INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA INFORMÁTICA




Os referenciais de segurança da informação e a melhoria contínua: um caso exploratório

ANDRÉ FILIPE FERREIRA TORRES
Outubro de 2014

POLITÉCNICO
DO PORTO

Instituto Superior de Engenharia do Porto

Os referenciais de segurança da informação e a melhoria contínua: um caso exploratório

André Filipe Ferreira Torres

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

Orientador: Doutor António Manuel Cardoso da Costa

Co-orientador: Eng. José Luís da Rocha Sousa

Júri:

Presidente:

Doutor Luís Miguel Moreira Lino Ferreira

Vogais:

Doutor Nuno Alexandre Magalhães Pereira

Doutor António Manuel Cardoso da Costa

Porto, Outubro 2014

Dedicatória

Aos meus pais e à Sofia

Resumo

Pensar a segurança num mundo em constante mudança e tecnologicamente enraizado cria desafios constantes. Mais ainda quando este aspeto é o fator central no desempenho das tecnologias nas organizações e o seu suporte ao desenvolvimento e evolução, que são capazes de sustentar sistemas complexos em diferentes áreas de atuação como a energia, transportes, finanças passando também pela investigação.

Sendo o setor da investigação e ensino um gerador e consumidor de grandes volumes de dados, é fundamental garantir a preservação da segurança da informação que assenta sobre os pilares da confidencialidade, integridade e disponibilidade.

Práticas e políticas para a gestão da segurança da informação têm sido desenvolvidas de modo a proporcionar às organizações um nível adequado para a gestão de segurança da informação. De igual modo, é importante que as organizações e os seus elementos constituintes sejam sensibilizados para este tema.

Nesta dissertação, pretende-se avaliar as diferentes normas para a segurança de informação e auditar uma organização, neste caso uma instituição de investigação na área da saúde, avaliando os seus pontos fortes e fracos e implementando soluções capazes de os resolver ou minimizar.

Com este trabalho concluiu-se que a segurança da informação assenta sobretudo nos processos e pessoas e não nas tecnologias. A auditoria realizada, a avaliação dos processos e a consciencialização das pessoas contribuíram para a implementação de uma cultura de segurança na organização.

Palavras-chave: Segurança da informação, auditoria, gestão do risco, tecnologias de informação, segurança de operações

Abstract

Thinking about security in a changing world and technologically pervasive creates constant challenges. Especially when this aspect is the central factor in the performance of technologies in organizations and their support to the development and evolution, which are capable of supporting complex systems in different areas such as energy, transport, finance, also passing through the research.

Since research and teaching sectors are producers and consumers of large amounts of data, is crutial to ensure the preservation of information security, based on the pillars of confidentiality, integrity and availability.

Practices and policies for the management of security information have been developed to provide an adequate level of information security management to organizations. Similarly, it is important that organizations and their constituents are made aware of this topic.

In this dissertation, we intend to evaluate the different standards for information security and audit an organization, in this case a research institution in health, assessing their strengths and weaknesses and implementing solutions able to solve or minimize them.

This study concluded that information security is primarily based on processes and people and not the technology. The audit, evaluation processes and awareness of people contributed to the implementation of a safety culture in the organization.

Keywords: Information security, auditing, risk management, information technology, operations security

Agradecimentos

Gostaria de agradecer ao meu orientador Doutor António Cardoso Costa pelo contributo e disponibilidade para este desafio.

Ao Laboratório Associado IBMC-INEB, em especial ao Eng. José Luís Sousa e aos colegas de departamento pelo apoio e pela possibilidade de poder realizar este trabalho.

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos e Símbolos

Lista de Acrónimos

AD LDS *Lightweight Directory Services*

ADAM *Active Directory Application Mode*

ASVS *Application Security Verification*

b-on Biblioteca do Conhecimento Nnline

BSI *British Standards Institute*

BYOD *Bring Your Own Device*

Cobit *Common Objectives for Information and related Technology*

CSRF *Cross-Site Request Forgery*

DOM *Document Object Model*

ENISA *European Union Agency for Network and Information Security*

HTML *HyperText Markup Language*

HTTP *Hypertext Transfer Protocol*

I^3S Consórcio de investigação em saúde

IBM *International Business Machines*

IBMC Instituto de Biologia Molecular e Celular

IEC *International Electrotechnical Commission*

INEB Instituto de Engenharia Biomédica

IPATIMUP Instituto de Patologia e Imunologia Molecular da Universidade do Porto

ISACA *Information Systems Audit and Control Association*

ISF *Information Security Forum*

ISMS *Information Security Management System*

ISO *International Organization for Standardization*

ITIL *Information Technology Infrastructure Library*

ITSEC	*Information Technology Security Evaluation Criteria*
LDAP	*Lightweight Directory Access Protocol*
NIST	*National Institute of Standards and Technology*
OML	*Open Methodology License*
OSSTMM	*Open Source Security Testing Methodology Manual*
OWASP	*Open Web Application Security Project*
PCI DSS	*Payment Card Industry – Data Security Standard*
RCTS	Rede Ciência, Tecnologia e Sociedade
SOX	*Sarbanes-Oxley*
SQL	*Structured Query Language*
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
URL	*Uniform Resource Locator*
XHTML	*Extensible Hypertext Markup Language*
XML	*Extensible Markup Language*
XSS	Cross-Site Scripting

1 Introdução

1.1 Enquadramento

Desde o início do desenvolvimento da digitalização das empresas que a segurança da sua informação tem constituído um problema, sobretudo quando essa informação torna-se fundamental para a manutenção do funcionamento organizacional. A abordagem a essa segurança tem variado entre "a nossa informação não é suficientemente interessante para que alguém a queira" ou "toda a nossa informação é importante". Acresce ainda a capacidade instalada de os sistemas tecnológicos e de comunicação se terem transformado numa arquitetura completamente ubíqua. A componente social sofreu também nos últimos anos um incremento fundamental na aceitação da incorporação tecnológica no dia-a-dia com a perceção de que essa introdução aumenta a qualidade dos processos de negócios num mundo cada vez mais globalizado e mais desafiador.

Para além dos meios tradicionais de fluxo da informação corporativa, a Internet emergiu como um novo e fundamental elemento dos sistemas de informação globais, sendo adotado de forma massiva pelos utilizadores, transformando de forma radical o desenvolvimento organizacional. Hoje em dia todas as organizações têm de alguma forma um acesso *web*. Isto permite um novo ponto de contacto na troca de informação e de ligação de dispositivos.

Estes factores entre outros contribuíram para uma cultura organizacional que se caracteriza não apenas por um ambiente tecnologicamente integrado mas também com necessidade de tornar acessível o acesso do utilizador a ferramentas que considera fundamentais. O centro de decisão da plataforma tecnológica organizacional neste ambiente ubíquo move-se abruptamente tendo como centro de decisão o utilizador.

Pode-se definir esta sociedade como sendo uma nova forma de organização social, proporcionada pelas novas características da informação — cara de produzir, mas de reprodução muito barata, graças ao enorme desenvolvimento das TIC. Esta característica repassa toda a sociedade, reclamando novos modos de expressão da cidadania, da relação

interpessoal e interinstitucional, da expressão cultural e, naturalmente, da organização económica e do governo. [Silva, J. A. d., 2001]

Este paradigma faz com que a quantidade de dados gerados hoje em dia seja enorme, e que paralelamente, o número de ameaças e a sua complexidade também têm vindo a crescer, tornando-se assim essencial a implementação de mecanismos capazes de assegurar a segurança da informação e dos meios que a transmitem ou a armazenam. Para combater essas ameaças governos e organizações têm vindo a criar legislações e padrões para assegurar a gestão da segurança da informação. Neste ambiente, a segurança da informação é um elemento fundamental e a sua correta implementação tem de ser uma ferramenta no apoio à relação do utilizador com a organização, passando pelos departamentos de sistemas de informação.

1.2 Objetivos

Neste documento pretende-se aprofundar e aplicar conceitos no âmbito da segurança informática e da informação no seio de uma organização, neste caso o Laboratório Associado do Instituto de Biologia Molecular e Celular e Instituto de Engenharia Biomédica. Os principais objetivos desenvolvidos neste trabalho são:

- Auditar as políticas e processos da organização;
- Identificar os riscos, ameaças e vulnerabilidades da organização;
- Estudar os padrões da gestão da segurança da informação para futura aplicabilidade;
- Sensibilizar os funcionários da organização para a importância da segurança da informação.

1.3 Estrutura da tese

O presente documento está organizado em sete capítulos:

- No primeiro capítulo é feita uma abordagem geral à importância da segurança informática e da informação;
- O capítulo 2 faz uma contextualização do problema, explicando o ecossistema da organização e fazendo uma antevisão da solução;
- No capítulo 3 revêm-se as temáticas da segurança da informação e da segurança informática. São apresentadas as ameaças, riscos e vulnerabilidades mais comuns e é mostrada a importância do fator humano no que diz respeito a assegurar a confidencialidade, integridade e disponibilidade. Inclui um levantamento da legislação nacional para a cibercriminalidade. Por último é apresentado um estudo sobre *frameworks* existentes para a gestão da segurança da informação.;
- No capítulo 4 são apresentados os resultados da auditoria aos recursos e processos da organização. Foi feita também uma análise de risco;

- No capítulo 5 são mostrados os resultados da implementação da solução;
- No sexto capítulo são apresentadas as conclusões e o trabalho futuro.

2 Contexto

A massificação das tecnologias de informação referida no capítulo anterior, estão intimamente ligadas aos avanços da investigação científica. Permitiu às instituições de investigação e seus elementos constituintes acederem e partilharem fontes de informação necessárias para novas descobertas científicas.

O Laboratório Associado IBMC-INEB, doravante chamado LA IBMC-INEB, é uma parceria do Instituto de Biologia Molecular e Celular e do Instituto de Engenharia Biomédica. É uma instituição de investigação e ensino nas áreas das ciências da vida, saúde e biomedicina. O LA IBMC-INEB conta atualmente com mais de 600 colaboradores – cerca de 500 investigadores e 100 técnicos. Em termos de organização o LA IBMC-INEB é composto por 56 grupos de investigação divididos por 6 divisões: Infeção e Imunidade, Biologia Molecular e Celular, Neurociências, Biomateriais, Sinal e Imagem Biomédica e grupos associados. 12 serviços de apoio à investigação e 14 grupos de serviços administrativos suportam também esta estrutura.

A incorporação das novas tecnologias da informação no LA IBMC-INEB ofereceu novas oportunidades, novos modelos de negócio e um conjunto de vantagens competitivas associadas, permitindo melhorias de eficiência e de integração entre os diferentes sistemas.

O que alguns autores chamam de sociedade da informação [Toffler, A., 1980] traduz-se no bem mais precioso, a informação. Essa informação está presente em todo o processo do *core business* da instituição, que é a de fazer investigação. Todavia, instituições deste tipo também dependem de outras unidades capazes de assegurar o bom funcionamento e até mesmo assegurar a competitividade da instituição. É exemplo disso o Departamento de Sistemas de Informação, que é responsável pelo desenvolvimento, implementação e gestão de um conjunto de tecnologias para a comunidade do LA IBMC-INEB, desde o Departamento Administrativo-Financeiro ao apoio dos grupos de investigação. É neste contexto de diversidade, competitividade, inovação, mudança e crescimento contínuo que emergem novos riscos que ameaçam um dos ativos mais valiosos para os processos do negócio – a informação.

Os tipos de ameaças à informação assentam sobre 3 pilares: confidencialidade, integridade e disponibilidade e dado que neste caso se trata de uma instituição de investigação as motivações que poderão levar à violação destes três pilares poderão passar pela espionagem organizacional com o objetivo de criação de patentes, passando por grupos de defesa animal contra a experimentação animal.

Torna-se necessário dotar a organização de soluções capazes de responder a este tipo de ameaças. As soluções poderão passar por implementação ou desenvolvimento de tecnologias, aplicação de normas de segurança, desenvolvimento de um plano de segurança, criação de procedimentos para gerir incidentes, especialização dos colaboradores do departamento de sistemas de informação, adoção de normas de disponibilização e serviços com controlo de qualidade e sensibilização dos utilizadores para as questões da segurança informática. Como forma de proteger a organização das ameaças, quer interna quer externas, adotar-se-á a implementação de um conjunto de normas para a gestão da segurança da informação, que servirá também como modelo de referência para o futuro consórcio de investigação em saúde I^3S, que corresponde à junção dos institutos de investigação IBMC, INEB e IPATIMUP.

3 Estado da arte

3.1 Segurança informática e da informação

Quando se trata de segurança da informação e segurança informática existe alguma confusão na sua correta definição, apesar de serem complementares, estas têm objetivos diferentes. A segurança informática é responsável pela proteção dos sistemas informáticos onde a informação é normalmente guardada ou transmitida. A norma internacional ISO/IEC 13335-1 de 2004 define segurança informática como sendo um termo relacionado com a implementação e manutenção da confidencialidade, integridade, disponibilidade, irrefutabilidade, responsabilidade, autenticidade e confiabilidade dos recursos da informação.

