através da gestão balanceada do risco e do retorno do investimento das TI. [Ferreira, 2009]

5.1.1 ITIL

ITIL é um conjunto de boas práticas para a gestão de serviços de TI, descreve a estrutura dos processos de gestão em TI sem detalhar como um processo em particular deve ser implementado. Tem como objetivo ajudar na definição das melhores práticas e critérios nas operações de gestão, incidindo sobretudo na definição do que é funcional (destaque para as fases 1 e 2 - Suporte e entrega de serviços). [ITIL, 2011]

Pode ser implementado através de 8 módulos:

1. Suporte a Serviços } Essência do ITIL
2. Entrega de Serviços
3. Perspetiva de Negócio
4. Gestão de Infraestruturas TI
5. Gestão de Aplicações
6. **Gestão de Segurança**
7. Planificação e Implementação
8. Gestão de Recursos de Software

A implementação do ITIL pode ser um processo difícil e moroso. Muitas vezes só após alguns anos de implementação é que as organizações conseguem resultados, tornando-se mais eficiente quando acompanhado das ferramentas corretas que suportem os processos e a troca de dados entre estes. A longo prazo, a implementação do ITIL, bem como a adoção de boas práticas, oferece um retorno positivo do investimento (ROI). [Miranda, 2006]

O ITIL visa ajudar a construir uma organização forte, relacionando os serviços fornecidos com as necessidades (presentes e futuras) e tornando o serviço cada vez mais eficiente em termos de custo. Tem ainda a vantagem de ser uma boa preparação para a certificação, pois garante

as melhores práticas nas TI e também a sua gestão financeira, relacionando os serviços com as necessidades reais da organização.

Melhorias significativas:

- No relacionamento entre as TI e a organização
- Na utilização da infraestrutura de TI
- Na utilização do pessoal das TI
- Na reputação das TI no seio da organização

5.1.2 Cobit

Cobit é uma framework para a gestão e controlo de TI através da definição, implementação, monitorização e melhoria dos processos, abrangendo todo o ciclo de vida das TI. Serve de suporte para a organização e para o desenvolvimento de projetos, facilita o trabalho dos gestores ao alinhar os objetivos da organização com os objetivos das TI, o que permite uma gestão mais eficiente de processos, auditorias e monitorização de TI. [ISACA, 2012]

O framework disponibilizado pelo Cobit, para além das ferramentas de implementação, possui alguns recursos tais como o controlo de objetivos, mapas de auditoria e um guia com técnicas de gestão. O Cobit compreende 4 domínios:

1. Planeamento e organização.
2. Aquisição e implementação.
3. Entrega e suporte.
4. Monitorização.

O Cobit direciona-se **sobretudo ao negócio** e pode ser um auxiliar para:

- Gestores que queiram avaliar o risco e controlar investimentos em TI,
- Utilizadores que queiram garantias sobre os serviços de TI de que dependem os seus produtos,
- Auditores que utilizam as recomendações do Cobit para avaliarem o nível de gestão de TI.

5.2 ISO 27001 e ISO 27002

A certificação em gestão da segurança da informação é possível através da implementação da norma **ISO 27001.** A ISO 27001 identifica os controlos que acrescentam segurança e qualidade ao SGSI, enquanto a ISO 27002 define como se pode implementar os controlos definidos e serve como base para construir um programa de segurança de informação. [ISO/IEC,2005a]

As empresas que pretendam garantir as melhores práticas de segurança devem utilizar as duas normas:

- A ISO 27001 define os requisitos auditáveis e é usada para auditorias e para certificar SGSI,
- ISO 27002 é um guia de execução que lista os controlos que uma organização deve considerar.

Figura 13 - Certificação ISO 27001

Uma organização pode-se certificar através da norma ISO 27001, mas não pode obter certificação na ISO 27002. [Calder, 2012]

A certificação corresponde a um controlo integrado da segurança e pode ser aplicada em qualquer tipo de organização, consistindo num conjunto de mecanismos de proteção tecnológica, processual, estrutural e humana.

A. Visão

A informação é um ativo tão importante na empresa como qualquer outro, por isso precisa de ser adequadamente protegida do crescente número de ameaças e vulnerabilidades que vão surgindo.

A segurança da informação consiste na proteção da informação dos vários tipos de ameaças, com o objetivo de minimizar o risco, garantir a continuidade do negócio e maximizar as oportunidades e o ROI. A segurança da informação é implementada através de um conjunto de controlos que incluem as políticas, processos, procedimentos, estrutura organizacional e funções de hardware e software. Os controlos precisam ser estabelecidos, implementados, monitorizados, analisados e melhorados constantemente, utilizando o ciclo de gestão PDCA. [ISO/IEC,2005a]

Desta forma estão reunidas as condições necessárias para criar um Sistema de Gestão de Segurança da Informação e são disponibilizadas as ferramentas necessárias para a melhoria contínua do sistema de gestão. As ferramentas deverão ser analisadas à medida que vão sendo detetados novos riscos e surgindo novas necessidades.

B. Abordagem por processo

A ISO utiliza a abordagem por processos, em que cada atividade é considerado um processo, onde são utilizados e geridos recursos tendo em vista a transformação de entradas em saídas.

Por norma a saída de um processo é a entrada do processo seguinte. A abordagem de processos implica a aplicação, identificação, gestão e interações dos processos existentes dentro de uma organização.

No âmbito da gestão da segurança da informação, a abordagem do processo salienta a importância de:

- Entender os requisitos de segurança da informação dentro de uma organização e a necessidade de estabelecer uma política para a segurança da informação;
- Implementar controlos para gerir os riscos de segurança da informação;
- Monitorizar e analisar criticamente o desempenho e eficácia do SGSI;
- Melhoria contínua com base nas medições.

C. Modelo de gestão PDCA

Para que o sistema esteja sempre atualizado deve-se utilizar o ciclo de gestão PDCA "Plan-Do-Check-Act", um ciclo de desenvolvimento que tem como objetivo a melhoria contínua. As etapas deste ciclo de gestão (ver figura 14) são: [ISO/IEC, 2005]

- Plan - corresponde à fase de **planeamento.** Nesta fase avaliam-se os riscos associados à ausência de segurança da informação e escolhem-se os meios de controlo apropriados; corresponde à definição da política, objetivos, processos e procedimentos capazes de diminuir os riscos e de proporcionar a melhoria da segurança da informação;
- Do - esta é a fase de **implementação** dos controlos escolhidos, políticas e procedimentos do SGSI;
- Check - nesta fase é monitorizado e avaliado o desempenho do SGSI, em termos de eficiência e eficácia; os resultados devem ser comunicados à Direção para que possam ser analisados criticamente;
- Act - nesta fase são feitas as mudanças necessárias para que o SGSI recupere a sua performance e alcance a melhoria contínua.

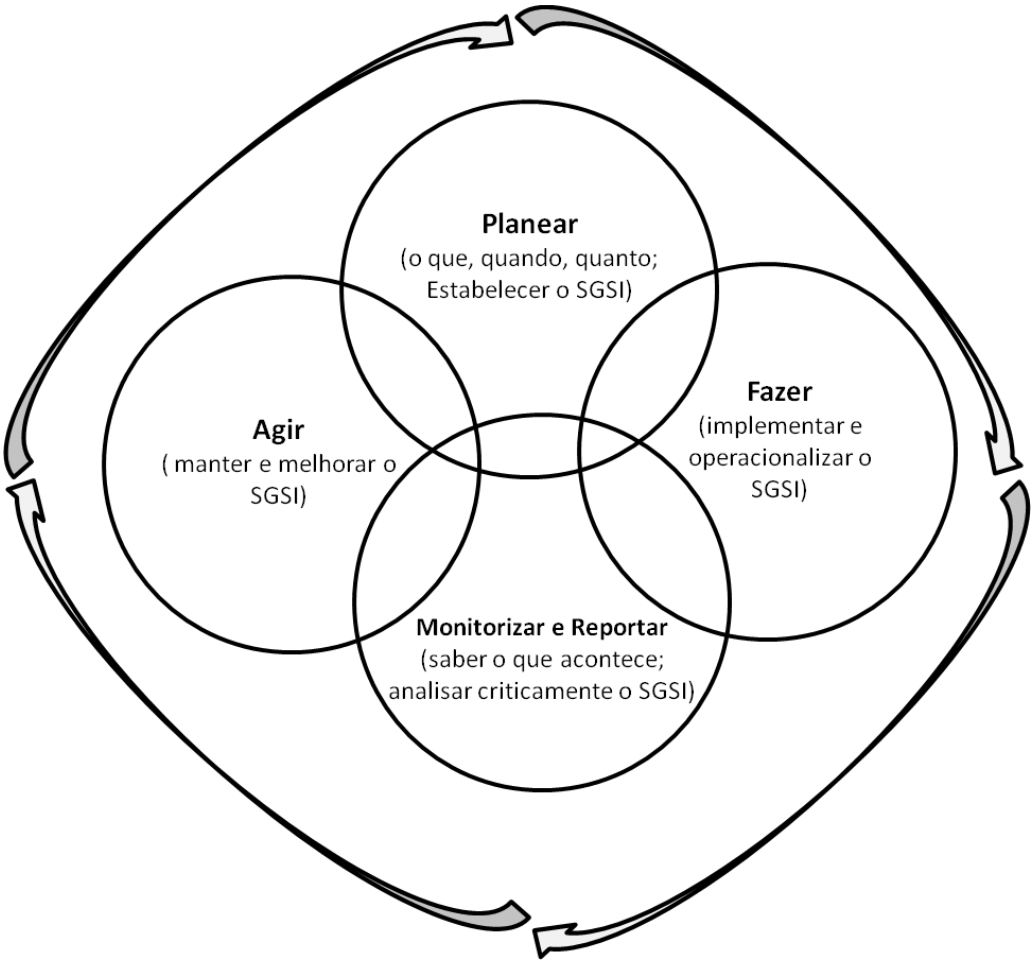

Figura 14 - Ciclo de gestão PDCA

Na figura 14 estão identificadas as fases inerentes ao processo de gestão PDCA, este é um processo contínuo, não um evento único, devendo ser repetido periodicamente para detetar novas necessidades. O modelo gestão PDCA está harmonizado com a norma para a gestão da qualidade (ISO 9001) e com a norma para a gestão do ambiente (14001).