Já a segurança da informação não se trata de um produto ou tecnologia, mas sim um processo [Kevin, M., Williams, S. and Steve, W., 2002] mais abrangente que, para além de ser responsável pela proteção da informação armazenada digitalmente em computadores é também responsável pela informação guardada de diferentes formas e através de diferentes canais, por exemplo documentos impressos ou escritos. A norma internacional ISO/IEC 27002 define-a como sendo a preservação da confidencialidade, integridade e disponibilidade.

Diferentes autores definem a expressão "Segurança da Informação" de formas também elas diferentes. [Sêmola, M., 2003] define segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Por sua vez, [Mitrović, P., 2005], defende que a segurança da informação é um termo que descreve a necessidade de proteger as informações com base no facto de que a informação é classificada como um ativo valioso. Para [Anderson, R., 2008], a segurança da informação é sobre poder. Trata-se de determinar quem será capaz de conceder (ou negar) o uso de um recurso. Já [Whitman, M., Mattord, H., 2011] consideram a segurança da informação como sendo a proteção das informações e dos seus elementos essenciais, incluindo os sistemas e hardware que usa, armazena e transmite essa informação.

Como referido anteriormente e também defendido por [Harris, S., 2005], a segurança da informação assenta em três pilares:

- **Confidencialidade** – Garantir que a informação não é disponibilizada ou acedida por pessoas ou entidades sem autorização;
- **Integridade** - Proteger informações, incluindo programas, backups, tempos de criação do arquivo, documentação sejam excluídas ou alteradas sem a permissão do proprietário das informações;
- **Disponibilidade** - Assegurar que os serviços não são degradados ou ficam indisponíveis sem autorização.

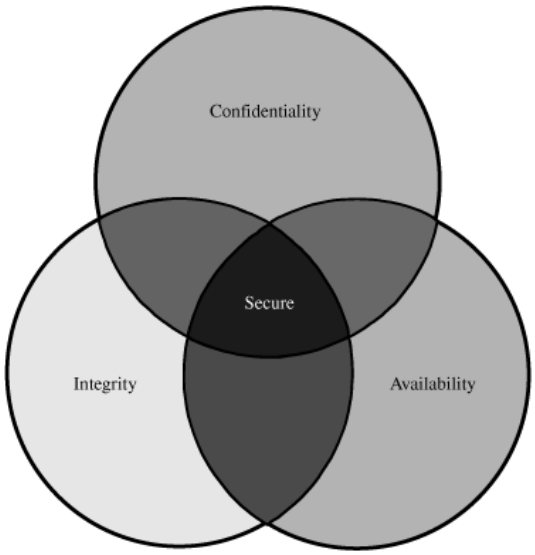

Figura 1 – Relação entre confidencialidade, integridade e disponibilidade retirado de [Pfleegeer, C. e Pfleeger, S., 2006]

Desde o primórdio da civilização que o Homem demonstrava preocupações nas questões da segurança da informação. Essas preocupações podem ser encontradas desde o império romano onde a necessidade de assegurar que a informação só seria acedida por determinadas pessoas fez com que a criptografia se tornasse cada vez mais complexa. São exemplo disso a cifra de César, uma cifra de substituição na qual cada letra do texto é substituída por outra e foi usada pelo imperador romano Júlio César para trocar informações com fins militares entre os seus generais. Passando pela era dos descobrimentos (entre o século XV e XVII) onde a possessão de mapas detalhados contendo indicações de marés e ventos significava uma vantagem competitiva sobre as restantes nações e que precisava de ser salvaguardada.

Avançando para o século XX, na década de 70, a IBM desenvolveu computadores que foram em grande parte utilizados por departamentos governamentais dos EUA e grandes empresas (dado o seu custo e tamanho), facto que levou ao surgimento das questões da segurança da informação, mas desta vez sob a forma digital. No setor militar impunha-se que a informação classificada teria de ser tratada de forma segura. Nos outros setores governamentais os dados sensíveis, como informação pessoal dos cidadãos, implicava a implementação de mecanismos de controlo de acesso.

A década de 80 representa o surgimento dos computadores pessoais, estes eram de menores dimensões que os seus antecessores, com preços mais acessíveis e já possuíam uma interface gráfica, software de produtividade, programação e jogos. Esta massificação foi também acompanhada pelo surgimento da Internet nas empresas, o que acabou por impulsionar o número e tipos de ataques a sistemas informáticos, desde vulnerabilidades do tipo força bruta para descoberta de passwords até a de explorar as más configurações existentes nos computadores. Exemplo disso, em 1988 um *worm* conseguiu infetar entre 5% a 10% do número de computadores ligadas à Internet, um valor que representava cerca de 60000 máquinas. [Networkworld, 2008]

Nos anos 90, a utilização do protocolo HTTP e da linguagem HTML, em conjunto com browsers gráficos, alterou por completo a forma como comunicamos. Um computador ligado à Internet significava que deixava de ser possível controlar que tipo de *inputs* eram enviados para a máquina, por exemplo *Stack Smashing*. Com o aumento do número vulnerabilidades reportadas, empresas como a Microsoft, Compaq, IBM, Intel e Hewlett-Packard fundaram em 1999 a *Trusted Computing Plataform Alliance* com o objetivo de tornar a Internet um lugar seguro para os utilizadores.

Com o aparecimento da *Web 2.0*, o utilizador passou a ter um papel dinâmico na Internet, deixando de ser um mero espectador para ser um membro participativo. *Web 2.0* é o termo usado para descrever uma variedade de recursos onde é possível compartilhar, colaborar, comunicar e criar conteúdos, como são exemplo disso sítios como o *Facebook*, *Youtube* ou *Wikipedia*. O número de ameaças na *Web* também aumentou devido a fatores como a utilização de servidores *Web* mal protegidos ou configurados, bases de dados que aceitam pedidos genéricos, uso de computadores com *software* desatualizado ou dispositivos de proteção mal configurados.

A informação nas organizações pode existir nos mais variados suportes: papel, armazenado ou transportado eletronicamente, o que faz com que cada vez mais as empresas procurem encontrar soluções no que diz respeito à sua proteção. Essa procura é devida ao facto de a informação ser um ativo importante para os negócios da organização. Segundo [Dias, 2000], a informação é o principal património da empresa e está sob constante risco.

3.2 Panorama atual

A Internet tem tido um grande impacto em todas as partes da sociedade. A vida quotidiana passando pela economia dependem cada vez mais das tecnologias de informação tornando-se estas no foco central do crescimento económico mundial. No caso português e de acordo com o relatório "A Sociedade da Informação em Portugal" de 2010, 60% dos agregados familiares possuíam computadores e destes, 50% tinham ligações de banda larga à Internet e 75% das pessoas referiram que usavam a Internet todos ou quase todos os dias. No que diz respeito às empresas, o mesmo relatório refere que 97% das empresas usam computador e que 94% têm acesso à Internet. Para o caso especifico das instituições que se dedicam à investigação

científica, o relatório diz que 86% do sistema nacional do ensino superior estava coberto pela RCTS onde se verificou que 5,6 milhões de downloads de artigos de publicações científicas internacionais disponibilizadas através da *b-on*. Do ponto de vista global 39 em cada 100 habitantes, em 2013, usavam a Internet. O número aumenta para 77 por cada 100 habitantes nos países industrializados.

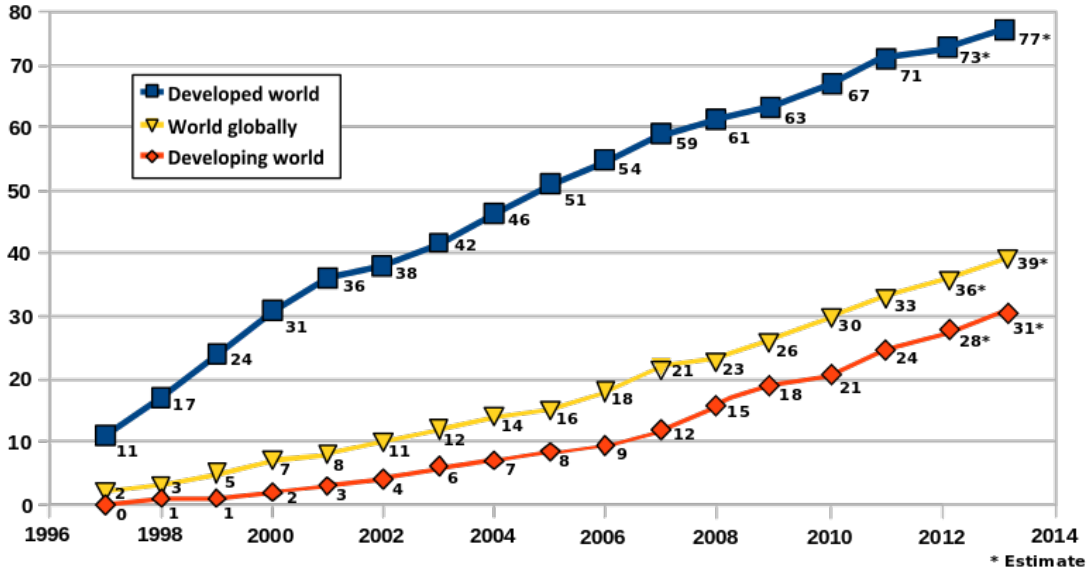

Figura 2 - Utilizadores da Internet por cada 100 habitantes, retirado de [Wikipedia, 2014]

Pode-se afirmar que a Internet tal como a conhecemos promove um espaço livre de partilha de informações e de ideias, quebrando barreiras políticas e sociais. No entanto, esta liberdade existente no ciberespaço acarreta também problemas relacionados com a segurança. [Tanebaum, A.S., 2003] definia a Internet como sendo um sistema fora do normal no sentido de não ter sido planeado nem ser controlado por ninguém.

Tanto os governos como o setor privado deverão ter um papel importante em assegurar a liberdade e respeito pelos direitos fundamentais e garantir a fiabilidade da Internet. Áreas da energia, saúde, transportes ou banca, dependem fortemente da segurança na Internet. Como exemplo, no ano de 2012 o mercado de compras online atingiu o valor de 1 trilião de dólares um aumento de 21,1% em relação a 2011. [Emarketer, 2013] Mas ao mesmo tempo que aumentam o número de transações online o número de fraudes também aumenta. Já em 2006 uma em cada dez pessoas foi vitima de fraude online e em 2011 as perdas relacionadas com a fraude online representaram 3,4 biliões de dólares.

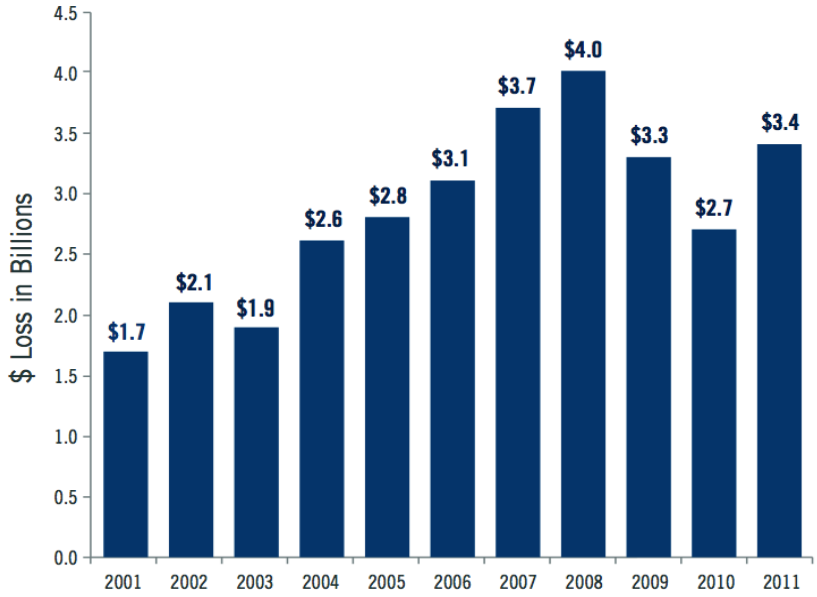

Figura 3 – Perdas de receitas online devido a fraude informática. Retirado de [Net-Security, 2012]

Outro fenómeno que tem tido grande destaque no que diz respeito à segurança informática é o *hacktivismo*. Podendo em alguns casos não estar relacionado com o crime informático, o *hacktivismo* pode ser definido como uma forma de promover ideais políticos na Internet. Este está também muitas vezes associados ao roubo e exposição de documentação de caráter confidencial ou pessoal. São também associados a atos de *defacing* de páginas *Web* ou ataques de negação de serviço com o intuito de fazer reivindicações políticas ou sociais.

São exemplo disso os grupos como os *Anonymous* ou *LulzSec,* que possuem ramificações em diferentes países, Portugal incluído. Foram noticiados, por exemplo, roubos de 1,5TB de dados do Departamento de Justiça dos EUA [Mashable, 2012], ataques de negação de serviço a sítios do governo do Reino Unido [Sol, 2012], divulgação de informação confidencial associada a contas bancárias de 1 milhão de pessoas [Sol, 2012] ou, em Portugal, ataques a sites de partidos e governamentais. [RR, 2013]

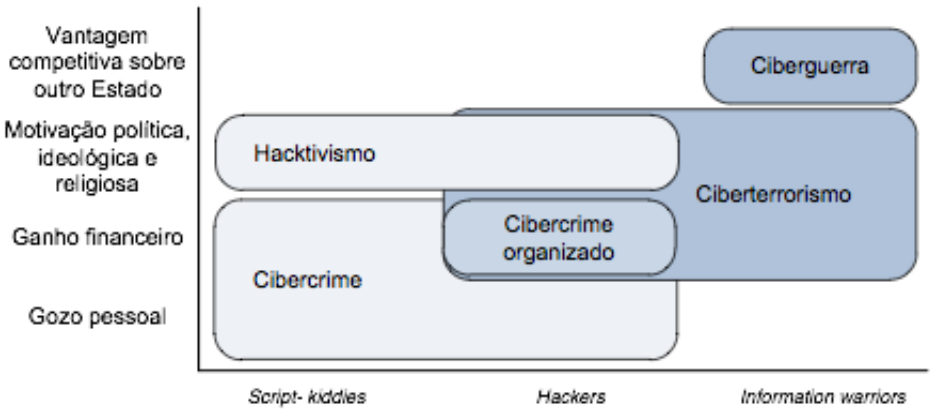

Figura 4 – Motivações dos ataques. Retirado de [Santos, J., 2011]

Vieram também à ribalta casos mais mediáticos como o da *WikiLeaks*, que se trata de um website onde são publicados documentos e informações confidenciais usurpadas de governos ou empresas. [CNN, 2013] A maior notoriedade deste caso deveu-se sobretudo à divulgação de informações sobre as incursões militares no Iraque e Afeganistão por parte dos EUA, levadas a cabo pelo soldado Bradley Mannings, onde são reportadas violações dos direitos humanos e crimes de guerra. [Guardian, the, 2013] Em 2013, um novo escândalo veio alertar as pessoas para a segurança da informação e a privacidade, quando Edward Snowden divulgou detalhes da vigilância de comunicações e tráfego de informações a nível mundial perpetrado pelo governo dos EUA [BBC, 2013], e em 2014 fotos de celebridades americanas foram expostas publicamente, possivelmente, devido a uma falha no sistema iCloud da empresa Apple. [Guardian, The, 2014]

3.3 Tipos de ameaças

3.3.1 Riscos, ameaças e vulnerabilidades

Neste capitulo será debatido o significado de risco, ameaça e vulnerabilidade no contexto da segurança da informação. É importante conhecer o significado destes três conceitos, pois estes funcionam como ponto central para todo o conhecimento das questões da segurança da informação. A Segurança da Informação existe para o gerir o risco e o risco existe em função das ameaças e vulnerabilidades.

A vulnerabilidade neste contexto pode ser definido como uma falha ou debilidade no hardware, software ou processo que pode comprometer um sistema, rede ou aplicação. De acordo com [Wadlow, T.A., 2000] as vulnerabilidades são os pontos fracos existentes nos ativos, que quando explorados por ameaças, afetam a confidencialidade, a disponibilidade e a integridade das informações de uma pessoa ou organização.

No caso da definição de ameaça, o NIST define-a como sendo a intenção ou a motivação que leva um indivíduo, organização ou governo a explorar uma vulnerabilidade. As motivações podem ser de cariz social, político ou financeiro.

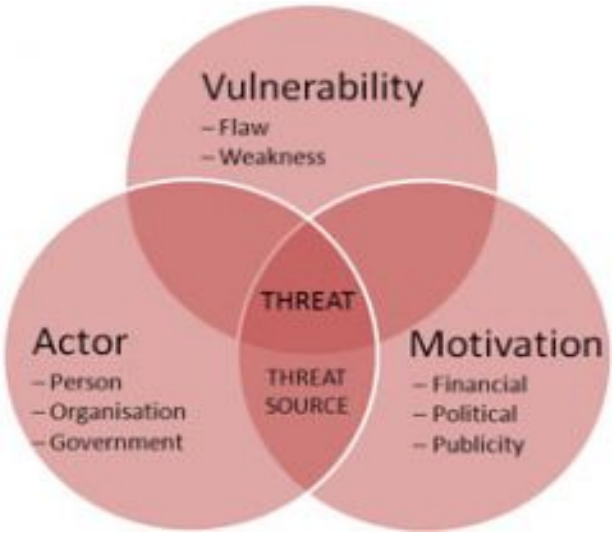

Figura 5 – Fatores que representam a ameaça

A ENISA define risco como sendo qualquer circunstância ou evento com potencial para afetar negativamente um ativo através de acesso não autorizado, destruição, divulgação, alteração de dados e / ou negação de serviço.

O risco é a hipótese de algo não esperado acontecer. É a combinação das ameaças e vulnerabilidades.

Risco = Ameaças X Vulnerabilidades

Figura 6 - Definição de risco, de acordo com a ENISA

A norma ISO/IEC 13335 diz que o risco contém elementos de uma ameaça (ator, motivação e vulnerabilidade), mais o elemento probabilidade e também o elemento do impacto no negócio.

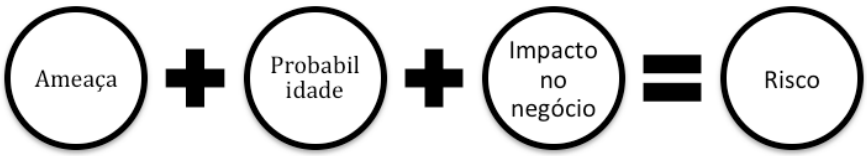

Figura 7 - Definição de risco, de acordo com a ISO 13335

3.3.2 Ameaças à segurança da informação

A ameaça é definida como qualquer causa inesperada ou potencial de um incidente indesejado, que tem um impacto negativo num sistema ou organização. Segundo [Loch, K. D., Carr, H. H. e Warkentin, M. E., 1992] podemos definir as ameaças em quatro dimensões: **Fonte,** que pode ser interna ou externa à organização; **perpetrador** que representa a origem da ameaça, podendo ser humana ou não humana (i.e. ambiental, tecnológica); **intenção** que define se o incidente é acidental ou intencional e a **consequência** do incidente que expõe quais os pilares da segurança da informação (integridade, confidencialidade ou disponibilidade) foram violados.

Figura 8 - As quatro dimensões da ameaça adaptado de [Loch, K. D., Carr, H. H. e Warkentin, M. E., 1992]

Tabela 1 – Exemplos de ameaças à segurança da informação.

Tipo de ameaça	Exemplos
Naturais	Terramotos, vulcões, fogos, tempestades, cheias, acidentes de transporte (carro, avião, etc).
Humanas	Erro humano, sabotagem, vandalismo, roubo, fraude, negligência.
Tecnológicas	*Bugs* no software, defeito técnico.
Competição organizacional	Espionagem, roubo de propriedade intelectual, infração de direitos de cópia.

Lista de ameaças mais comuns realizadas sob o meio digital

As redes informáticas abriram novas oportunidades para a exploração de vulnerabilidades dos sistemas. O roubo ou a corrupção de dados e serviços aumentaram significativamente com a Internet até porque esta está cada vez mais presente no quotidiano das pessoas e organizações. Existem diferentes métodos de ciberataques e ciberameaças que devem ser compreendidos por todos aqueles que façam uso das TIC para melhor se prepararem e defenderem das ameaças.

- **Engenharia social** – é uma técnica usada para obter informações importantes ou confidenciais através da exploração do conhecimento ou confiança das pessoas;
- **Man-in-the-middle** – é uma forma de ataque, em que é intercetada e retransmitida informação trocada entre duas partes num dado canal;
- **Man-in-the-browser** – consiste na infeção do computador da vítima (normalmente um *trojan*) e que é capaz de modificar as comunicações entre o cliente e o servidor de uma maneira impercetível, tanto para a vítima como para a aplicação;
- **Trojan** – é um programa malicioso que é introduzido no computador sem que a vítima o saiba, com o intuito de abrir uma ligação com o computador de atacante de forma a que este tenha controlo sobre o computador da vítima;
- **Worms** – um *worm* é um programa semelhante a um vírus que é capaz de se replicar por um sistema inteiro. Pode ter como objetivos sabotar um sistema informático até apagar completamente dados;
- **Vírus** – é um pedaço de *software* malicioso com o intuito de infetar um computador, e que se pode espalhar para outros computadores;
- **Eavesdropping** – é uma técnica que tem por a base a violação da confidencialidade, através da interceção de uma comunicação privada como uma chamada telefónica ou videoconferência;
- **Phishing** – esta técnica tenta obter dados pessoais como palavras-passe, números de cartões de crédito, etc.. normalmente através do envio de *emails* fraudulentos que tentam fazer-se passar por uma pessoa ou organização de confiança e desta maneira enganar a vítima;
- **Keylogger** – programa capaz de capturar todas as teclas digitadas pelo utilizador;
- **Spyware** – é um programa de computador que é instalado no computador da vítima e que é capaz de recolher informações sobre a vítima, como por exemplo recolher os seus hábitos na Internet, e enviar esses dados para outra entidade;
- **Website Defacement** – é o ato de modificar o aspeto de determinada página *web*. Normalmente este tipo de ataques tem por objetivo a disseminação de mensagens de cariz político ou social;
- **Negação de serviço** – um ataque de negação de serviço tem como objetivo impedir os utilizadores de conseguirem aceder a determinado serviço;
- **Ransomware** - é um tipo de *malware* que restringe o acesso ao computador ou aos arquivos e exibe uma mensagem que exige um pagamento para que a restrição seja

removida. Os dois meios mais comuns de infeção são através de *emails* que contenham anexos maliciosos ou *websites* infetados;

- **Botnet –** um conjunto de computadores infetados que são controlados remotamente. Podem funcionar como um exército de computadores para realizar as mais diversas tarefas como enviar emails contendo *spam*, propagar *malware* ou até mesmo ser usado para realizar ataques de negação de serviço;
- **Clickjacking –** é um método que usa as ações de um utilizador numa determinada página *web* para realizar operações maliciosas. O atacante coloca um *iframe* num elemento clicável, por exemplo um botão, para conseguir que a vitima clique nesse *iframe* e realize sem o seu conhecimento uma operação definida pelo atacante.

3.3.3 Risco de segurança em aplicações – OWASP Top 10

A OWASP é uma organização sem fins lucrativos que se dedica a informar, avaliar e a combater os riscos da segurança de *software.* Um dos trabalhos mais conhecidos desta organização é a lista das dez vulnerabilidades mais criticas nas aplicações *web.* Em 2013, o documento definia os seguintes riscos:

3.3.3.1 Injeção de código

Este tipo de ataque ocorre quando é enviado para um interpretador um determinado parâmetro como parte de um comando ou consulta. Esses parâmetros enviados pelos atacantes podem enganar o interpretador e desta forma conseguir que este execute comandos indesejados. São habitualmente encontrados em consultas SQL e LDAP, usando como técnicas *SQL Injection* e *LDAP Injection,* respetivamente, e podem levar ao comprometimento do servidor.

SQL Injection

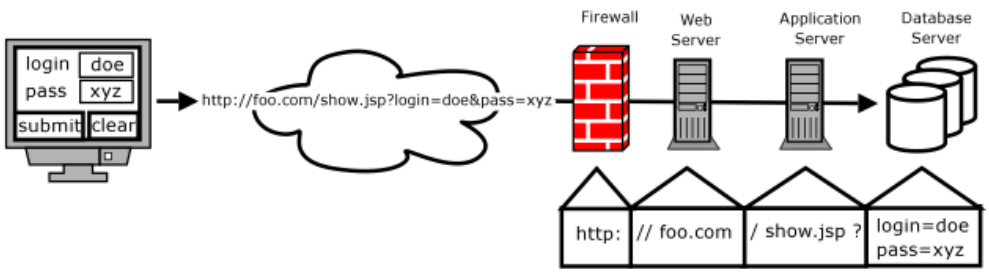

Figura 9 - Processo de um ataque do tipo SQL Injection retirado de [Halfond e Orso, 2005]

- **Tautologias**

Este método de ataque tem por finalidade iludir os sistemas de autenticação, extrair informação e identificar parâmetros injetáveis. Para atingir a seu objetivo, é injetado código numa ou mais condições de forma a que a transformação da condição seja sempre avaliada como verdadeira.

```
SELECT * FROM user_details WHERE userid = 'abcd' AND password = 'anything' OR 'x'='x'
```

Código 1 – Exemplo de uma tautologia adaptado de [Halfond, Viegas, Orso, 2006]

- **Consultas ilegais/Logicamente incorretas**

Neste caso o objetivo é o de identificar parâmetros injetáveis, extrair dados e perceber a estrutura da base de dados. É um método considerado preliminar, pois permite a obtenção de informações relativas à base de dados (nomes de tabelas, campos, etc) e que depois permite escalar para outros métodos de ataque. Ao executar uma condição inválida é retornado uma mensagem de erro descritiva. Estas mensagens servem para os programadores ou administradores de base de dados fazerem *debug* das suas aplicações/configurações. No entanto, muitas aplicações em produção retornam estas mensagens que acabam por ajudar o atacante a atingir o seu objetivo.

```
SELECT accounts FROM users WHERE login='' AND pass='' AND pin= convert (int,(select top 1 name
FROM sysobjects WHERE xtype='u'))
```