D. Implementar um SGSI

Para implementar um SGSI são necessárias várias tarefas, que vão desde o estabelecer, implementar, manter e monitorizar a segurança da informação na organização, tendo por base a gestão do risco. Esta gestão contempla a estrutura organizacional, políticas, responsabilidades e práticas, planeamento, procedimentos, processos e recursos. [ISO/IEC,2005].

A adoção de um SGSI é uma decisão estratégica da organização, influenciada pelas suas necessidades e objetivos, requisitos de segurança, processos aplicados, tamanho e estrutura.

A primeira tarefa a executar pela organização que pretenda implementar um SGSI, consiste em identificar os riscos decorrentes da ausência de segurança. Após este levantamento, devem ser identificados os requisitos de segurança. Segundo a norma existem 3 tipos principais de requisitos:

- Requisitos legais, regulamentares e contratuais que devem ser respeitados pela organização e pelos seus parceiros,
- Princípios, objetivos e requisitos do negócio que a empresa desenvolve para apoiar as suas decisões,
- Avaliação do risco da organização - deve ser feita de acordo com a estratégia de negócio e os objetivos da organização, deve-se identificar as ameaças e vulnerabilidades, qual a probabilidade de ocorreram e quais os impactos que podem causar.

Após **identificados os riscos e os requisitos de segurança,** devem-se selecionar os controlos apropriados tentando reduzir os riscos para um nível aceitável. Com base nos critérios de aceitação de risco, que devem estar de acordo com a regulamentação e legislação nacional e internacional, compete à organização decidir quais os controlos de segurança que devem ser ativados, dando prioridade àqueles que possam melhorar o desempenho do negócio. O custo de implementar certos controlos deve ser equilibrado com o risco que a falha representa para o negócio. A avaliação de risco deve ser repetida periodicamente para conseguir identificar novas ameaças ou ameaças que mudam.

E. Controlos

Na ISO 27002 são contemplados 11 controlos principais de segurança. De acordo com a figura 15, dentro de cada controlo existem várias categorias principais de segurança. A ordem dos controlos é aleatória, por isso não é obrigatório seguir a ordem apresentada na norma, podendo-se ajustar de acordo com as necessidades da organização.

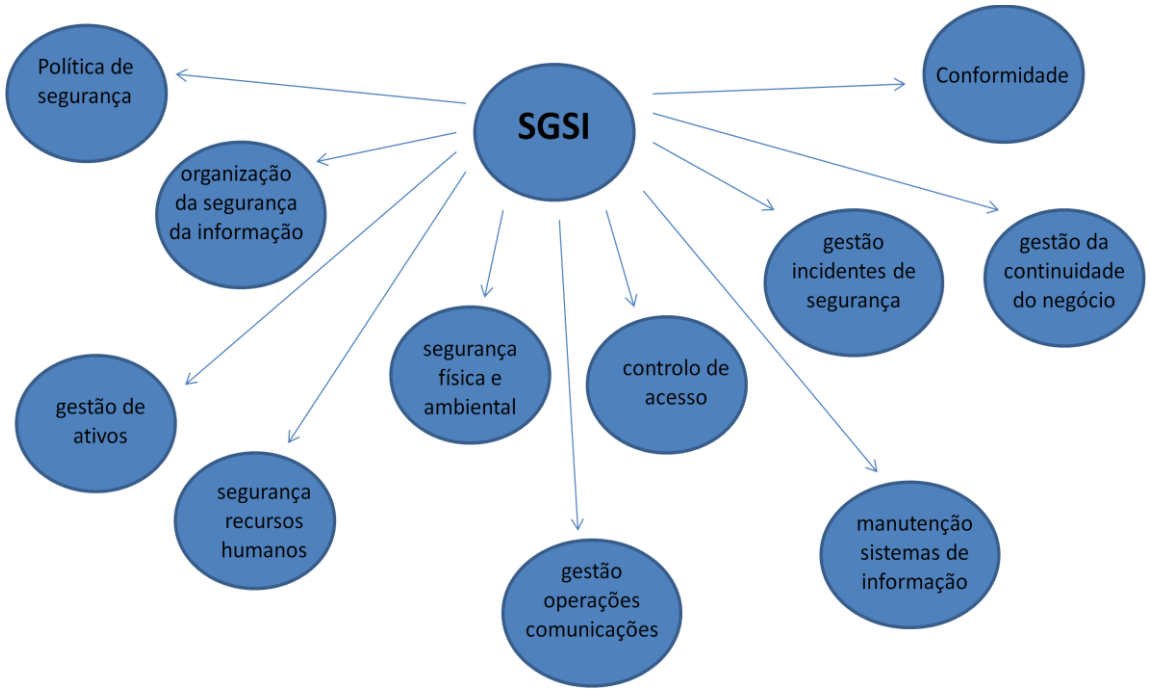

Figura 15 - Controlos do SGSI

A organização que pretenda obter a certificação deve analisar criteriosamente estes controlos, implementando aqueles que considere ser adaptados às suas necessidades. Será brevemente explicado o que cada controlo pretende implementar:

1. Política de segurança: a direção deve fornecer orientações para a segurança da informação de acordo com os requisitos do negócio, leis e regulamentação;
2. Organização da segurança da informação: fornecer diretrizes para gerir a segurança da informação dentro da organização e nas partes externas;
3. Gestão de ativos: atribuir responsabilidades aos ativos dentro da organização, implementando formas de protegê-los num nível adequado;
4. Segurança dos recursos humanos: atribuir responsabilidades aos recursos humanos de modo a evitar o roubo, fraude, danos, etc.
    - As consequências destas ações devem ser claramente transmitidas.
    - É necessário o envolvimento de toda a equipa para assegurar a segurança da informação e evitar o aparecimento de ameaças.
5. Segurança física e ambiental: implementar medidas para que pessoas não autorizadas acedam ao sistema, causando interferências nas instalações e na informação.
6. Gestão de operações e comunicações: garantir que os recursos de processamento da informação são corretamente utilizados, isto aplica-se também à entrega de serviços a terceiros. Neste controlo são verificados vários itens:
    - minimizar o risco de falhas nos sistemas;
    - proteger a integridade do software e da informação;

- garantir a integridade e a disponibilidade da informação através de cópias de segurança;
- gerir a segurança na rede;
- prevenir a divulgação não autorizada;
- garantir a segurança de serviços de comércio eletrónico ;
- implementar mecanismos de monitorização de eventos.

7. Controlo de acesso: Pretende controlar o acesso à informação, garantindo que apenas utilizadores autorizados têm acesso à mesma e implementando mecanismos para que utilizadores não autorizados não consigam ter acesso aos recursos. Os mecanismos implementados devem controlar o acesso à rede, ao sistema operativo e à informação de certas aplicações.
8. Aquisição, desenvolvimento e manutenção de sistemas de informação: garantir que a informação produzida é segura, prevenindo a ocorrência de erros, falhas, modificações não autorizadas e vulnerabilidades.
9. Gestão de incidentes de segurança da informação: os incidentes de segurança devem ser reportados por todos os utilizadores e monitorizados para que posteriormente sejam corrigidos.
10. Gestão da continuidade do negócio: implementar mecanismos para que não haja "inaceitável" prejuízo no caso de o negócio ser interrompido, assegurando uma retoma rápida.
11. Conformidade: representa a conformidade com aspetos legais, legislação, estatutos, regulamentações, certificação em segurança da informação e conformidade com auditorias.

Embora a aplicação dos controlos seja feita de acordo com a necessidade da organização, alguns deles são considerados boa prática para a segurança da informação em qualquer tipo de empresa, como por exemplo:

- Elaboração de documento com a politica da segurança da informação,
- Atribuição de responsabilidades de segurança da informação,
- Educação e prática de segurança da informação,
- Processamento correto em aplicações,
- Gestão técnica das vulnerabilidades,
- Gestão contínua do negócio,
- Gestão dos incidentes de segurança e melhoria.

Os controlos considerados essenciais são:

- Proteção de dados - privacidade
- Proteção dos documentos da organização
- Direitos de propriedade intelectual

} Módulo Conformidade

Nem todos os controlos presentes na norma podem ser aplicados por uma organização, assim como pode ser necessário implementar outros controlos que não estejam contemplados na norma. Deste modo, cada empresa deve desenvolver o seu próprio manual com a política de segurança da organização, em que devem estar identificadas todas as questões práticas implementadas.

A norma recomenda que cada organização apenas implemente os mecanismos de proteção adequados à sua realidade e que possam diminuir o impacto de eventuais falhas de segurança. Fundamentalmente, a norma é um padrão reconhecido de gestão da informação, assenta no modelo de gestão PDCA, apostando na melhoria contínua através da identificação de riscos e incidentes de segurança, mudanças e objetivos de negócio.

F. Vantagens da certificação

Quando uma empresa é certificada, comprova-se que possui um sistema de gestão da informação onde estão implementados os mecanismos de proteção de dados adequados à sua realidade. O sistema procura garantir a confidencialidade, a integridade e a continuidade do negócio, diminuindo o impacto que possíveis falhas possam ter sobre o sistema.

As principais vantagens da certificação são:

- Aumento da credibilidade comercial -> os intervenientes do sistema sentem-se mais seguros ao saber que a organização tem implementado mecanismos de proteção da informação;
- Redução de custo dos incidentes -> muitas vezes o custo de uma perda de dados é superior ao custo da implementação da certificação;
- Cumprimento de leis e regulamentos -> no que diz respeito ao ordenamento jurídico português ou outros regulamentos.
- Diminuição dos riscos causados pelos incidentes de segurança -> ao certificar-se a organização está a conhecer melhor o seu sistema de informação, as suas vulnerabilidades e que mecanismos estão disponíveis para proteção de incidentes de segurança.