Código 2 – Consulta ilegal com o objetivo de causar um erro de conversão de forma a revelar informações. Retirado de [Halfond, Viegas, Orso, 2006]

- **União de consultas**

Este tipo de ataque pode ser feito através da inserção de uma consulta de união num parâmetro vulnerável. Com esta técnica, um atacante pode enganar a aplicação a retornar informações de uma tabela diferente.

```
SELECT accounts FROM users WHERE login='' UNION SELECT cardNo from CreditCards where
acctNo=10032 -- AND pass='' AND pin=
```

Código 3 – Exemplo de união de consultas retirado de [Halfond, Viegas, Orso, 2006]

- **Inferência**

No caso da inferência a consulta é modificada de forma a que a resposta seja verdadeira ou falsa *(true or false).* É usada em bases de dados mais seguras que não retornam qualquer tipo de mensagens informativas capazes de indicar se o ataque está ou não a ser bem sucedido. Assim, o atacante após encontrar um parâmetro vulnerável, injeta condições que ele quer saber se são verdadeiras ou falsas. Ou seja, se a condição for verdadeira a página continua a funcionar normalmente, se for falsa o comportamento será diferente. Este tipo de injeção é

chamado de injeção cega *(Blind Injection).* Existe outro tipo de ataque por inferência chamado de *Time Attack*. Neste método o atacante observa o tempo de resposta da base de dados para verificar o estado do seu ataque. Este ataque apesar de ser parecido com o *Blind Injection*, usa um diferente método de inferência.

```
http://www.example.com/product.php?product_id=100 AND IF(version() like '5%', sleep(15), 'false'))
```

Código 4 - Exemplo de uma consulta pelo método de inferência retirado de [Halfond, Viegas, Orso, 2006]

Na consulta descrita acima, o atacante validará se a base de dados é a versão 5 do MySQL se a resposta do servidor for feita 15 segundos depois.

- **Procedimentos Armazenados *(Stored Procedures)***

Este ataque tenta executar *stored procedures* existentes na base de dados, muitas das quais instaladas por omissão, e que permitem lançar comandos capazes de interagir com o sistema operativo, escalamento de privilégios ou *buffer overflows*.

```
SELECT * FROM user_details WHERE userid = 'abcd' AND password = ''; SHUTDOWN; -- '
```

Código 5 - Exemplo de um *Stored Procedure* adaptado de [Halfond, Viegas, Orso, 2006]

- **Piggy-backed Queries**

Com este método de *SQL Injection* são adicionadas *querys* extra à *query* original. A *query* inicial é executada normalmente assim como as subsequentes, devido por exemplo a uma má configuração da base de dados, permitindo que também sejam executadas.

```
SELECT * FROM users WHERE userid = '1%' AND password = ''; drop table xyz -- '
```

Código 6 – *Piggy-backed query* adaptado de [Halfond, Viegas, Orso, 2006]

No exemplo acima, será executada a *query* original que retornará todos os utilizadores da tabela *users* cujo *userid* começa com o número "1". Depois a base de dados reconhecerá o símbolo delimitador da *query* (";") e executará a segunda *query* que irá eliminar a tabela *xyz*.

- **Encodings**

Neste caso, o atacante injeta texto codificado, usando hexadecimal, ASCII e carateres Unicode para ultrapassar os métodos de defesa, dado que nem todas as técnicas de análise e deteção são totalmente eficazes contra diferentes tipos de codificação.

```
SELECT * FROM users WHERE login= '' AND pass=' ';exec(char(Ox73687574646j776e))'
```

Código 7 – Consulta usando codificação, adaptado de [Halfond, Viegas, Orso, 2006]

No exemplo de cima a função char(Ox73687574646j776e) codifica em hexadecimal o comando *shutdown*.

LDAP Injection

O LDAP *(Lightweight Directory Access Protocol)* é um protocolo para a gestão de diretórios, que permite armazenar informações sobre pessoas, dispositivos e outros aspetos de uma rede. O OpenLDAP, o ADAM e o AD LDS são as implementações mais habituais do protocolo LDAP. Este protocolo baseia-se no modelo cliente/servidor, desta forma o cliente faz o pedido e o servidor envia a resposta com a informação do diretório. Os métodos deste protocolo são os seguintes:

- **Bind** – Autentica e especifica a versão do LDAP
- **Search** – Procura e retorna informações do diretório
- **Compare** – Verifica se tem um determinado valor
- **Add new entry** – Adiciona um novo registo
- **Delete an entry** – Apaga um registo
- **Modify an entry –** Modifica um registo
- **Unbind** – Fecha a ligação

De acordo com o RFC 4515 os filtros usados por este protocolo são:

- **Filter** = (filtercomp)
- **Filtercomp** = and / or / not / item
- **And** = & filterlist
- **Or** = | filterlist
- **Not** = ! filter
- **Filterlist** = 1*filter
- **Item**= simple / present / substring
- **Simple** = attr filtertype assertionvalue
- **Filtertype** = ”=” /” =”/ ”¿=” / ”¡=”
- **Present** = attr = *
- **Substring** = attr ”=” [initial] * [final]
- **Initial** = assertionvalue
- **Final** = assertionvalue

Os ataques do tipo LDAP injection são muito semelhantes aos ataques de SQL injection, na medida em que consistem na manipulação de parâmetros enviados pelo cliente para a aplicação. Se determinada aplicação for vulnerável, o atacante injetará código à sua consulta de forma a ter acesso ou modificação de recursos.

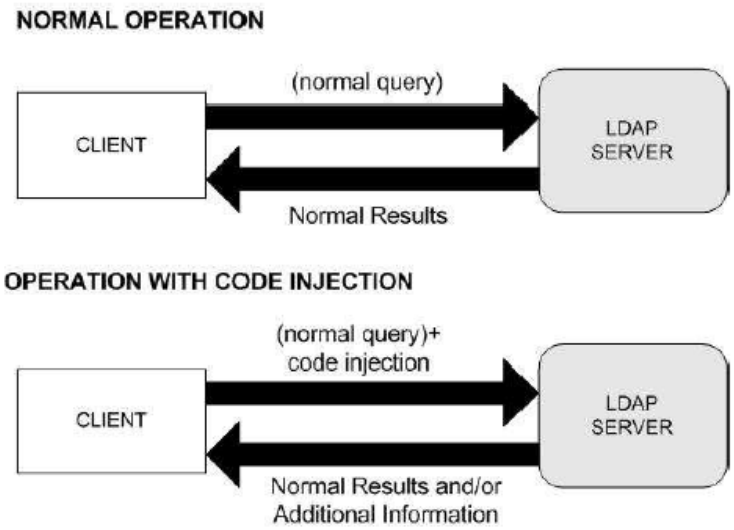

Figura 10 - Processo de consulta LDAP retirado de [Veracode, 2013]

Classic Code Injection

Método mais comum para saber se determinada aplicação é vulnerável à injeção de código. O atacante faz um pedido para o servidor de uma consulta inválida e se o servidor retornar algum tipo de mensagem de erro, este ficará a saber que a sua consulta foi executada e que pode explorar as técnicas de injeção de código para extrair informações.

- **AND LDAP Injection**

Neste caso, é feita uma consulta no diretório LDAP onde é usado o operador AND (“&”) e em que um ou mais parâmetros são introduzidos pelo utilizador.

```
(&(parametro1=valor1)(parametro2=valor2))
```

Código 8 – Consulta LDAP usando o operador AND retirado de [Alonso, Bordón, Béltran e Guzman, 2008]

Por exemplo, num sistema de autenticação em que o utilizador tem de introduzir o utilizador e a palavra-passe é possível fazer com que aplicação permita a autenticação sem possuir uma palavra-passe.

```
(&(Utilizador=ValorUtilizador)(PalavraPasse=ValorPalavraPasse))
```

Código 9 – Exemplo de consulta LDAP para autenticação usando o operador AND retirado de [Alonso, Bordón, Béltran e Guzman, 2008]

No exemplo acima corresponderia à *query* normal que permitiria a autenticação através da validação do utilizador e palavra-passe corretas

```
Utilizador: Maria)(&))
PalavraPasse: 123456
```

```
(&(Utilizador=Maria)(&))(PalavraPasse=123456))
```

Código 10 – Exemplo de ataque através de um sistema de autenticação adaptado de [Alonso, Bordón, Béltran e Guzman, 2008]

Neste exemplo a *query* seria modificada e apenas o primeiro filtro seria processado (&(Utilizador=Maria)(&)). Como o resultado da *query* será sempre verdadeiro, o atacante ganharia acesso ao sistema sem possuir uma palavra-passe válida.

- **OR LDAP Injection**

Neste caso é feita uma consulta no diretório LDAP onde é usado o operador OR ("|") e em que um ou mais parâmetros são introduzidos pelo utilizador.

```
(|(parametro1=valor1)(parametro2=valor2))
```

Código 11 - Consulta LDAP usando o operador OR retirado de [Alonso, Bordón, Béltran e Guzman, 2008]

Este método pode ser usado, por exemplo, pelo atacante para saber quais os recursos disponíveis no sistema.

```
(|(Recurso=Impressoras)(Recurso=Scanners))
```

Código 12 – Exemplo de consulta para obtenção de recursos adaptado de [Alonso, Bordón, Béltran e Guzman, 2008]

```
http://www.exemplo.com/Recursos.php?Recurso=Impressoras)(uid=*))

(|(Recurso=Impressoras)(uid=*))(Recurso=Scanners))
```

Código 13 – LDAP Injection para obtenção de recursos adaptado de [Alonso, Bordón, Béltran e Guzman, 2008]

Blind Injection

Uma maneira de impedir a injeção de código é através da proibição do servidor mostrar mensagens de erro, quando *querys* inválidas são executadas. No entanto, este tipo de filtragem apenas previne as técnicas explicadas no tópico anterior.

Se a aplicação não retornar mensagens de erro, isso não significa que a aplicação esteja segura, já que o atacante pode tirar proveito do facto de que o LDAP gerará sempre uma resposta verdadeira ou falsa.

- **AND Blind LDAP Injection**

```
(&(Recurso=Impressora)(Marca=HP*))
```

Código 14 – Consulta para listagem de impressoras adaptado de [Alonso, Bordón, Béltran e Guzman, 2008]

A *query* acima lista as impressoras da marca HP que existam no diretório. Caso a resposta à consulta seja verdadeira, será mostrado ao utilizador a impressora, caso contrário nada será mostrado. Se o atacante quiser usar o método de Blind LDAP Injection, ele construirá a query da seguinte forma:

```
(&(Recurso=*)(Recurso=*))(& (Recurso=void)(Marca=HP*))
```

Código 15 – Exemplo de uma consulta do tipo blind LDAP injection adaptado de [Alonso, Bordón, Béltran e Guzman, 2008]

No exemplo de cima apenas a parte (& (Recurso=*)(Recurso=*)) é processada, e como o filtro "Recurso=*" é sempre verdade, retornará alguma impressora.

- **OR Blind LDAP Injection**

Neste caso para deduzir a informação é usado o operado lógico OR ("|").

```
(|(Recurso=void)(Recurso=void))(&(Recurso=void)(Marca=HP*))
```

Código 16 – Blind LDAP injection usando o operador OR adaptado de [Alonso, Bordón, Béltran e Guzman, 2008]

A consulta no exemplo acima não retorna qualquer impressora do diretório LDAP. Assim, o atacante pode usar os exemplos abaixo para obter informações.

```
(|(Recurso=void)(Recurso=utilizadores))(& (Recurso=void)(Marca=HP*))

(|(Recurso=void)(Recurso=grupos))(& (Recurso=void)(Marca=HP*))
```

Código 17 – Obtenção de informações usando blind LDAP Injection adaptado de [Alonso, Bordón, Béltran e Guzman, 2008]

3.3.3.2 Quebra de autenticação e gestão de sessão

Quando uma determinada função de autenticação é incorretamente implementada, o atacante pode tirar proveito para assumir a identidade de outro utilizador. Estas falhas são encontradas em contas expostas, ID's de sessão, tempo de expiração, pergunta secreta, etc..

Por exemplo, uma aplicação que envie o ID de sessão no URL pode ser explorada se alguém, que não o próprio utilizador, tiver acesso a esse URL.

```
http://exemplo.com/componentes/item;jsessionid=RLUSWLUTHIEGOUP8AB8?prod=discos
```

Código 18 – Modificação do ID de sessão retirado de [OWASP, 2013]

3.3.3.3 Cross-site scripting (XSS)

Falhas do tipo XSS ocorrem quando o atacante envia um ecerto de código que é capaz de explorar o interpretador do browser da vítima e desta forma poder roubar sessões, inserir conteúdo malicioso, desfigurar websites ou redirecionar o utilizador para outros sites. Existem três tipos de ataques do tipo XSS: Non-persistent, persistente e DOM-based.