G. Obter a certificação

Para obter a certificação, a organização deve responder às 5 áreas de controlo identificadas na ISO 27001, sendo cada uma delas sujeita a uma auditoria.

Sistema de gestão de segurança da informação: define a necessidade de estabelecer, implementar, operacionalizar, monitorizar, analisar e melhorar o SGSI, utilizando o ciclo de gestão PDCA. Estas fases devem ser devidamente documentadas e devem incluir:

- Identificação e analise da gestão de risco bem como metodologias de tratamento,
- Áreas de atuação e limites do SGSI,
- Quadro de gestão para medir objetivos,
- Identificação de ativos e tecnologia, etc.

Responsabilidade de gestão: atribuição de responsabilidades à gestão do SGSI, como o compromisso da gestão. Devem ser identificados os objetivos de segurança da informação, os recursos adequados para os atingir e a tolerância ao risco.

Auditorias internas: necessidade de realizar auditorias internas do SGSI; estas devem ser devidamente documentadas e devem incluir os critérios, frequência, metodologia e responsabilidades.

Gestão da revisão do SGSI: periodicamente o desempenho do SGSI deve ser analisado e revisto, bem como as suas entradas e saídas;

Melhorar o SGSI: identificação de ferramentas para melhorar o desempenho do SGSI, bem como das ações corretivas.

5.3 Selo de segurança digital para as escolas

A atribuição do **selo de segurança digital para as escolas** é uma iniciativa da European Schoolnet. É um serviço de apoio e de acreditação a nível europeu para as escolas e representa um importante incentivo para tornar a Internet um local mais seguro para as crianças e jovens. Esta iniciativa foi divulgada no dia da Internet Segura, a 7 de Fevereiro de 2012, é um projeto que nasceu devido à necessidade de apoio que as escolas sentiram nesta área e reúne vários parceiros, como é o caso dos Ministérios da Educação europeus (Portugal, Itália, Bélgica, Áustria, Dinamarca, Holanda), organizações ligadas à educação (Espanha, Estónia e Áustria), empresas do setor (Microsoft, Kapersky Lab, Liberty Global, Telefonica) e a European Schoolnet. [EUN,2011]

Os elementos deste projeto incluem:

- Um portal onde é disponibilizada uma base de dados com recursos educativos sobre segurança digital. Aqui estão disponíveis diversos materiais, desde planos de aulas até políticas a implementar nas escolas;

- Uma ferramenta de avaliação que pode ser utilizada pela escola para testar as suas práticas de segurança digital. Posteriormente serve para comparar com os padrões definidos internacionalmente;
- Uma comunidade de especialistas na área.

Figura 16 - Certificação eSafety

De Fevereiro até Julho de 2012 arrancou o projeto piloto, tendo este sido implementado em 4 (ou 6) escolas de cada país. As escolas que estiveram envolvidas neste projeto forneceram feedback até setembro de 2012. As escolas que pretendam participar neste processo de creditação devem registar-se no site, para que posteriormente possam:

- Rever as práticas eSafety da escola;
- Submeter evidências para o Laboratório eSafety de modo a obter a creditação;
- Receber um plano de ação sugerido pela eSafety de modo a progredir para níveis mais elevados de creditação;
- Aceder a um elevado número de recursos;
- Aceder a links de escolas que tenham obtido a acreditação eSafety.

A candidatura é realizada através do envio de evidências das práticas correntes utilizadas na escola e do preenchimento do questionário online. O questionário e as evidências serão avaliados e comparados com os níveis apresentados por outras escolas e pelas médias nacionais para que seja atribuído um nível de segurança eletrónica: ouro, prata ou bronze.

O questionário online deve ser preenchido pelo diretor da escola, pelo responsável pelas TIC e ainda por outros profissionais de ensino que ajudem a caracterizar o sistema. Contempla questões que definem a infraestrutura, políticas e práticas da organização, como por exemplo:

- Se os computadores estão protegidos com antivírus,
- Se os ambientes de aprendizagem e de administração são separados,
- Como são geradas as palavras passe dos alunos e funcionários,
- Se os alunos e professores podem utilizar dispositivos USB nos computadores da escola, etc.

A avaliação do questionário gera um plano de ação e outros documentos de referência que devem ser usados para melhorar a segurança e o desempenho do sistema da escola.

5.4 Objetivos da solução

O principal objetivo é eliminar as vulnerabilidades existentes na rede informática da escola, através da implementação de mecanismos que garantam a proteção da informação e a diminuição do risco de perdas de informação.

Perante as opções que foram apresentadas, a implementação de um SGSI parece a decisão acertada. A adoção de um sistema de gestão da Segurança da Informação deve ser uma decisão estratégica da Direção da escola e deve refletir:

- As necessidades,
- Os objetivos,
- Os requisitos de segurança,
- Os tipos de utilizadores,
- A dimensão e estrutura da organização.

Os objetivos da solução a implementar devem passar por:

- Transmitir aos utilizadores quais os requisitos de segurança da informação,
- Implementar e operacionalizar controlos para gerir os riscos de segurança,
- Monitorizar e analisar criticamente o desempenho do SGSI,
- Desenvolver um manual de procedimentos,
- Estimular a melhoria contínua da organização e dos seus atores.

O manual desenvolvido pela escola para suporte do SGSI deve conter:

- a política de segurança da informação da organização,
- o grau de proteção atribuído à informação, que deve resultar de uma análise
    - dos mecanismos que protegem a informação de terceiros e que garantem a confidencialidade;
    - da integridade e que até que ponto estão implementados mecanismos que garantem a veracidade da informação;
    - da disponibilidade da informação, prevenindo que o sistema tenha interrupções quer em hardware, quer em software.
- conselhos de utilização dos recursos informáticos /equipamentos,
- regras e procedimentos que acrescentem segurança aos recursos de informação. [ISO/IEC,2005]

6 Proposta de soluções

Muita coisa pode ser feita para melhorar o sistema informático utilizado nas escolas, umas mais facilmente exequíveis, outras de implementação mais lenta.

A candidatura à certificação do *esafetyschool* traz vantagens para as escolas, até porque obriga a analisar as práticas e políticas implementadas. Com esta recolha efetuada e o serviço de informação caracterizado, torna-se mais simples implementar um SGSI esta é a solução que pode fazer frente aos problemas detetados nas escolas.

As escolas podem desenvolver um SGSI de acordo com a ISO 27002, uma vez que as boas práticas enunciadas neste código de práticas são reconhecidas internacionalmente. Como esta norma não foi desenhada para aplicar a certificação, não especifica quais os requisitos que o SGSI deve satisfazer para obter a certificação, enquanto a ISO 27001 já inclui estas especificações. Em termos técnicos isto quer dizer que uma organização que utilize a ISO 27002 entra em conformidade com o guia de boas práticas mas não oferece uma estrutura que possibilite a verificação de cumprimento com o standard. [Calder, 2012]

A solução que passamos a apresentar passa por implementar um Sistema de Gestão da Segurança da Informação através da definição de uma política de segurança da informação adaptada à realidade da escola. Para ser eficaz e eficiente, este documento deve ser desenvolvido por cada escola, refletindo as suas reais necessidades, vulnerabilidades, mecanismos, etc. O modelo que propomos é genérico e pode ser implementado pela maior parte das escolas, no entanto não reflete as necessidades individuais de cada instituição de ensino.

Serão apresentadas duas soluções:

- Uma proposta para implementar um modelo de gestão de segurança da informação na escola,
- Um documento com a política de gestão da informação, direcionada aos utilizadores.

A proposta de implementação foi elaborada com base nos controlos da ISO 27002, ressalvando a necessidade de análise, monitorização e implementação de novos controlos de modo a atingir a melhoria continua.

A utilização destes controlos ajuda a criar uma política de gestão da segurança da informação e é um meio para se conseguir responder aos requisitos definidos na ISO 27001 para obter a certificação em segurança da informação.

A adoção da norma visa criar padrões de segurança através da implementação e divulgação de práticas de gestão, com o objetivo de manter as características informacionais dos recursos.

Antes de apresentarmos a proposta de implementação de um SGSI, referimos que a metodologia utilizada envolveu várias etapas, que passamos a explicar:

1. Análise da ISO 27001 e da ISO 27002.
2. Perceção das diretrizes presentes na norma.
3. Definição do SGSI.
4. Criação do objetivo e âmbito de aplicação do SGSI.
5. Identificação da legislação.
6. Identificação dos requisitos de segurança.
7. Análise das vulnerabilidades.
8. Seleção dos controlos enunciados na ISO 27002.

O documento com a política de segurança da informação que se propõe deve ser aprovado pela direção, publicado e comunicado a todos os intervenientes do sistema.

6.1 Solução 1: Proposta de documento com a política de segurança da informação

Política de segurança

A informação é um ativo dentro da escola e como tal devem ser aplicados os devidos mecanismos de proteção que possam fazer frente a ameaças, vulnerabilidades e falhas.

Para atingir este objetivo estamos a implementar um SGSI, de acordo com a ISO 27001 e com a ISO 27002, constituído pelo conjunto de políticas, processos, procedimentos e funções de software/hardware que visam assegurar a proteção da informação do maior número de ameaças possível.

A segurança da informação é assegurada através da implementação de um conjunto de controlos, que devem ser estabelecidos, implementados, monitorizados e revistos sempre que necessário de modo a detetar novas necessidades.

A escola, através da sua política de segurança da informação, deve contribuir para a formação dos seus utilizadores, fornecendo diretrizes apropriadas que incentivem a formação individual, preparando-os para utilizar com proficiência as Tecnologias da Informação.

A gestão da segurança da informação é uma decisão estratégica da Direção da escola, como tal é inteiramente apoiada e acompanhado pela equipa da Direção. A escola nomeou um coordenador de informática que é o responsável pela análise da segurança e desenho e implementação de soluções. Este coordenador deve gerir uma equipa técnica, que o deve apoiar na implementação de soluções.

Objetivos da política: [Atsec, 2007]

- Obrigatoriedade de autenticação para aceder ao sistema
- Confidencialidade na comunicação
- Integridade da documentação criada
- Cumprimento da legislação
- Formação de uma equipa técnica que seja responsável pela manutenção do sistema
- Formação dos utilizadores
- Aprovação da política pela Direção
- Transmissão da política do SGSI a todos os utilizadores
- Publicitação da política de segurança da informação

Para conseguir levar a cabo uma política de proteção da informação foram implementados controlos, de acordo com a ISO 27002, que garantam uma correta gestão da informação.

Conformidade

A escola compromete-se a cumprir com a legislação aplicável**,** através do respeito pela propriedade intelectual, aplicando os devidos mecanismos de proteção aos documentos organizacionais e aos documentos que contêm dados pessoais.

Os direitos de **propriedade intelectual** devem ser respeitados:

- É proibido a instalação de software que não seja legal, bem como a utilização de material sem a devida atribuição de créditos de propriedade intelectual.
- Sempre que seja necessário adquirir software, deve-se adquirir através da compra ou então através da utilização de software livre.
- As licenças, discos e manuais que comprovem a propriedade de licenças devem ser guardados e mantidos sob a responsabilidade do coordenador de informática.
- É proibido copiar livros, artigos, ou outros documentos que não estejam incluídos na lei de direito autoral.

Os **documentos organizacionais** que comprovem a atividade da escola devem ser protegidos de perda, destruição e falsificação. À documentação com este carater deve ser aplicada técnica de cifragem, sendo necessário armazenar as chaves pelo período de tempo que a informação tenha de permanecer armazenada.

A escola aprova a **política de privacidade** e proteção de dados pessoais aplicando a devida proteção aos dados que são disponibilizados por alunos e funcionários da escola.

Dados pessoais são qualquer informação, em qualquer suporte, relativa a uma pessoa singular, identificada ou identificável através de algum número de identificação.

A escola é responsável pelo tratamento de dados, aplicando os devidos mecanismos que garantam a correta proteção destes e a não publicitação. [ISO/IEC, 2005a]

Gestão de ativos

A escola deve iniciar um processo de inventariação de todos os ativos, devendo atribuir um proprietário responsável e também o método de proteção adequado:

- Ativos de informação.
- Ativos de software.
- Ativos físicos - equipamento tecnológico, hardware.
- Serviços.
- Pessoas e suas qualificações. [ISO/IEC, 2005a]

Responsabilidades

Todos os utilizadores do sistema têm a obrigação de agir em conformidade com a política de segurança da informação:

- Compete ao coordenador de informática a análise de vulnerabilidades e a escolha de controlos adequados para salvaguardar a segurança da informação;
- A equipa técnica deve ajudar na implementação das soluções escolhidas pelo coordenador e pela Direção;
- A Direção deve apoiar o desenvolvimento da política de segurança, disponibilizando os recursos necessários.
- Os utilizadores devem zelar pelo equipamento, devendo reportar avarias ou alguma situação anómala.
- Cada utilizador é responsável pela informação que produz, devendo tomar as devidas precauções explícitas nesta política. [ISO/IEC, 2005a]

Recursos humanos

Papéis e responsabilidades

- Todos os utilizadores do sistema devem ter responsabilidades atribuídas, de acordo com o seu papel na organização.
- Assim, todo o utilizador é responsável por preservar o equipamento e a informação, devendo adotar uma postura correta e agir de acordo com a política definida.
- Sempre que um utilizador cause um dano gravoso deve ser responsabilizado pelos seus atos. Os utilizadores têm o dever de preservar o equipamento físico, não alterando as suas configurações iniciais, e devem agir de acordo com as regras da escola.
- Os utilizadores têm a obrigação de comunicar ocorrências. Nas salas de informática, devem ser disponibilizadas folha de ocorrências, para que o professor registe o nº do computador e a avaria detetada. Sempre que um utilizador detete uma anomalia num computador deve comunicar à pessoa responsável na sala de aula, para que esta possa tomar conta da ocorrência.
- Sempre que seja contratado um novo funcionário/ professor para a escola, a direção deve pôr o funcionário a par da política de segurança da informação, alertando para a necessidade de cumprimento e quais as consequências no caso de violação da política. O mesmo se aplica aos alunos.

Consciencialização, educação e treino em segurança da informação

- A escola intervém no processo de consciencialização dos seus utilizadores para a necessidade de segurança através da promoção de palestras e workshops direcionados a toda a comunidade escolar.

- A Direção financia ações de formação na área da gestão da segurança para o coordenador de informática, bem como para a equipa técnica responsável pela manutenção do sistema de informação.
- Os professores de informática devem participar nos projetos da *Isecom* e Seguranet, estimulando a consciencialização para a necessidade de segurança pelos alunos.

Segurança física e do ambiente

Perímetros de segurança

A criação de perímetros de segurança tem por objetivo prevenir que pessoas não autorizadas tenham acesso físico ao equipamento. A informação critica e sensível deve ser mantida em áreas seguras com barreiras implementadas de controlo de acesso. Todo o equipamento crítico, como é o caso de servidores e equipamento de interconexão responsáveis pelo funcionamento da rede, devem ser mantidos longe do alcance dos utilizadores.

Os servidores devem ser usados somente para este fim, não devendo ser aproveitados para posto de trabalho, pois no caso de haver um erro, as consequências podem ser muito graves para a rede.

Servidores, hubs e switches devem estar localizados numa sala a que ninguém tenha acesso, localizado preferencialmente ao lado da Direção. Apenas poderá ter acesso a esta sala o diretor da escola, o coordenador de informática ou qualquer outra pessoa nomeada por estes.

Segurança na sala de aula

Para garantir a segurança dos equipamentos, as salas de informática devem estar fechadas à chave e só o funcionário pode abrir. O acesso a estas salas só é permitido com o professor responsável.

Segurança dos equipamentos

Os servidores devem ser protegidos contra a falta de energia elétrica através da utilização de UPS.

Gestão das operações e comunicações

Proteção contra códigos maliciosos

Este controlo visa proteger a integridade de software e da informação, prevenindo a introdução de código malicioso, como vírus, cavalos de troia, etc.

Na escola só é permitido instalação de software legal. Para que os computadores funcionem sem erros de software é necessário que quer o sistema operativo, quer os programas instalados, sejam legais com licenças válidas. A escola pode sempre optar por instalar programas com licença livre, evitando assim grandes despesas de aquisição.

No que diz respeito à prevenção de vírus, todos os computadores devem ter software antivírus instalado e firewall ativo. Os computadores estão configurados para que, sempre que seja iniciada sessão, seja feito um scan rápido e as atualizações sejam instaladas automaticamente.

Não permitir instalação de programas

Os utilizadores não devem ter permissões para instalar software na sua área pessoal. Sempre que seja necessário instalar algum programa no âmbito de quaisquer disciplinas, terá de ser o professor responsável a solicitar a instalação ao coordenador de informática. Neste pedido deve estar descrito qual o programa a instalar, em que computadores o mesmo deve ser feito, durante quanto tempo, etc. As permissões atribuídas ao grupo de utilizadores apenas possibilitam o armazenamento de ficheiros.

Desativar entradas USB do computador

As entradas USB dos computadores deverão estar desativadas, desta forma tornando-se impossível a ligação de dispositivos USB, dispositivos de reprodução MP3, discos externos, etc. A escola deve incentivar os alunos a utilizarem soluções de cloud computing, desta forma é possível proceder ao armazenamento de ficheiros na web sem ter de ligar dispositivos externos ao sistema. Esta medida visa prevenir a propagação de vírus nos computadores da escola.

Cópias de segurança

A informação crítica deve ser alvo de backups regulares. Considera-se crítica toda a informação que é vital para o funcionamento das atividades da escola e que por norma resulta dos processos de gestão, financeiros, administrativos, etc. A informação proveniente da secretaria, da Direção e dos professores, sobretudo a proveniente da aplicação "alunos" e outras de carater administrativo, enquadram-se nos requisitos de informação crítica para a escola.

Conforme o manual emitido pelo Ministério da Educação, "*é importante criar uma política de cópias de segurança*" definindo dias, horas e quem vai realizar estas cópias. A cópia de segurança pode ser agendada para o fim-de-semana e pode ser armazenada no disco do servidor de ficheiros na rede. Posteriormente pode-se gravar os backups para um DVD, pois é o suporte que apresenta um valor mais reduzido por MB. [Ramos, 2011]

Gestão da segurança na rede

Separação física e lógica

Na escola existem 4 grupos de utilizadores, havendo uma separação física e lógica entre este, com diferentes níveis de acesso e atribuição de privilégios distintos.

- Secretaria.
- Direção.
- Professores.
- Alunos.

Utilização de Proxy para aceder à web

Um proxy funciona como um agente procurador, encarregando-se da tradução de ações e de protocolos entre ambientes diferentes. Ao utilizar um servidor proxy para aceder à Internet, o proxy vai atuar como um intermediário entre o cliente e o pedido que está a ser feito ao servidor na Web, como é possível verificar na figura 17. A vantagem é que o acesso tem de seguir as regras definidas, pois todos os pedidos de acesso são feitos pelo proxy e só depois devolvidos ao cliente. [Aragão, 2012]