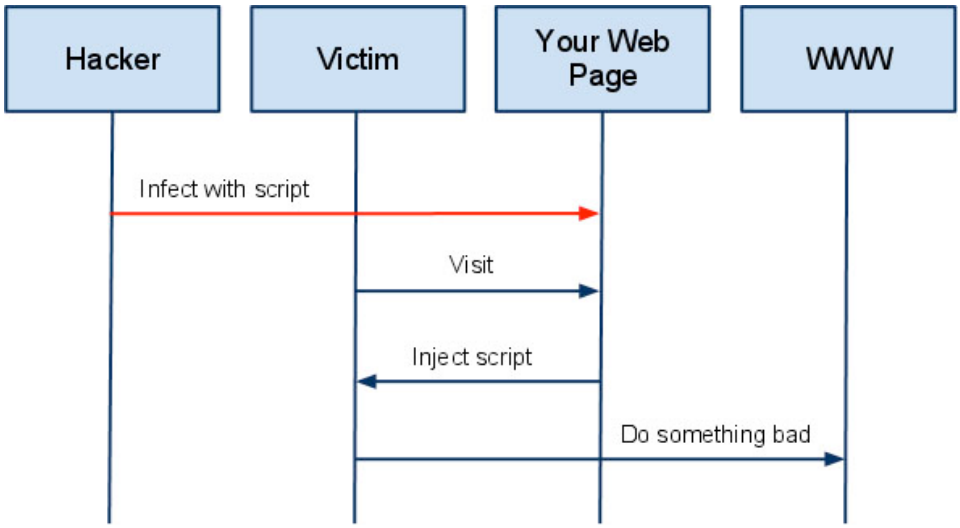

Figura 11 – Diagrama de sequência de um ataque XSS retirado de [Acunetix, 2013]

- **Non-persistent ou Reflected**

Dos três tipos de ataque XSS é o mais comum, mas também é considerado o menos perigoso. É usado sobretudo em ataques de *phishing*. Neste ataque código malicioso é executado pelo *browser* da vítima mas não fica guardado em nenhum lado, sendo enviado como parte da resposta do servidor. Este método pode ser dividido em três partes:

a) Reconhecimento

O atacante procura por sites vulneráveis, tentado injetar código malicioso em páginas que contenham formulários de pesquisa.

```
http://www.exemplo.com/pesquisa.php?termo=<script>alert("XSS");</script>
```

Código 19 – Exemplo de XSS adaptado de [OWASP, 2013]

b) Engenharia Social

Através da engenharia social o atacante procura fazer com que a vítima aceda ao *link* malicioso, usando um dos seguintes métodos:

- Email fazendo-se passar como credível para a vítima contento um link malicioso;
- Website contendo links maliciosos;
- *Clickjacking* que consiste em esconder um website malicioso dentro de um website fidedigno. O utilizador é enganado ao achar que está num site seguro, quando no entanto existe, por exemplo, um *iframe* transparente que pode despoletar ataques de XSS.

c) Execução/Consequências

Após a vítima clicar no link, o código malicioso será executado e ao mesmo tempo serão enviados para o atacante os resultados do ataque. Os objetivos deste ataque são principalmente:

- Roubo de cookies para realizar mais ataques;
- Roubo de informação, que permite ao atacante ter acesso a mais fontes de informação que podem permitir outros ataques.

➢ **Persistent**

Neste método, o código injetado pelo atacante será guardado normalmente numa base de dados. É habitualmente usado em aplicações que possuem sistemas de comentários como fóruns ou blogs. Se o atacante, por exemplo, colocar o seguinte código num *post* de um fórum

```
<script>
document.location='http://www.exemplo.com/xss.php?cookie='+document.cookie;
</script>
```

Código 20 – Exemplo de um ataque XSS persistente retirado de [OWASP, 2013]

um utilizador registado nesse fórum, ao ler essa mensagem, enviaria sem o seu conhecimento a cookie de sessão para o servidor do atacante. O atacante poderia então fazer-se passar por esse utilizador do fórum.

- **DOM Based**

O DOM é uma API para representação e interação com objetos que existem em documentos HTML, XHTML e XML. Define a estrutura lógica de documentos e a forma de como um documento é acedido e manipulado. Na especificação DOM, o termo "documento" é usado no sentido lato - cada vez mais, o XML é utilizado como uma forma de representar diferentes tipos de informações que podem ser armazenados em diferentes sistemas. O XML apresenta estes dados como documentos, e o DOM pode ser usado para gerir esses dados. [w3, 2000]

Um ataque do tipo Dom XSS ocorre quando os scripts do lado do cliente manipulam o DOM da página, permitindo que o atacante execute JavaScript no navegador da vítima. Este ataque é diferente dos outros dois tipos apresentados dado que o servidor não retorna JavaScript executável para o *browser.* Em vez disso, os dados que foram tratados pelo servidor, ou que nunca foram enviados para o servidor são convertidos para JavaScript executável pelo código que está a correr na página.

```
Select your language:
<select><script>
document.write("<OPTION
value=1>"+document.location.href.substring(document.location.href.indexOf("
default=")+8)+"</OPTION>");
document.write("<OPTION value=2>English</OPTION>");
</script></select>
```

Código 21 – Exemplo de DOM XSS

3.3.3.4 Referência insegura e direta a objetos

Este tipo de falhas acontece quando um programador ou administrador de sistemas inadvertidamente expõe determinada informação, como um ficheiro ou um diretório, e que contém informação sensível a pessoas não autorizadas.

3.3.3.5 Configuração incorreta de segurança

A incorreta configuração de aplicações, servidores de aplicações, servidores web, bases de dados ou software desatualizado permitem ao atacante acesso a informação ou funções do sistema e que podem comprometer todo o sistema.

3.3.3.6 Exposição de dados sensíveis

A exposição de dados sensíveis como dados médicos, cartões de crédito e palavras-passe é uma falha que pode ser explorada tanto em dados em tráfego como em repouso. O erro mais comum é a não encriptação desses dados.

3.3.3.7 Falta de função para controlo do nível de acesso

Utilizadores autenticados ou não conseguem ter acesso a determinadas funções para as quais não deveriam ter acesso, simplesmente através da alteração do URL

```
http://www.exemplo.com/app/admin
```

Código 22 - Modificação do URL retirado de [OWASP, 2013]

3.3.3.8 Cross-Site Request Forgery (CSRF)

Um ataque deste tipo permite ao atacante redirecionar o browser da vítima, que tenha uma sessão ativa, a realizar determinada operação sem o seu conhecimento. Por exemplo, a transferência de dinheiro do banco da vítima para a conta do atacante.

```
<img src="http://banco.com/transferirFundos?quantia=1500&contaDestino=12345
/>
```

Código 23 – Exemplo de um ataque CSRF [OWASP, 2013]

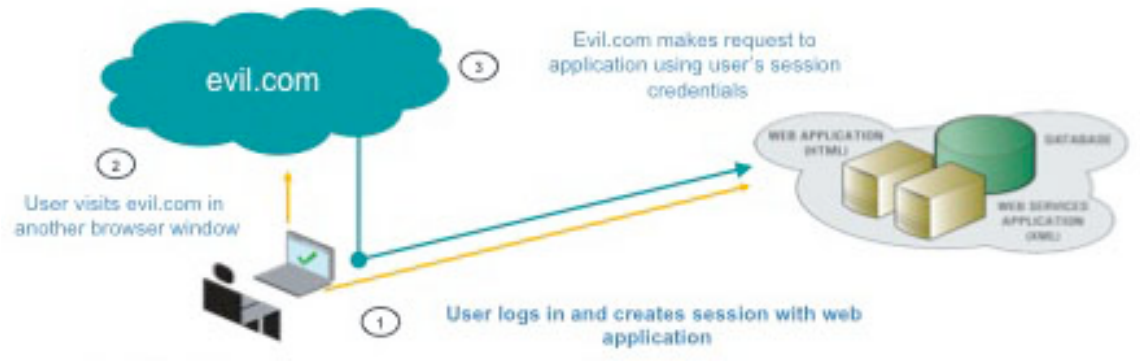

Figura 12 – Processo de ataque do tipo CSRF retirado de [Citrix, 2010]

3.3.3.9 Utilização de componentes vulneráveis conhecidos

Um indivíduo mal intencionado pode tirar partido de vulnerabilidades existentes em bibliotecas, *frameworks* ou módulos. Para isso o atacante procura em bases de dados de vulnerabilidades a forma de a explorar e consequentemente comprometer o servidor.

3.3.3.10 Redireccionamentos e encaminhamentos inválidos

As aplicações *web* normalmente redirecionam os utilizadores para outras páginas, no entanto um atacante pode apontar determinado URL para uma outra página que pode executar ou instalar *malware*.

```
http://www.exemplo.com/redirect.php?url=malware.com
```

Código 24 – Redireccionamento de URL retirado de [OWASP, 2013]

3.4 Fator humano

A segurança é uma combinação de pessoas, processos e tecnologia. [Schneier, 1999] O fator humano torna-se assim numa das principais ameaças à segurança, em especial os funcionários das organizações. Uma arquitetura de segurança é tão forte quanto o seu elo mais fraco (Arce, Iván, 2003). Nesta combinação de pessoas, processos e tecnologia pode-se afirmar que são as pessoas que desempenham um papel crucial na garantia da segurança da organização, mas são também elas o elo mais fraco.

Apesar do fato de que uma quantidade considerável de tecnologia ser projetada para funcionar sem as pessoas, a tecnologia é desenhada para ser gerida e utilizada por pessoas. Não importa o quanto a tecnologia deve ser independente da intervenção humana, as pessoas precisam de interagir com ela em vários pontos no tempo. (Schultz, Eugene 2005)

Um estudo revela que em 2012 14% dos ataques tinham origem interna e 92% tinham origem externa.

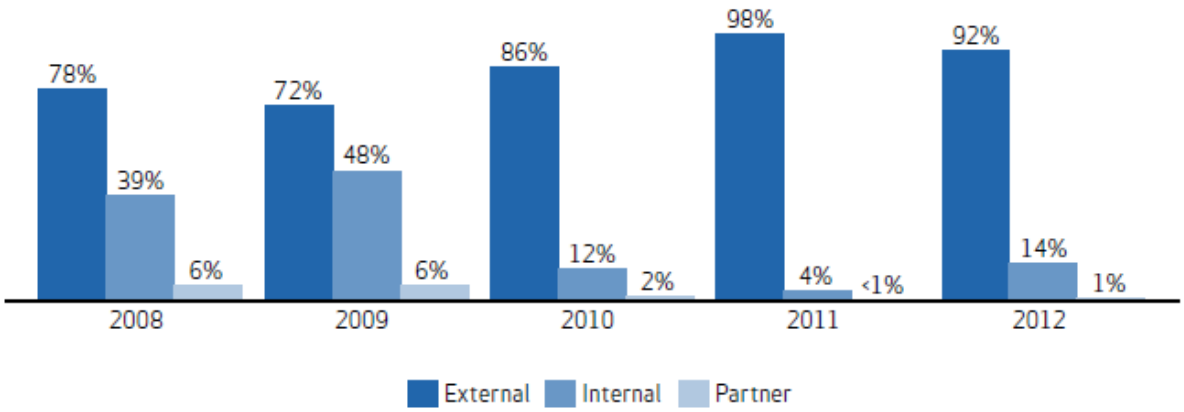

Figura 13 – Origem dos ataques retirado de [Verizon, 2013]

Apesar da diferença ser considerável é necessário ter em atenção os seguintes três pontos:

- Os atores externos são em número maior que os atores internos;
- As ameaças internas acarretam um risco maior para a organização;
- Se contarmos os danos, os ataques internos tendem geralmente a ficar por cima - principalmente porque eles têm a informação muito mais detalhada e podem direcionar melhor os seus ataques. (Schneier, 2008)

Pode-se então considerar que uma proporção substancial de violações de segurança são provenientes de dentro da organização, principalmente devido ao desconhecimento dos utilizadores ou comportamentos negligentes, como a partilha de palavras-passe e abertura de e-mails e anexos de fontes desconhecidas. Essas atividades podem potencialmente abrir a

organização a ataques de *hackers* e consequentemente comprometer os ativos da organização. [Abawajy, 2008]

Os erros humanos que podem pôr em risco a segurança da organização podem ser dos seguintes tipos e exemplos:

- **Erro**
  - Falhas de programação
  - Inserção de dados incorretos
- **Descuido**
  - Não fazer *logoff*
  - Partilha de passwords
- **Fraude**
  - Disseminação deliberada de vírus
  - Criação intencional de funções maliciosas dentro de aplicações
- **Curiosidade/Desconhecimento**
  - Clicar em links de emails maliciosos
  - Instalação de software proveniente de fontes duvidosas

Um método para tirar partido do erro humano por parte dos atacantes é a engenharia social. Este método faz uso da manipulação ou exploração da confiança das pessoas para obter acesso a informações de organizações. Um ataque deste tipo é o *phishing*, no qual os atacantes enviam um email para o(s) alvo(s). A mensagem enviada tira partido do fato da vítima confiar na origem e no conteúdo da mensagem do email, o que normalmente a leva a carregar num *link* ou executar um ficheiro capaz de infetar o computador.

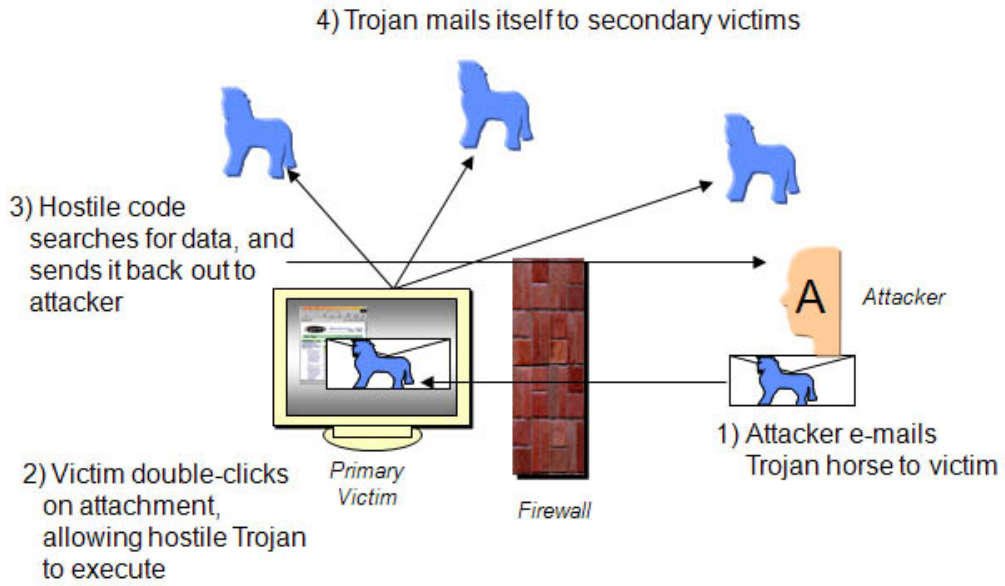

Figura 14 - Exemplo de um ataque de phishing retirado de [Gartner, 2010]

Num estudo global, feito a mais de 1900 empresas de 64 países diferentes e pertences a 25 diferentes setores de negócio, o treino e consciencialização das questões da segurança para os seus funcionários continua a estar em último lugar nas prioridades dos decisores da organização. (Ernst & Young 2013 relatório)

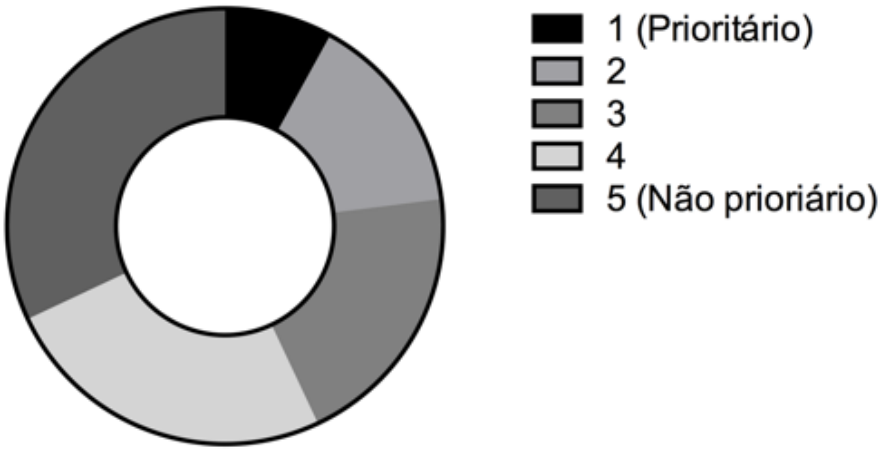

Figura 15 – Gráfico representativo das prioridades das organizações no que diz respeito à consciencialização dos funcionários nas questões da segurança da informação [Ernst & Young, 2013]

Embora os riscos significativos da segurança da informação resultem primeiramente de fatores humanos, as organizações continuam a investir em tecnologia como soluções de segurança (*firewalls*, antivírus, IDS) para defender os bens da organização. (Abawajy, 2012). A segurança da informação continua a ser ignorado pelos gestores de topo, gestores de nível médio e funcionários. O resultado dessa negligência é que os sistemas organizacionais são muito menos seguros do que eles poderiam ser e que as violações de segurança são muito mais frequentes e prejudiciais do que o necessário. (Straub, D.W. & Welke, R.J 1998)

Apesar do uso de tecnologias ser importante na melhoria contínua da segurança organizacional, é igualmente fundamental investir na formação e treino dos funcionários. A formação e a consciencialização da importância da segurança informacional deve ser implementada quer ao nível das pessoas diretamente relacionadas com a área das tecnologias das informação, como também nos restantes utilizadores/funcionários da organização.

Devem ser incutidas as seguintes medidas na organização:

- Sensibilizar os funcionários das suas responsabilidades de segurança e uso adequado dos ativos da organização, dados e tecnologia;
- Contratar as pessoas certas com as habilitações e competências adequadas, incluindo os papéis de alto risco;
- Fazer com que a segurança da informação faça parte da avaliação de desempenho dos funcionários;
- Conhecer e controlar quem detém privilégios elevados.

3.5 Legislação nacional

3.5.1 Enquadramento legal

As questões relacionadas com a segurança informática e a segurança da informação são, em território nacional ou onde a legislação portuguesa seja aplicável, salvaguardadas pelos seguintes decretos lei:

- Lei nº 67/98 de 26 de outubro – Lei da **proteção de dados pessoais**;
- Lei nº 109/2009 de 17 de agosto – Lei do **cibercrime**;
- Decreto Lei nº 62/2003 de 3 de abril – Decreto lei que visa compatibilizar o regime jurídico da **assinatura digital** estabelecido no Decreto lei nº 290-D/99;
- Lei nº 252/94 de 20 de outubro e Lei nº 16/2008 de 1 de abril – Leis da **proteção jurídica de programas de computador**;
- Lei nº 5/2004 de 10 de fevereiro - Lei das **comunicações eletrónicas**;
- Lei nº 41/2004 de 18 de agosto – Lei da **proteção da privacidade no setor das comunicações eletrónicas**;
- Código civil.

3.5.2 Lei da proteção de dados pessoais

A lei nº67/98 refere no artigo 1º *"A presente lei transpõe para a ordem jurídica interna a Diretiva nº 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados."*

No artigo 2º é definido o princípio geral da seguinte forma: *"O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais."*

O ponto 1 do artigo 4º da Lei nº 67/98 "*aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou estes destinados."*

3.5.3 Lei do cibercrime

O objeto do artigo 1º da lei nº 109/2009 *"estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico, transpondo para a ordem jurídica interna a Decisão Quadro nº 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre o Cibercrime do Conselho da Europa."*

As disposições processuais penais materiais e processuais são atribuídas aos seguintes crimes informáticos:

- Falsidade Informática (artigo 3º);
- Dano relativo a dados ou programas informáticos (artigo 4º);
- Sabotagem informática (artigo 5º);
- Acesso ilegítimo (artigo 6º);
- Interceção ilícita (artigo 7º);
- Reprodução ilegítima de programa protegido (artigo 8º).

3.5.4 Leis da proteção jurídica de programas de computador

A lei 252/94 de 20 de outubro de acordo com o ponto 1 do artigo 1º *"transpõe para a ordem jurídica interna a Diretiva nº 91/250/CEE, do Conselho, de 14 de maio, relativa à proteção jurídica dos programas de computador."*

A lei da proteção jurídica de programas de computador abrange algumas questões como:

- Autoria (Artigo 3º);
- Reprodução e transformação (Artigo 5º);
- Direitos do utente (Artigo 6º);
- Descompilação (Artigo 7º);
- Direitos de pôr em circulação (Artigo 8º);
- Direitos do titular originário (Artigo 9º);
- Limites (Artigo 10º);
- Autonomia privada (Artigo 11º);
- Apreensão (Artigo 13º);
- Tutela penal, tutela por outras disposições legais e tutela internacional (Artigo 14º, 15º e 17º respetivamente);
- Vigência (Artigo 16º).

3.5.5 Lei das comunicações eletrónicas

O artigo 1º da lei 5/2004 *"estabelece o regime jurídico aplicável às redes e serviços de comunicações eletrónicas e aos recursos e serviços conexos e define as competências da autoridade reguladora nacional neste domínio, no âmbito do processo de transposição das Diretivas nº 2002/19/CE, 2002/20/CE, 2002/21/CE, e 2002/22/CE, todas do Parlamento Europeu e do Conselho, de 7 de março, e da Diretiva nº 2002/77/CE, da Comissão, de 16 de setembro."*

3.5.6 Lei da proteção da privacidade no setor das comunicações eletrónicas

A lei 41/2004 de 18 de agosto diz no ponto 2 do artigo 1º que *"a presente lei aplica-se ao tratamento de dados pessoais no contexto de redes e serviços de comunicações eletrónicas acessíveis ao público, especificando e complementando as disposições da Lei nº 67/98, de 26 de outubro (Lei da Proteção de Dados Pessoais)."*

O capitulo II da lei da proteção da privacidade no setor das comunicações eletrónicas expõe os aspetos que as organizações prestadoras dos serviços devem ter em atenção em relação à segurança e confidencialidade, e que são os seguintes:

- Segurança (Artigo 3º);
- Inviolabilidade das comunicações eletrónicas (Artigo 4º);
- Armazenamento e acesso à informação (Artigo 5º);
- Dados de tráfego (Artigo 6º);
- Dados de localização (Artigo 7º);
- Faturação detalhada (Artigo 8º);
- Identificação da linha chamadora e da linha conectada (Artigo 9º);
- Exceções (Artigo 10º);
- Reencaminhamento automático de chamadas (Artigo 11º);
- Centrais digitais e analógicas (artigo 12º);
- Listas de assinantes (Artigo 13º).

3.6 Padrões

O crescimento das organizações e a competitividade do mercado global tornaram o papel da segurança da informação um dos pilares do negócio. Todavia, para a sua correta implementação é necessário um conjunto de referências capazes de regular a segurança da organização. Foi a partir deste desafio que surgiu um novo conceito, chamado de Sistema de Gestão de Segurança da Informação, que, para além de tratar a disseminação da informação no meio digital, é também capaz de criar uma cultura de segurança informacional no seio dos utilizadores da organização.

Um sistema de gestão de segurança da informação assegura que são implementadas medidas para garantir a segurança da informação e quais os procedimentos aplicáveis caso exista uma quebra de segurança.

De acordo com Campos (2006), existe um incidente de segurança quando um dos três princípios básicos de segurança é desrespeitado, que são a confidencialidade, integridade e disponibilidade.

Tanto organizações privadas como governamentais têm desenvolvido padrões que procuram assegurar as melhores práticas e níveis da segurança dos dados. São exemplo disso normas como o COBIT, ITIL, ISO 27001, SOX, PCI, OWASP, ...

3.6.1 ITIL

O ITIL é um conjunto de boas práticas que descreve como os recursos das tecnologias de informação devem ser organizadas para acrescentar valor ao negócio, documentando os processos, funções e papéis dos seus intervenientes. O ITIL surgiu nos finais do anos 80, no Reino Unido, quando o governo deste país apurou que o nível de qualidade fornecido pelos serviços de TI não era suficientemente bom.

Em 2001 foi lançada a segunda versão da norma, tornando-se numa das *frameworks* mais usadas pela indústria no que diz respeito às práticas de gestão de serviços de TI. Na versão 3 do ITIL, lançada em 2007 e atualizada em 2011. [ITIL, 2011]

Esta versão está dividida em 5 volumes, num total de 26 processos:

Estratégia de Serviço

- Gestão estratégica;
- Gestão financeira;
- Gestão do Portfólio de serviço;
- Gestão da demanda.

Desenho de Serviço

- Gestão da capacidade;
- Gestão da continuidade do serviço de TI;
- Gestão da disponibilidade;
- Gestão do fornecedor;
- Gestão da segurança da informação;
- Gestão do catálogo de serviço;
- Gestão do nível de serviço.

Transição e Serviço

- Avaliação;
- Gestão da configuração e de ativo do serviço;
- Gestão de libertação e implantação;
- Gestão da mudança;
- Gestão do conhecimento;
- Planeamento e suporte da transição;
- Validação e teste de serviço.

Operação de Serviço

- Cumprimento de requisição;
- Gestão de acesso;
- Gestão de evento;
- Gestão de incidente;
- Gestão doe problema.

Melhoria contínua de serviço

- Mensuração de serviços;
- Processo de melhoria em 7 etapas;
- Relatório de serviço.

Figura 16 - Processo ITIL retirado de [Portalgsti, 2013]

3.6.2 Cobit

O COBIT, criada em 1996 pela ISACA, é uma *framework* para a gestão das tecnologias de informação. O COBIT contém os seguintes componentes: sumário executivo, objetivos de

controlo, mapas de auditoria, ferramentas de implementação e um guia com técnicas de gestão. Em suma, a missão do COBIT é a de desenvolver e promover uma lista de pontos de controlo que seja aceite no dia a dia de gestores de negócio e auditores.