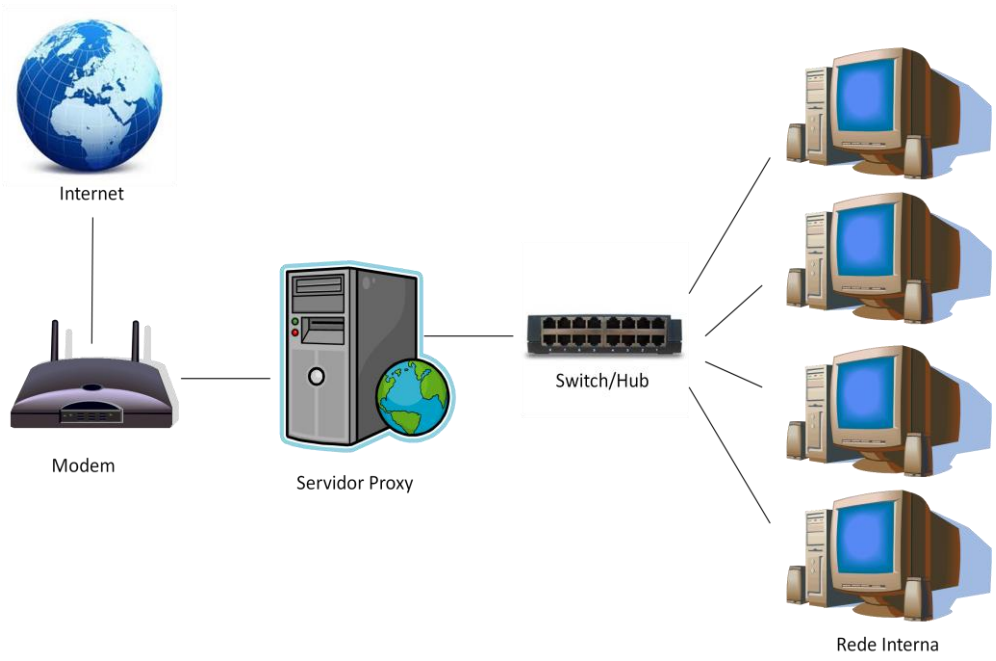

Figura 17 - Utilização de um servidor proxy

Ao configurar o browser para usar um servidor proxy para se conectar à Internet, é criada uma barreira de segurança entre a rede interna da escola e a Internet, impedindo que pessoas que se encontrem algures na Internet consigam ter acesso a dados que estão localizados na rede da escola. A utilização de um proxy traz amplas vantagens no âmbito da segurança, até porque ajuda a filtrar conteúdos podendo negar o acesso a certos recursos, considerados inseguros pela escola.

- A utilização de um Proxy Web serve para garantir a segurança da rede local, pois vai funcionar como intermediário no acesso à Internet;
- A utilização de um Proxy de filtro de conteúdo é indicado para filtrar páginas e assim negar o acesso a certos conteúdos, tais como:
    - Redes sociais.
    - Youtube.
    - Sites de jogos.
    - Sites de pornografia.
    - Etc.

Perímetros de segurança nas redes sem fios

A rede wi-fi da escola está colocada numa sub-rede IP, separada por uma firewall restritiva, com a potência do sinal no mínimo. O protocolo utilizado é o WPA2 (ou melhores).

Monitorização

O objetivo da monitorização de sistemas é detetar atividades de processamento da informação. O logging consiste no registo de eventos (em servidores, bases de dados e redes), enquanto a monitorização consiste na análise dos eventos com o objetivo de detetar anomalias e tendências. [Costa, 2010]

O registo de ocorrências permite mais tarde responsabilizar os utilizadores pelas suas ações, tornando-se possível:

- Estudar padrões de comportamento de utilizadores, dos objetos e das redes,
- Estudar possíveis quebras de segurança,
- Avaliar a eficácia de elementos de segurança,
- Analisar ataques.

Os eventos que se pretende monitorizar na rede da escola são:

- Eventos relativos a gestão de contas de utilizadores (alteração nos atributos de segurança),
- Eventos relativos a controlo de acesso (logins e logoffs mal sucedidos, acessos negados à conta),
- Alteração de configurações,
- Tentativas de acesso a aplicações e a recursos do sistema,
- Comandos introduzidos pelo utilizador,
- Desempenho do sistema e da rede,
- Tráfego de rede (tráfego que entra e sai da rede).

Os logs devem ser automaticamente analisados e gerados alertas para informar irregularidades. Para além do registo de logs, sugere-se o uso da ferramenta *Snort* para auscultar a rede. O *snort* é uma ferramenta *open source* de deteção de intrusão na rede (NIDS), baseada na implementação de regras e geração de alarmes, e tem a vantagem de interagir com a *Firewall*. [Snort,2010]

Controlo de acesso

Criar perfis individuais de utilizador

A utilização dos recursos informáticos da escola só é possível a utilizadores devidamente autenticados.

A autenticação pode ser implementada através de mecanismos de controlo de acesso, cada utilizador tendo um perfil individual composto por nome do utilizador e palavra passe. Para poder aceder ao sistema, o utilizador terá de inserir as suas credenciais de acesso, tornando assim possível que vários utilizadores utilizem o mesmo computador.

A criação de perfis de utilizador traz grandes vantagens para a escola, pois o utilizador tem um perfil obrigatório e todas as alterações que fizer na sua área de trabalho serão perdidas assim que este terminar a sessão. [Stanek, 2012]

Este tipo de configuração é feita no servidor, devendo ser atribuído um perfil de utilizador obrigatório a cada utilizador, desta forma o perfil fica ativo assim que o utilizador iniciar sessão num computador da rede. Apenas o administrador pode fazer alterações nesta configuração.

As permissões atribuídas aos utilizadores dos computadores da escola passam pelo armazenamento de ficheiros, configuração do conteúdo da área de trabalho, adição de endereços nos favoritos, configurações no Internet Explorer e nos locais na rede.

Registo do utilizador

- No início do ano letivo são registados todos os utilizadores e é atribuída uma palavra passe;
- Sempre que entre um novo aluno ou funcionário/professor para a escola, após o início do ano letivo, a secretaria deve comunicar esse facto ao coordenador de informática para que este possa fazer o registo do utilizador.

Gestão de privilégios -> Atribuir cotas no disco a cada grupo de utilizadores

Devem ser atribuídas cotas em disco a cada utilizador ou grupo de utilizadores para armazenamento de ficheiros, limitando assim a utilização do disco.

As cotas de disco servem para monitorizar e gerir o espaço em disco, impedindo que o utilizador exceda o limite de cota que lhe foi atribuída. Sempre que o utilizador esteja perto do limite imposto pelo administrador da rede é apresentada uma mensagem de aviso com a informação de quantos MB faltam para atingir o limite.

Garantir que o computador arranca apenas pelo disco

Os computadores devem estar configurados de forma a arrancar apenas pelo disco rígido, desta forma conseguindo-se prevenir situações em que os utilizadores tentam adulterar o sistema introduzindo um Sistema Operativo através de CD ou Pendrive.

Controlo de acesso à rede

Criação de VPN

Numa rede local, como é o caso da rede da escola, podem-se implementar redes virtuais que na prática funcionam como se fossem várias redes independentes.

A utilização de VPN oferece vantagens ao nível organizacional, implementa segurança na rede, tornando-a inacessível para quem não faça parte dela, e por fim permite partilha de tráfego. [Microsoft, 2012]

Ao utilizarem a VPN, os utilizadores conseguem-se conectar ao seu local de trabalho e podem aceder a recursos remotos na rede. A utilização de VPNs garante o cumprimento de alguns requisitos de segurança, tais como:

- Autenticação por acesso remoto, prevenindo acessos não autorizados à rede;
- Confidencialidade - um atacante que tente aceder à rede não consegue ter acesso aos dados pois são usadas técnicas de encriptação para prevenir acesso à informação privada;
- Integridade - as mensagens são transmitidas através de tuneis virtuais cifrados, o que garante a integridade das mensagens transmitidas.

A VPN pode ser configurada apenas para permitir o acesso a professores e funcionários da escola.

Manutenção de sistemas de informação

Processamento correto nas aplicações

As aplicações de gestão devem garantir um correto processamento de dados. Sempre que seja utilizada uma aplicação de gestão, deve-se permitir a validação dos dados de entrada através da verificação do tipo de dados, tamanho do campo, entrada duplicada de caracteres, etc. É o caso da aplicação “alunos”, onde os professores registam as notas, faltas, etc., e onde um simples erro de digitação pode trazer consequências graves.

Gestão de vulnerabilidades técnicas

Deve-se fazer uma constante identificação e eliminação de vulnerabilidades, sobretudo quando se utiliza a Internet, pois esta dá origem a inúmeras vulnerabilidades. É importante configurar corretamente o firewall e utilizar um software antivírus que faça atualizações automáticas.

O coordenador de informática é o responsável pela análise dos logs e dos alertas lançados pelo sistema de monitorização, competindo ao coordenador detetar vulnerabilidade e decidir quais as sanções a aplicar.

Gestão de incidentes de segurança

A gestão de incidentes de segurança da informação é feita através dos relatórios de eventos de segurança e o sistema de deteção de intrusão na rede, tendo em vista a anulação destes incidentes e a melhoria do SGSI.

O coordenador de informática é o responsável pela análise regular destes relatórios, devendo comunicar resultados à Direção sempre que se verifique alguma irregularidade.

Gestão da continuidade do negócio

A presente política foi implementada de modo a contribuir para a continuidade da atividade da escola em caso de falha na rede ou nos equipamentos.
É importante manter um inventário detalhado de todo o equipamento e software, licenças, cópias de segurança, bem como de todos os ativos da escola.

Em desenvolvimento

Para que o SGSI seja adequado à realidade da escola é necessário desenvolver algumas tarefas que não estão contempladas nesta proposta, tais como:

- Gestão dos ativos.
- Análise de risco, requisitos de segurança e aceitação de risco. Esta análise é que caracteriza a organização e consequentemente o SGSI. Existem vários softwares disponíveis que oferecem as ferramentas necessárias para fazer uma correta gestão de riscos, como é o caso do vsRisk v1.6, que está alinhado com a ISO 27001 e com a ISO 27002. [Beckert, 2012]

6.2 Solução 2: Recomendações para o utilizador

Âmbito

Este manual serve como documento de apoio a todos os utilizadores do sistema informático da escola e tem como objetivo assegurar a correta difusão da política de segurança da informação, fornecendo aos utilizadores a informação necessária de como devem interagir com o sistema de modo a não comprometer a segurança do mesmo.

Através deste manual pretende-se que toda a comunidade escolar saiba adotar uma postura correta perante o sistema, percebendo porque foram tomadas certas opções e quais os mecanismos escolhidos para tentar implementar um sistema mais seguro. Para elaborar este documento foi considerada a norma ISO 27002, as deliberações do *esafetyLabel* e as recomendações de segurança da Internet Segura.