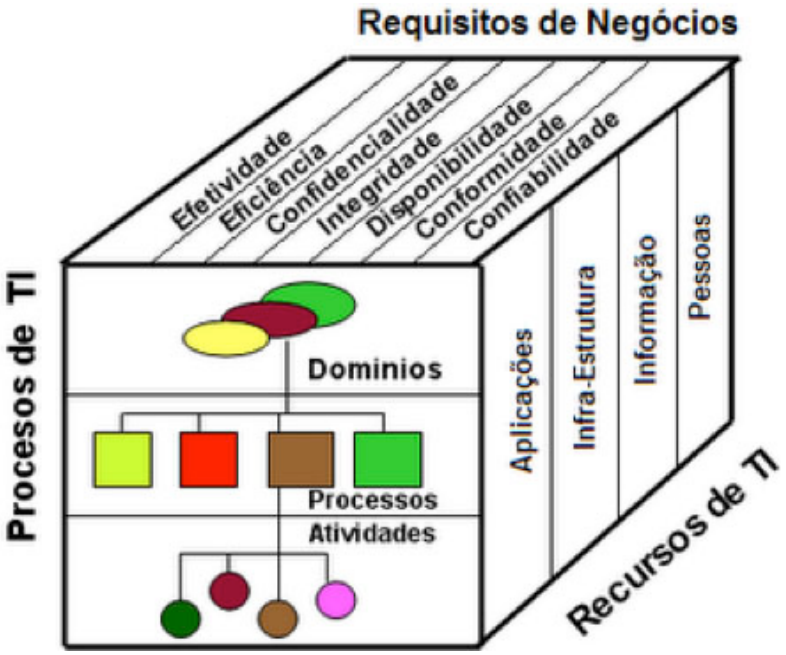

Figura 17 - Cubo de COBIT retirado de [SM3G, 2013]

Na figura acima exibida apresentam-se três dimensões. A primeira, os requisitos de negócio, como um dos pilares das organizações. O segundo, os processos de TI, encontram-se divididos em três níveis: **Domínio** que engloba a capacidade de planear e organizar, implementar, suporte e monitorização; **Processos** que são compostos por 34 recursos divididos nos quatro domínios; e **Atividades** que são as ações necessárias para atingir os resultados. A última dimensão, Recursos de TI, mostra os recursos que são precisos para validar os requisitos através dos processos de TI. [ISACA, 2012]

O COBIT também oferece orientação aos profissionais de segurança de tecnologias de informação a implementar e gerir atividades relacionadas com a segurança da informação.

O COBIT relacionado com a segurança de informação pode:

- Aumentar a satisfação dos utilizadores nas questões relacionadas com a segurança da informação
- Reduzir a complexidade e aumentar a relação custo-eficácia
- Aumentar o apoio à inovação e à competitividade
- Reduzir os incidentes de segurança da informação
- Melhorar a integração da segurança de informação

3.6.3 SOX

Sox é uma abreviatura de Sarbanes-Oxley, uma lei norte-americana criada e proposta pelo senador Paul Sarbanes e deputado Michael Oxley, que acabou aprovada em julho de 2012. Esta lei foi redigida com o objetivo de proteger os investidores, melhorando a precisão e confiabilidade das demonstrações financeiras feitas de acordo com as leis de segurança. Um dos principais motivos foi o escândalo financeiro da empresa Enron.

No SOX não existe um guião específico de implementação e avaliação de controlos internos, por isso as empresas fazem uso de *frameworks* reconhecidas pelas suas boas práticas como são o caso da COBIT ou ISO/IEC 27k. Resumidamente, o SOX foca-se mais na parte do processo que está relacionada com a geração de relatórios financeiros.

Os seus requisitos são os seguintes:

- Controlar a criação, edição e versionamento dos documentos num ambiente de acordo com os padrões ISO, para controlo de todos os documentos relativos à secção 404;
- Registar os riscos associados aos processos de negócios e armazenar os desenhos de processo;
- Utilizar ferramentas como editores de texto e alteração dos documentos da secção 404;
- Publicar em múltiplos websites os conteúdos da secção 404;
- Gerir todos os documentos controlando seus períodos de retenção e distribuição;
- Digitalizar e armazenar todos os documentos que estejam em papel, ligados à secção 404.

3.6.3.1 Secção 404

A secção 404 da lei Sarbane-Oxley diz que deve ser realizada uma avaliação anual dos controlos e procedimentos internos para a emissão dos relatórios financeiros. Será também necessário um auditor independente lançar o seu parecer e validar a eficiência dos controlos internos da organização no que diz respeito aos procedimentos para a emissão dos relatórios financeiros. [SOX, 2012]

3.6.4 PCI DSS

O PCI DSS é um padrão de segurança de informação especialmente dedicado para organizações que tratam informação originária de cartões de crédito e débito ou POS. Com o PCI DSS existe um conjunto de requisitos para a proteção de dados sensíveis incluindo comerciantes, emissores, prestadores de serviços bem como todas as outras entidades que transmitem, processem ou armazenem dados do titular do cartão.

O PCI DSS é composto por 6 objetivos e 12 requisitos:

Construir e manter uma rede segura

- Instalar e manter uma *firewall* para proteger os dados do portador do cartão;
- Não usar a palavra-passe ou outros parâmetros que vêm por defeito nos ativos existentes.

Proteger a informação do titular do cartão

- Proteger a informação do titular do cartão;
- Encriptar a transmissão de dados referentes ao titular do cartão em redes abertas ou públicas.

Manter um programa de gestão de vulnerabilidades

- Usar e atualizar regularmente programas antivírus em todos os sistemas que são habitualmente afetados por *malware*;
- Desenvolver e manter sistemas e aplicações seguras.

Implementar fortes medidas de controlo de acesso

- Restringir o acesso aos dados do titular do cartão;
- Atribuir um ID único para cada pessoa com acesso ao computador;
- Restringir o acesso físico ao titular do cartão.

Monitorizar e testar regularmente a rede

- Monitorizar todo o acesso aos recursos da rede e dados do portador do cartão;
- Testar regularmente a segurança dos sistemas e processos.

Manter um política de segurança de informação

- Manter uma política que aborde as questões da segurança de informação.

Apesar do PCI DSS estar mais focado para transações eletrónicas, a sua correta implementação numa organização aumentará o nível da segurança da informação. [pcisecuritystandards, 2010]

3.6.5 Common Criteria

O *Common Criteria* é um conjunto de diretrizes que foram desenvolvidas para a avaliação dos produtos de segurança e sistemas de computador com o objetivo de garantir que tais produtos e sistemas são capazes de responder às exigências das normas de segurança.
O *Common Criteria* possui dois componentes-chave que definem esses critérios e que são os seguintes:
Perfil de proteção: Define os padrões estabelecidos para os requisitos de segurança exigidos para um produto especifico, por exemplo uma *firewall*.

Evaluation Assurance Level: Define os níveis que são usados para avaliar um produto e indica a forma como o produto foi completamente testado. O nível vai de 1 a 7, sendo 1 o nível mais baixo e 7 o nível de avaliação maior. O produto com nível 7 significa que este passou por mais testes, mas isso não significa que o produto tem nível de segurança superior a outros produtos. [Commoncriteriaportal, 2014]

Com esta norma é possível avaliar a segurança de um sistema ou ser usado para o desenvolvimento de um. Tornou-se em 1999 como norma internacional ISO/IEC 15408

3.6.6 ISF

O ISF é uma organização independente fundada em 1989, que procura através da implementação de melhores metodologias e processos esclarecer e resolver questões relacionadas com a segurança da informação e gestão de risco.
Está estruturado em cinco componentes: Gestão de segurança, aplicações de negócio, instalações de computadores, redes, desenvolvimento e sistemas. Estes componentes são depois divididos em 30 áreas que por sua vez dividem-se em 135 secções. Por exemplo:

Gestão da segurança

- requisitos de segurança;
- segurança da organização;
- ataques.

Aplicações de negócio

- gestão das aplicações;
- ambiente do utilizador;
- gestão do sistema.

Instalação nos computadores

- Gestão das instalações;
- Controlo de acesso;
- Continuidade do serviço;
- Segurança local.

Redes

- Gestão da rede;
- Gestão do tráfego;
- Operações de rede;
- Redes de voz.

Desenvolvimento de sistema

- Gestão do desenvolvimento;

- Requisitos de negócio;
- Testes;
- Implementação.

3.6.7 OSSTMM

No ano de 2000, Pete Herzog criou a OSSTMM, uma *framework* de teste de segurança. O OSSTMM é um documento que pode ser implementado e distribuído livremente já que a sua licença encontra-se ao abrigo da OML. É uma metodologia que está escrita de maneira a que as organizações obtenham o valor máximo de negócio das suas rotinas e atividades. Apesar não falar especificamente em comandos ou ferramentas, o documento consegue abranger vários temas e testes de segurança. [ISECOM, 2012]

O OSSTMM define as seis formas de metodologias de segurança da seguinte forma:

1. **Segurança da informação** (existência de informação de qualquer tipo na Internet de uma entidade qualquer tipo)
2. **Segurança nos processos** (Engenharia social,..)
3. **Segurança de tecnologias da Internet** (Firewall, Intrusion Detection System)
4. **Segurança nas comunicações** (Voip, Modem, Fax,..)
5. **Segurança wireless** (802.11, Bluetooth,..)
6. **Segurança física** (perímetro de segurança, controlos de acesso,...)

3.6.8 ITSEC

O ITSEC são critérios de avaliação da informação estruturados e que foram desenvolvidos na união europeia. O seu objetivo demonstrar a conformidade de um produto ou sistema contra a sua meta de segurança. Atualmente na versão 1.2 é composto por 11 níveis de F0 a F10 para avaliar os requisitos funcionais e 7 níveis de E0 a E6 para avaliar os requisitos de garantia. [ITSEC, 1991]

Requisitos funcionais de segurança

- **F0.** Identificação e autenticação;
- **F1.** Auditoria;
- **F2.** Utilização de recursos;
- **F3.** Caminhos/canais confiáveis;
- **F4.** Proteção de dados do utilizador;
- **F5.** Gestão de segurança;
- **F6.** Acesso ao produto;
- **F7.** Comunicações;
- **F8.** Privacidade;
- **F9.** Proteção de segurança das funções do produto;

F10. Suporte criptográfico.

Requisitos de garantia de segurança

- **E0.** Documentos de orientação e manuais;
- **E1.** Gestão da configuração;
- **E2.** Avaliação das vulnerabilidades;
- **E3.** Entrega e operação;
- **E4.** Apoio ao ciclo de vida;
- **E5.** Garantia de Manutenção;
- **E6.** Desenvolvimento**.**

3.6.9 ISO 27001

A norma ISO/IEC 27001:2005 é uma especificação e uma referência internacional, publicada em 2005, para a gestão da segurança da informação. A sua origem remonta a 1992, quando no Reino Unido foi publicado o documento "Código de boas práticas de gestão de segurança da informação". Em 1995 esse trabalho é republicado pelo BSI com o nome de BS7799. No ano de 2000 a BS7799 é novamente republicada, mas desta vez como uma norma de nome ISO 17799. Em 2013 é publicada a versão atual da norma ISO/IEC 27001. Esta norma tem como objetivos estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação.

A ISO 27001 usa uma abordagem *top-down* com base no risco e é tecnologicamente neutra. A especificação define um processo de planeamento de seis partes:

1. Definir um política de segurança;
2. Definir o escopo do Sistema de gestão de segurança da informação;
3. Realizar uma avaliação de risco;
4. Gerir riscos identificados;
5. Selecionar os objetivos de controlo e os controlos a serem implementados;
6. Preparar uma declaração de aplicabilidade.

A especificação inclui detalhes para a documentação, responsabilidade de gestão, auditorias internas, melhoria contínua e ação corretiva e preventiva. A norma exige a cooperação entre todos os setores da organização.

A ISO/IEC 27001:2013 possui 14 objetivos de controlo:

Tabela 2 - Pontos de controlo da norma ISO 27001

Ref	Controlos
A.5	Política de segurança da informação
A.6	Organização da segurança da informação
A.7	Segurança na gestão de recursos humanos
A.8	Gestão de ativos
A.9	Controlo de acesso
A.10	Criptografia
A.11	Segurança física e ambiental
A.12	Segurança de operações
A.13	Segurança de comunicações
A.14	Aquisição, desenvolvimento e manutenção de sistemas de informação
A.15	Relações com fornecedores
A.16	Gestão de incidentes de segurança da informação
A.17	Aspetos de segurança da informação na gestão da continuidade do negócio
A.18	Conformidade

3.6.10 ISO 27002

A norma ISO 27002 estende a norma ISO 27001 ou seja, os seus capítulos detalham as maneiras de lidar com a segurança da informação. Possui diferentes capítulos para diferentes aspetos da segurança da informação. A segurança da informação normalmente implica tecnologias da informação, mas a ISO 27002 está também focalizada na informação em papel e outros ativos, embora a maior parte da norma foque o departamento das tecnologias da informação.

Na sua primeira versão, a norma ISO 27002 foi concebida para ser uma norma de largo espectro para todas as organizações que necessitavam de segurança da informação. Isso significa que uma empresa governamental, independente ou uma organização sem fins lucrativos pode seguir o mesmo padrão. Resumidamente, a ISO 27002 detalha os controlos e procedimentos envolvidos na manutenção da informação segura. Enquanto a ISO 27001 oferece apenas uma ou duas frases sobre o controlo, a ISO 27002 explica detalhadamente os controlos.