Este documento está organizado ao longo de 3 secções principais:

- A secção I, infraestrutura, tem a informação relativa à infraestrutura física do sistema,
- o ponto II diz respeito à política implementada pela escola, onde está definido o que se pode e o que não se pode fazer,
- o ponto III diz respeito a um conjunto de boas práticas que o utilizador deve adotar para garantir a segurança na navegação.

I - Infraestrutura

1. A rede informática da escola está organizada da seguinte forma: existem 3 tipos de perfis, o de alunos, o de professores e o de gestão administrativa (secretaria e Direção). Cada um dos perfis tem privilégios distintos, havendo uma separação lógica entre a plataforma de aprendizagem e a plataforma administrativa.
2. Todos os computadores têm antivírus instalado e as licenças são legais, o que permite que as atualizações sejam instaladas automaticamente. Os computadores estão configurados para que, sempre que seja iniciada sessão, seja feito um scan automático pelo antivírus.
3. A escola disponibiliza internet gratuita a todos os alunos, quer por cabo, quer por wireless.
4. A escola é responsável por toda a cablagem e gestão do equipamento, assim sendo os utilizadores estão proibidos de manusear o equipamento, desligar cabos, alterar ligações, etc.
5. A escola disponibiliza uma impressora para que os alunos possam realizar impressões. Está localizada na biblioteca e apenas a funcionária tem autorização para colocar papel e retirar as impressões.
6. Para além dos computadores instalados nas salas de aula, os alunos e professores podem requisitar um computador portátil por um período de tempo (normalmente 1 aula de 90 minutos), sendo necessário preencher o formulário de pedido com 24 horas de antecedência.

II - Política

7. A atribuição de palavras passe é feita de forma automática no início de cada ano letivo. Cada utilizador tem uma palavra passe e um nome de utilizador para aceder ao sistema.
8. Os computadores da escola só conseguem arrancar pelo disco rígido. Com esta medida pretende-se evitar situações em que os alunos tentam arrancar com outro Sistema Operativo através de um dispositivo amovível.
9. O aluno não tem permissões para instalar programas nos computadores da escola. Sempre que seja necessário instalar algum programa no âmbito de quaisquer disciplinas, terá de ser o professor responsável a solicitar a instalação ao coordenador de informática.
10. As portas USB dos computadores estão desativadas, desta forma torna-se impossível a ligação de dispositivos USB, MP3, discos externos, etc. Esta medida visa prevenir a propagação de vírus.
11. Por outro lado, a escola incentiva os seus utilizadores a recorrerem a soluções de cloud computing para armazenamento de ficheiros.
12. Sempre que um aluno queira utilizar um computador, por exemplo na biblioteca, é necessário que preencha uma folha com o nome, número de aluno e hora de entrada e saída. Este registo é feito com o objetivo de controlar os equipamentos, pois sempre que se verifique uma avaria/roubo/danificação propositada, o aluno terá que ser responsabilizado pelos danos causados.
13. O ponto anterior aplica-se também aos computadores da sala de aula. Pretende-se com esta medida diminuir o número de roubos e de material danificado.
14. O aluno está expressamente proibido de ligar ou desligar hardware ou cabos dos computadores, como é o caso do rato, cabos de rede, etc.
15. Não se pode comer ou beber enquanto se utiliza os computadores da escola.
16. O aluno não tem permissões de acesso, a partir dos computadores da escola, para aceder a conteúdo impróprio ou que se considere que pode afetar a sua concentração e desempenho. Serão criadas listas negras com endereços de sites e com termos de pesquisa. Exemplo de sites a que não têm acesso:
    a. Redes sociais,
    b. Youtube
    c. Sites de pornografia…
17. O aluno tem Internet gratuita a partir de qualquer ponto no interior do recinto da escola, podendo utilizar dois tipos de ligação: por cabo ou wireless.
18. A ligação por cabo, nos computadores pessoais, só é permitida se o aluno trouxer um cabo de rede e se houver tomadas disponíveis nas salas de aula. Com esta medida pretende-se verificar um menor número de tomadas partidas e cabos danificados.
19. A ligação via wireless é permitida a partir de todos os computadores, para tal é necessário fazer a configuração da rede. No final deste manual é possível verificar como aceder à rede wireless em segurança.
20. Sempre que se detetar um comportamento estranho, por parte de um aluno, como por exemplo prática de cyberbulling ou outro tipo de crimes, o aluno será encaminhado de imediato para o serviço de acompanhamento psicológico da escola (ou agrupamento) e será chamado o encarregado de educação para ser colocado a par da situação.

21. A escola encoraja todos os alunos a utilizarem as ferramentas de reporte de conteúdos maliciosos sempre que seja detetado material suspeito.
22. A escola compromete-se a contribuir de forma positiva na formação dos seus utilizadores no que diz respeito a práticas seguras na internet. Desta forma, serão realizadas palestras e seminário gratuitos sobre esta temática, ao longo do ano letivo.

III - Boas Práticas

Nesta secção disponibilizamos alguns conselhos de boas práticas que o utilizador deve adotar na interação com o sistema.

Manuseamento do equipamento

- Quando está a utilizar o computador deve-se ter o cuidado de não tapar as aberturas do monitor e da caixa, pois estas servem para que exista uma correta circulação de ar;
- Evitar quedas e pancadas fortes com o equipamento informático;
- Não introduzir quaisquer objetos nos orifícios do computador, sob o risco de choque elétrico;
- Não desligar o computador sem antes encerrar corretamente o sistema operativo;
- Uma vez que cada aluno tem uma senha própria, aconselha-se a terminar sessão sempre que abandone o computador;
- Não sobrecarregar o computador com ficheiros inúteis;
- Cada utilizador tem um volume em disco para gravar os seus ficheiros, no entanto aconselha-se os alunos a efetuar cópia de segurança dos ficheiros mais importantes, como é o caso dos trabalhos de avaliação.

Internet

- Sempre que inserir uma palavra passe salvaguarde a sua privacidade, isto é, verifique se não tem uma câmara direcionada ou alguém a tentar espreitar para a mesma.
- Confirmar a identidade do sistema de autenticação, verificar sempre o endereço existente na barra de endereços, bem como o certificado do servidor.
- Quando são transmitidos dados privados (como dados de autenticação) verificar se esta transmissão é feita por um canal seguro. A comunicação é segura quando aparece um cadeado fechado no browser.
- Fazer sempre o término de sessão. Fechar na “cruz” apenas fecha a janela, mantendo a sessão iniciada do utilizador.
- Não permitir o armazenamento de credenciais de acesso, principalmente em computadores públicos.

- Fazer sempre as atualizações quer do antivírus, quer do sistema operativo ou de qualquer programa instalado no computador pois isto ajuda a mantê-lo em segurança.

Ataques mais comuns na Internet

Para evitar um **esquema fraudulento** deve-se:

- Procurar o máximo de informações sobre a origem das mensagens recebidas,
- Desconfiar sempre que vir algo que pareça suspeito (Ex: remetentes desconhecidos),
- Desconfiar de certas frases, tais como: “Consulte a sua conta”; “Clique na ligação abaixo para aceder à sua conta", etc.

Para evitar o **cyberbullying,** é necessário que toda a comunidade escolar esteja informada sobre as práticas mais comuns neste tipo de crime e as armas disponíveis para o combater. É importante que o jovem se sinta à vontade com os professores ou com os próprios pais para dialogar sobre este tipo de problemas. No caso de estar a ser alvo deste tipo de ataque deve mudar a conta de email e guardar as mensagens para que posteriormente possam servir de prova.

Compete ao educador:

- Ensinar como usar corretamente a Internet,
- Não permitir a partilha de dados pessoais,
- Instalar computadores em locais comuns da casa,
- Instalar software de prevenção de cyberbullying.

Para evitar ser vítima de **phishing**, o utilizador:

- não deve enviar informações pessoais ou financeiras por email,
- não deve clicar em nenhum link, lembrando-se sempre que empresas legítimas não pedem este tipo de informação por este meios.
- deve regularmente ver os extratos do cartão de crédito para verificar se há algum débito indevido,
- deve ser cauteloso ao abrir um anexo de um email que receba, seja quem for o remetente.
- Deve usar sempre um bom antivírus.

O **SPAM** pode-se tornar muito incomodativo, enchendo a caixa de email com assuntos sem interesse. Para não se tornar um spammer basta ter alguns cuidados, tais como:

- Antes de enviar um email pensar se o mesmo é de interesse para o remetente,
- Refletir antes de reenviar emails suspeitos como correntes, lendas, boatos, etc.,
- Respeitar os assuntos nos fóruns e listas de discussão,
- Não utilizar contactos de amigos presentes em listas para enviar propaganda,

- Seguir as normas de etiqueta (netiqueta), como por exemplo preencher o campo assunto do email para que o destinatário decida se interessa abrir, etc.

A forma mais comum de propagação de um **vírus** informático é através da receção de email, mas também pode ocorrer através do download de programas que escondem dentro deles outros programas infetados ou clicando em certos recursos na Internet, etc. Também pode ocorrer se o utilizador não instalar as atualizações do Sistema Operativo, fazendo com que o mesmo vá ficando desatualizado.

Para evitar a propagação de vírus deve-se:

- Ter um antivírus instalado e a fazer atualizações automáticas.
- Não abrir ficheiros de origem desconhecida.
- Manter o Sistema Operativo atualizado.
- Ter uma firewall sempre ativa.

Depois de falarmos sobre as precauções para evitar os ataques mais comuns na internet, parece oportuno sugerir algumas **práticas corretas na utilização de algumas tecnologias** mais populares entre jovens, como é o caso dos telemóveis, blogues, redes sociais, IMS e Chats, tecnologia P2P, correio eletrónico e por fim a utilização da rede wireless.

Telemóveis

Os telemóveis mais recentes, ao permitirem acesso à Internet e partilha de dados, quer através do Bluetooth, quer através de videochamada, podem facilitar alguns ataques à segurança, como é o caso de:

- cyberbullying através do envio de SMS ou MMS com fotos cujo objetivo seja intimidar quem está a receber ou através do envio de fotos de outros jovens, sem que estes tenham dado autorização,
- Receção de Spam com técnicas de phishing,
- Propagação de vírus que pode permitir o acesso a conteúdos no telemóvel através do Bluetooth.

As recomendações para evitar este tipo de perigos passam por:

- não dar o número de telemóvel a desconhecidos,
- não responder a SMS quando desconhecemos quem é o remetente,
- não atender chamadas com número oculto.
- ter sempre saldo no telemóvel para fazer uma chamada de emergência caso seja necessário.

Blogues

Os blogues servem para partilhar informação variada, sob a forma de notícias, funcionando como um diário online. Ao permitir a inserção de comentários por parte de outros utilizadores pode-se dar origem a diversas ameaças, como é o caso do SPAM, do phishing e

do cyberbullying. A colocação de imagens pessoais pode levar a que terceiros façam uso inapropriado delas, por isso é importante que o bloguista seja responsável pelos conteúdos que insere no seu blogue.

As recomendações de segurança para a criação de blogues passam por:

- fazer uma leitura da declaração de privacidade do fornecedor,
- saber se o blogue é pago,
- informar-se se existe algum email para onde seja possível reportar problemas,
- visitar outros blogues do mesmo servidor para verificar se os mesmos interessam.

As questões relacionadas com a privacidade são muito importantes, tais como:

- nunca disponibilizar informação privada,
- não ceder a password a ninguém,
- usar um endereço de email genérico,
- não colocar imagens pessoais,
- definir regras como o tipo de comentários que são aceites,
- ter sempre um plano para o caso de algo correr mal,
- ter um moderador para menores de idade.

Redes sociais virtuais

O grande objetivo das redes sociais é promover a interação entre os utilizadores, facilitando a comunicação. Ao facilitarem o contacto com outros indivíduos, podem representar vários perigos, como é o caso de:

- Roubo de identidades - o atacante rouba as credenciais do utilizador e envia spam ou mensagens contendo phishing para os seus contactos na rede.
- Falsa identidade - como é tão fácil criar um perfil, qualquer pessoa pode criar o perfil que bem entender, isto acontecendo sobretudo com os pedófilos que criam perfis falsos como se fossem uma criança de modo a atrair outras crianças para a sua rede.
- Oferecer demasiados dados pessoais. Deve-se evitar colocar dados como o local de residência ou a escola que frequenta.
- Cyberbullying, praticado através da descriminação, insultos, ameaças, etc.
- Ausência de controlo de idade - embora muitas redes sociais exijam uma idade mínima para criar uma página, isto pode ser facilmente contornado.
- Moderação fraca, pois cada vez são mais os utilizadores e não existem pessoas suficientes para fazer a moderação de conteúdos.

As recomendações para evitar o tipo de abusos anteriormente mencionados passam por:

- Criar palavras passe seguras através da combinação de vários tipos de caracteres e nunca utilizar dados pessoais de referência como datas, nomes, etc.,
- Deve-se aceitar apenas utilizadores que se conheça pessoalmente,

- Colocar o perfil como privado,
- Não aceitar pedidos de amizade quando o conteúdo da página não agradar,
- Não responder a comentários ofensivos,
- Não divulgar dados pessoais, como morada, contacto telefónico, etc.,
- Utilizar as definições de segurança do facebook, como é o caso de apenas permitir que amigos tenham acesso ao nosso perfil e editar as configurações das aplicações e das fotografias definindo quem as pode visualizar,
- Não cair na tentação de marcar encontros com amigos virtuais,
- Não revelar pormenores reveladores através de fotografias, tais como sítios que costuma frequentar,
- Não colocar informações sobre terceiros que possam comprometer a integridade dos mesmos,
- Pedir permissão a outras pessoas antes de publicar fotos delas,
- Falar com os pais, sendo estes adicionados à lista de amigos para que o controlo parental seja mais eficiente.
- No Facebook existe uma opção "denunciar foto" que serve para denunciar conteúdo ilegal, sendo esta denúncia anónima. Isto também é válido para os casos de cyberbullying, em que o jovem é aconselhado a remover o comentário mas antes deve clicar em "denunciar".

Chats e IMs

Como permitem a comunicação em tempo real, podem representar diversos perigos para os mais novos, pois nunca se sabe quem está do outro lado. Este é um dos sítios preferidos pelos molestadores de crianças, para a prática de cyberbulying, para o roubo de identidade e para a fraude através de phishing.

Para prevenir este tipo de ataques deve-se:

- Ter atenção aos temas explorados nos chats,
- Utilizar um nickname que não revele aspetos da nossa verdadeira identidade,
- Evitar preencher dados do perfil,
- Não divulgar informação privada a desconhecidos,
- Não aceitar encontrar-se com estranhos,
- Registar todas as conversas,
- Não abrir ficheiros ou links enviados por estranhos.

Peer-to-peer

Tipo de comunicação que consiste na partilha direta de ficheiros entre utilizadores, muito utilizado para a partilha de ficheiros de áudio, vídeo, programas e software.

Os perigos associados a este tipo de partilha são:

- a violação dos direitos de autor,
- a propagação de vírus,
- a instalação de programas spyware e addware é normalmente intrínseca à instalação do programa para ter acesso ao P2P,
- download de ficheiros falsos - que diz respeito a menores pode ser bastante perigoso, pois estes podem pensar que estão a descarregar uma música mas afinal trata-se de material pornográfico.

O jovem deve:

- certificar-se da qualidade do programa a instalar através de pesquisa prévia na Internet,
- verificar o que contém a pasta de partilha, uma vez que esta está acessível a todos os utilizadores,
- correr um bom antivírus antes de abrir um ficheiro descarregado P2P,
- Se for um menor a utilizar este tipo de serviço deve ser sempre sob vigilância, sobretudo no momento em que abre os ficheiros, uma vez que pode conter material inapropriado.

Correio eletrónico

O email permite o envio de mensagens instantâneas pela Internet e é amplamente utilizado por todo o tipo de utilizadores. Os perigos associados à utilização de email são sobretudo a propagação de vírus através de phishing. Os efeitos de um vírus podem ser:

- recolha de informação, por exemplo recolher a informação dos contactos da caixa de email para depois enviar SPAM para estes,
- criação de uma backdoor para que o atacante passe a ter acesso ao sistema ou para que possa praticar o ataque DoS (negação de serviços),
- um sistema infetado é usado sempre como meio para atacar outros sistemas.

Utilização da rede wireless

As redes wi-fi permitem uma maior portabilidade no acesso à Internet pois dispensam a utilização de cabos. De modo a não expor os equipamentos a possíveis ataques, aconselha-se os utilizadores da rede wireless:

- A ligarem-se apenas a redes wireless que conhecem pois a ligação a redes desconhecidas pode trazer problemas de segurança,
- Quando está a usar uma rede pública ter cuidado ao transmitir dados privados, verificando se o canal é seguro (por exemplo - protocolo https),
- Quando não precisar de usar a rede wireless desligar a placa de rede sem fios,
- Desativar o modo ad-hoc da placa de rede, isto faz com que se ligue apenas a pontos de acesso,

- Usar ligações encriptadas para o ponto de acesso, dando preferência a protocolos seguros. Quando estiver disponível deve optar pelo WPA2, senão opte pelo WPA, em último caso opte pelo WEP, evitando ligar-se à rede wireless sem qualquer tipo de encriptação.
- Assegure-se que o computador tem mecanismos de proteção ativos antes de aceder à Internet (antivírus e firewall).

A comunicação wireless é feita através do espectro eletromagnético, se não houver mecanismos de segurança qualquer pessoa com a tecnologia apropriada consegue invadir uma rede, usando-a para fins indevidos e podendo causar interferência de dados. Assim, para aumentar a segurança neste tipo de rede deve-se:

- Mudar o nome de utilizador e a palavra passe do equipamento de acesso ao meio,
- Esconder o SSID faz com que a rede não seja anunciada pelo ponto de acesso,
- Quando não der para esconder o SSID, deve-se alterar o que veio de origem,
- Filtrar endereços MAC – é possível configurar o ponto de acesso para permitir apenas o acesso a determinados endereços MAC,
- Alterar regularmente a chave de acesso à rede,
- Desligar os pontos de acesso quando não estiverem a ser utilizados.

A adoção destas medidas pode trazer grandes benefícios para os utilizadores da rede wi-fi, pois previne certos problemas de segurança garantido a integridade da informação.

7 Conclusões

Com a realização desta dissertação foi possível tirar várias conclusões. A ausência de legislação e de um ministério da educação que intervenha nas questões referentes à segurança da informação obriga as escolas a desempenharem um papel proactivo na definição de uma política de segurança da informação.

É importante consolidar junto das escolas, dos alunos, dos diretores, dos professores e de toda a comunidade escolar o desenvolvimento de competências TIC, nomeadamente no que diz respeito à criação de hábitos seguros. Neste contexto, a participação das escolas nos projetos da ISECOM e SeguraNet possui várias vantagens:

- Para o professor, que tem um suporte material para desenvolver as suas aulas num tema atual e emergente como o da segurança em sistemas informáticos;
- Para o aluno, que passa a ter a possibilidade de aprender diversos assuntos relacionados com a segurança através da análise do problema e a sua experimentação prática em laboratório;
- Para a escola, pois os alunos, ao estarem informados dos perigos que correm no mundo virtual, provavelmente terão uma atitude mais cuidadosa e correta na utilização dos recursos informáticos;

Concluímos que a solução não passa apenas pela sensibilização dos utilizadores para os problemas de segurança, mas sim pela criação de um sistema que proteja a informação. O crescimento na produção de informação, dentro das escolas, obriga-as a tomar medidas eficazes para protegerem os seus conteúdos, sendo necessário recorrer a ferramentas e normas auxiliares.

As metodologias do tipo ITIL, Cobit e ISO 27001 oferecem vantagens na gestão das TI e proporcionam a certificação em segurança da informação. Mas, uma vez que a implementação de um processo desta natureza é moroso e nem sempre se vêm resultados a curto prazo, só organizações robustas e de maior complexidade costumam apostar neste tipo de soluções.

A ISO 27001 não é usada apenas para o processo de certificação, ao ser aplicada ajuda a organização a criar um SGSI através da definição de uma política de segurança adaptada às suas necessidades. Por sua vez, a ISO 27002 fornece um conjunto de controlos que garantem as melhores práticas para gerir a segurança da informação dentro da escola.

A solução indicada para o problema estudado passa pela criação de uma política de segurança e atividades que reflitam os objetivos do negócio. Neste sentido consideramos a norma ISO 27001, não com o intuito de obter a certificação, mas sim para perceber quais as recomendações e requisitos necessários para a criação de um SGSI. A solução que propomos (ponto 6) passa pela adoção de um modelo de gestão de segurança da informação, elaborado de acordo com a ISO 27002 e oferece-nos a aplicação das melhores práticas de segurança. Propôs-se ainda a adoção de um manual para o utilizador, direcionado aos alunos, com questões menos técnicas e com algumas recomendações de boas práticas na utilização da Internet.

A adoção desta política ajudará a criar um standard na utilização de recursos, a definir regras e a atribuir responsabilidades aos utilizadores. Faz sentido começar na escola esta atribuição de responsabilidades aos alunos, que devem desde cedo ser sensibilizados para a importância que a informação representa na sociedade do conhecimento.

Concluímos que para implementar um sistema de gestão de segurança da informação não basta definir uma política, é necessário analisar as práticas, procedimentos, questões técnicas e regulamentares da escola. A adoção de um SGSI é uma decisão estratégica que deve partir da Direção, mas que requer um constante diálogo com o responsável pelas TI, sendo necessário a definição de uma equipa técnica que possa fazer a análise e implementação de controlos.

A solução apresentada não elimina definitivamente os problemas de segurança, pois novas ameaças surgem quase diariamente. Para poder detetar novas vulnerabilidades e ameaças que vão surgindo é importante que seja assumida uma atitude dinâmica e que periodicamente seja repetido o ciclo de gestão PDCA.

7.1 Trabalho futuro

A adoção da ISO 27002 ajuda a criar um sistema que protege a segurança da informação e é um forte contributo para obter a certificação da ISO 27001. A certificação só é conseguida através da realização de auditorias e respetiva documentação dos 5 controlos obrigatórios (SGSI; Responsabilidade de gestão, Auditorias do SGSI, Gestão e revisão do SGSI, Melhoria do SGSI) acompanhada do plano de ação.

O modelo proposto aborda algumas questões relacionadas com o SGSI e com a responsabilidade de gestão e poderá servir como base para o processo de certificação, sendo

necessário desenvolver e documentar as restantes fases. Este processo pode ser facilitado com a aquisição de um software de auxílio.

Como a implementação de um SGSI é um processo que pode levar meses ou até mesmo anos e deve contemplar todos os elementos da organização, a nossa proposta seria as escolas adotarem o modelo proposto e tentarem corresponder aos requisitos da ISO 27001 para que, num futuro próximo, consigam obter a certificação e assim reforçar o cumprimento da segurança.

8 Referências

[APCER,2012] APCER, ISO/IEC 27001- Tecnologias da informação, http://www.apcer.pt/index.php?option=com_content&view=article&id=138%3Aisoiec-27001&catid=8&Itemid=436&lang=pt [último acesso: Out 2012]

[Beckert, 2012] Beckert I.,vsRisk v1.6(Standalone)- the Cybersecurity Risk Assessment Tool (CD-ROM), www.itgovernance.co.uk/products/744 [último acesso: Out 2012]

[Aragão, 2012] Aragão F., Proxies o que são?, http://pplware.sapo.pt/informacao/proxies-o-que-sao [último acesso: Set 2012]

[Atsec, 2007] Atsec information security corporation – ISMS Implementation Guide. 2007. http://www.atsec.com/downloads/documents/ISMS-Implementation-Guide-and-Examples.pdf [último acesso: Set 2012]

[Costa, 2009] Costa A., Monitorização de sistemas informáticos, Modulo 6.Departamento de Engenharia informática. Instituto Superior de Engenharia Informática do Porto.

[Costa,2010] Costa F., As metas de Aprendizagem e a Segurança na Internet, http://www.seguranet.pt/metas [último acesso: Out 2012]

[CPSI, 2005] Comunidade Portuguesa de Segurança da Informação, Certificação da segurança para as organizações - http://ismspt.blogspot.pt/2005/09/certificao-de-segurana-para-organizaes.html [último acesso: Set 2012]

[Calder, 2012] Calder A., Information Security and ISO 27001 – an Introduction - http://www.itgovernance.co.uk/iso27001.aspx#ISOB [ultimo acesso: Out 2012]

[DRE, 2012] Diário da República - http://dre.pt/pdfgratis/2012/06/11401.pdf [último acesso: Out 2012]

[EC, 2012a] European Comission, Safer Internet Programme: Empowering and Protecting Children Online, http://ec.europa.eu/information_society/activities/sip/projects/ [último acesso: Out 2012]

[EC, 2012b] European Comission, European Schoolnet, Safer Internet Programme, http://www.saferinternet.eu/web/insafe-inhope/home [último acesso: Set 2012]

[EC, 2011] European Comission, Coalition to make the internet a better place for Kids, http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition_statement.pdf [último acesso: Out 2012]

[EUN, 2011] European School net, esasetylabel - Be an safety school, http://www.esafetylabel.eu/web/guest/esafetyschool [último acesso: Set 2012]

[Facebook, 2012] Facebook, Centro de Segurança Familiar, https://www.facebook.com/safety [último acesso: Set 2012]

[Ferreira,2009] Ferreira C., Gestão de TI Profissionalizada. Casa dos Bits. Semana nº 915 de 13 a 19 de Fevereiro de 2009,http://www.semanainformatica.xl.pt/915/est/100.shtml [último acesso: Set 2012]

[Google, 2012] Google, Ferramentas de Segurança do Google, http://www.google.com/goodtoknow/familysafety/tools/ [último acesso: Ago 2012]

[HHS, 2012] Hacker High School, Cyber Security Skills for the Real World, http://www.hackerhighschool.org [último acesso: Out 2012]

[inst-informática,2007] Instituto de informática do ministério das finanças, O Instituto de Informática, http://www.inst-informatica.pt/o-instituto [último acesso: Out 2012]

[Internetsegura, 2012a] Internet Segura, Sobre o projeto Internet Segura, http://www.internetsegura.pt/ [último acesso: Set 2012]

[Internetsegura, 2012b] Internet Segura, Riscos e Prevenção, http://www.internetsegura.pt/ [último acesso: Set 2012]

[ISACA, 2012] ISACA, Cobit 5: A Business Framework for the Governance and Management of Enterprise IT, http://www.isaca.org/COBIT/Pages/default.aspx [último acesso: Set 2012]

[ISECOM, 2012] Institute for Security and Open Methodologies, http://www.isecom.org/ [último acesso: Out 2012]

[ISO/IEC, 2005a] ISO/IEC 17799:2005(E), Information technology — Security techniques — Code of practice for information security management. Second edition, 2005-06-15.

[ISO/IEC, 2005b] ISO/IEC 27001 Information technology — Security techniques — information security management systems - Requirements. First edition, 2005-10-15.

[ITIL, 2011] Information Technology Infrastructure Library, What is ITIL? http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx [último acesso: Set 2012]

[Livingstone et al., 2011] Livingstone S., Haddon L., Görzig A., and Ólafsson (2011) *EU Kids Online Final Report*. http://eprints.lse.ac.uk/39351/ [último acesso: Out 2012]

[Livingstone et al., 2012] Livingstone S., Ólafsson K., O'Neill B., Donoso V. Towards a better internet for children, Junho 2012.

[MCTEP,2005] Ministério da Ciência, Tecnologia e Ensino Superior, LigarPortugal – Um programa de ação integrado no PLANO TECNOLÓGICO do XVII Governo: Mobilizar a Sociedade de Informação e do Conhecimento, http://www.ligarportugal.pt/pdf/ligarportugal.pdf [último acesso: Set 2012]

[Microsoft, 2012] Microsoft, Virtual Private Networks http://msdn.microsoft.com/en-us/library/aa503420.aspx [último acesso: Set 2012]

[Min-edu, 2010] Ministério da educação, http://legislacao.min-edu.pt/np4/133/ [último acesso: Out 2012]

[Min-edu, 2003] Ministério da Educação, http://www.drelvt.min-edu.pt/seg-esc/normativos-manual-utilizacao.pdf [último acesso: Out 2012]

[Min-edu, 2008] Ministério da Educação, Internet na Sala de Aula – Redes de Área Local. Estudo de Implementação, http://www.pte.gov.pt/pte/pt/Projectos/Projecto/Documentos/index.htm?proj=27 [último acesso: Set 2012]

[Miranda, 2006] Miranda L., ITIL - Information Technology Infrastructure Library, http://www.sinfic.pt/SinficNewsletter/sinfic/Newsletter88/Dossier1.html [último acesso: Out 2012]

[PTE, 2009] Plano Tecnológico da Educação, http://www.pte.gov.pt/ [último acesso: Out 2012]

[Ramos, 2011] RAMOS, A., Manual de Cópias de Segurança para Documentos Informatizados http://www.sg.min-edu.pt/pt/manuais/ [último acesso: Out 2012]

[Simões, 2011] Simões, J. - Mediações dos usos da internet. Resultados do projecto EU Kids Online. Conferência nacional, 4-2-2011, FCSH-UNL

[Stanek, 2012] Stanek W., Microsoft TechNet - Managing User Profiles, http://technet.microsoft.com/en-us/library/bb726990.aspx [último acesso: Set 2012]

[Snort,2010] Snort – About Snort, http://www.snort.org/snort [último acesso: Out 2012].

[Vasconcelos, 2011] Vasconcelos A., As TIC na Administração Pública – que futuro?, http://www.itsmf.pt/LinkClick.aspx?link=Eventos%2f13+Workshop%2fApresentacao_Governance_TIC-AMA.pdf&tabid=170&mid=700&language=pt-PT [último acesso: Out 2012].

[Wikipedia,2012] Wikipedia, Information Security Management System, http://en.wikipedia.org/wiki/Information_security_management_system