3.6.11 OWASP – ASVS Standard 2009

A OWASP é uma comunidade aberta dedicada a formar as organizações ou indivíduos para o desenvolvimento e manutenção de aplicações confiáveis e seguras. Todos os documentos, ferramentas, fóruns são gratuitos e livres para quem esteja interessado no tema da segurança das aplicações.

O projeto OWASP ASVS fornece um padrão aberto capaz de testar a segurança das aplicações. Este divide-se em quatro níveis de verificação:

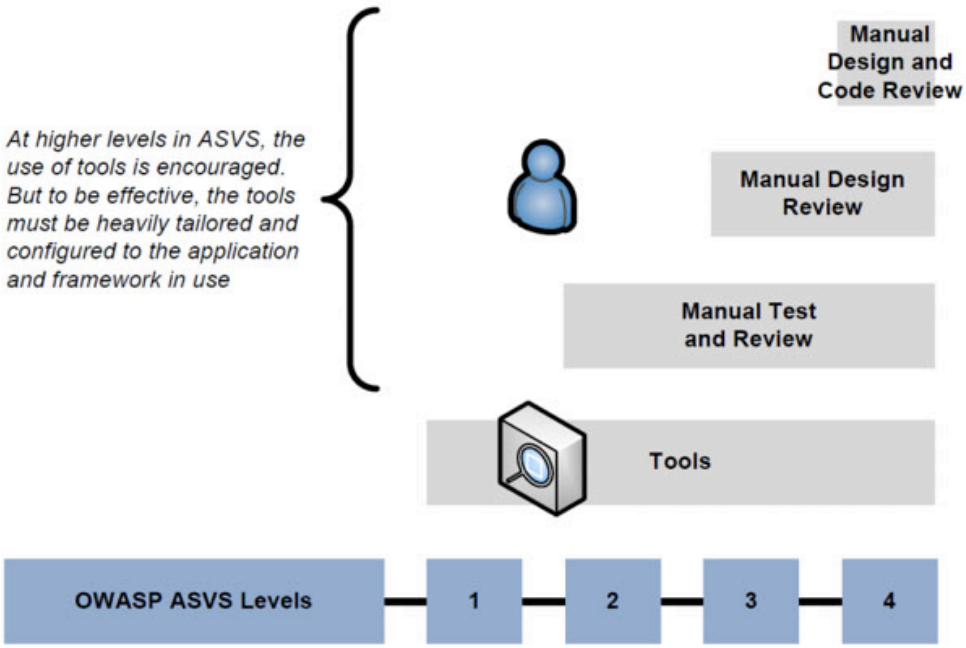

Figura 18 - Os níveis de verificação do OWASP ASVS retirado de [OWASP, 2009]

3.6.11.1 Nível 1

No nível 1 a verificação é feita usando certos automatismos, como ferramentas que permitem identificar vulnerabilidades em determinadas aplicações, sem que o utilizador precise de interagir constantemente com essas ferramentas. Este nível destina-se sobretudo para testar aplicações onde é necessário garantir os seus controlos de segurança. As ameaças à segurança são normalmente vírus ou *worms*. Este nível é constituído por dois subníveis: nível 1A

Neste nível existe ainda dois subníveis: Nível 1A que diz respeito ao uso de scanners de vulnerabilidades em aplicações e nível 1B que é dedicado ao uso de ferramentas de scan do código fonte da aplicação.

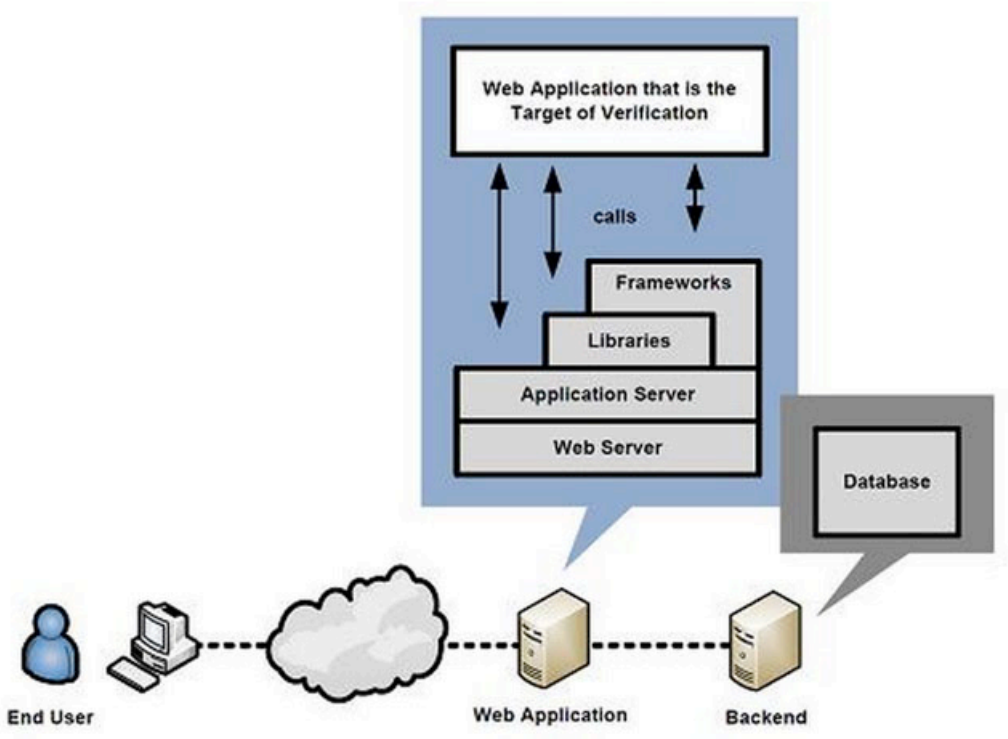

Figura 19 – Representação do nível de verificações no nível 1 retirado de [OWASP, 2009]

3.6.11.2 Nível 2

No nível 2 a verificação é feita de forma manual. É normalmente utilizado para aplicações que lidam com informações pessoais como dados de cartões de crédito ou informação pessoal sensível. As ameaças neste nível são habitualmente vírus, *worms* e indivíduos com pouco ou algum conhecimento em ataques informáticos e que fazem uso de ferramentas profissionais ou open-source para realizar os seus ataques.

O âmbito de verificação inclui a verificação de todo o código desenvolvido ou modificado de determinada aplicação bem como a análise de componentes de terceiros que fornecem funcionalidades para a aplicação. Este nível é também dividido em dois subníveis: Nível 2A que consiste na criação de teste dinâmicos para verificar a segurança de uma determinada aplicação. É normalmente chamada de *pentesting* – Testes de penetração. O nível 2B consiste na análise do código fonte da aplicação. Esta análise é feita por um humano que procura e analisa falhas no desenho, implementação ou controlos de segurança da aplicação.

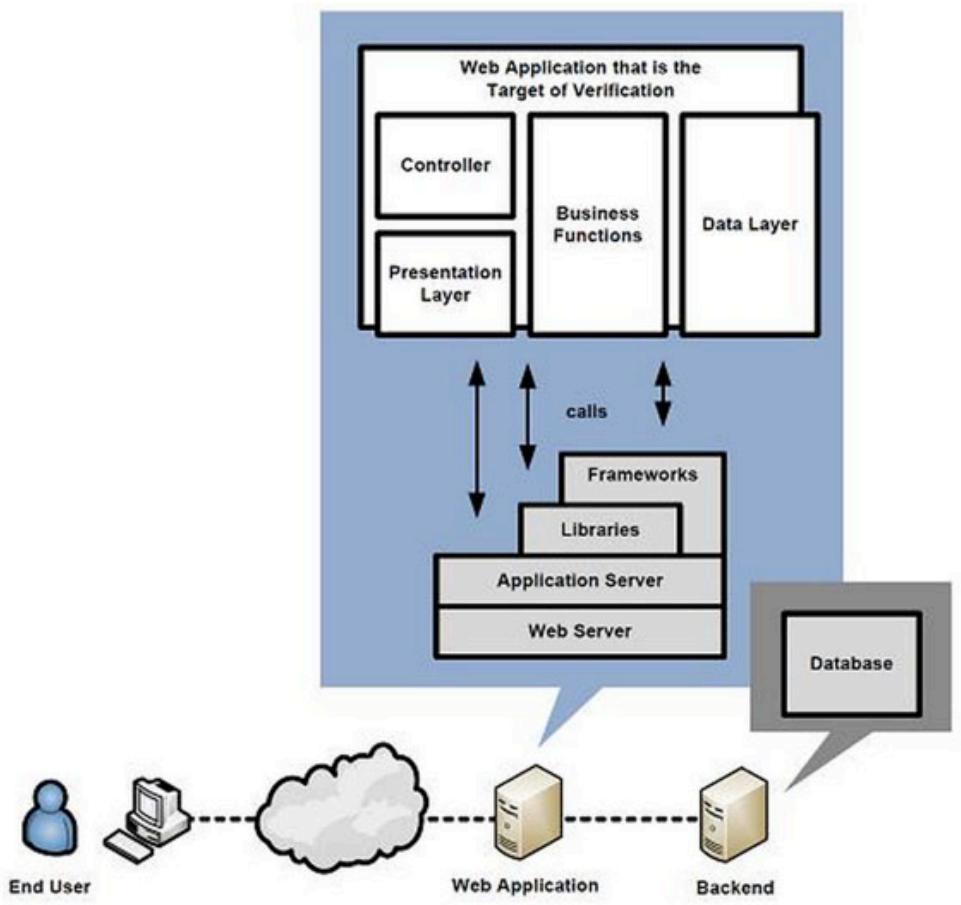

Figura 20 - Representação do nível de verificações no nível 2 retirado de [OWASP, 2009]

3.6.11.3 Nível 3

O nível 3 é adequado para aplicações que lidam com transações *business-to-business*, incluindo processamento de informação relativa a saúde, funções de negócio críticos ou outros ativos sensíveis. As ameaças neste nível são *vírus*, *worms*, oportunistas e alguns indivíduos especializados que fazem ataques focalizados em alvos específicos e que são capazes de desenvolver as suas próprias ferramentas. Neste nível o âmbito de verificação inclui todo o código desenvolvido para a aplicação, bem como componentes de terceiros.

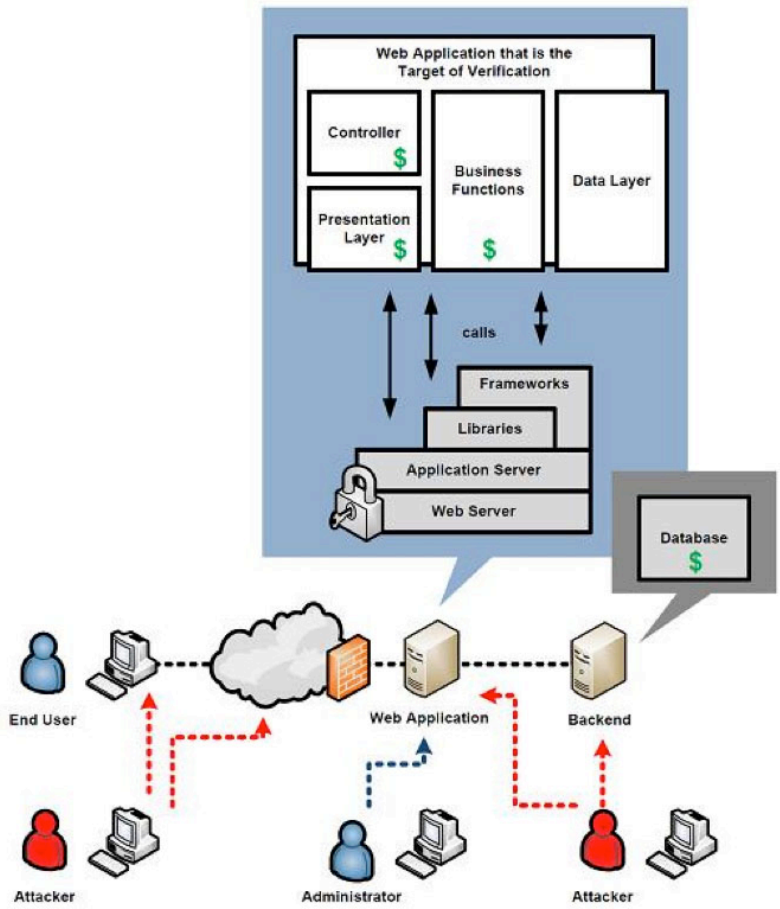

Figura 21 - Representação do nível de verificações no nível 3 retirado de [OWASP, 2009]

3.6.11.4 Nível 4

No nível 4 é requerido que todo o código da aplicação, incluindo o código não explicitamente examinado, seja identificado como parte da definição da aplicação. Ou seja o código a ser revisto deve incluir todas as bibliotecas, *frameworks* e outro código da qual a aplicação dependa. [OWASP, 2009]

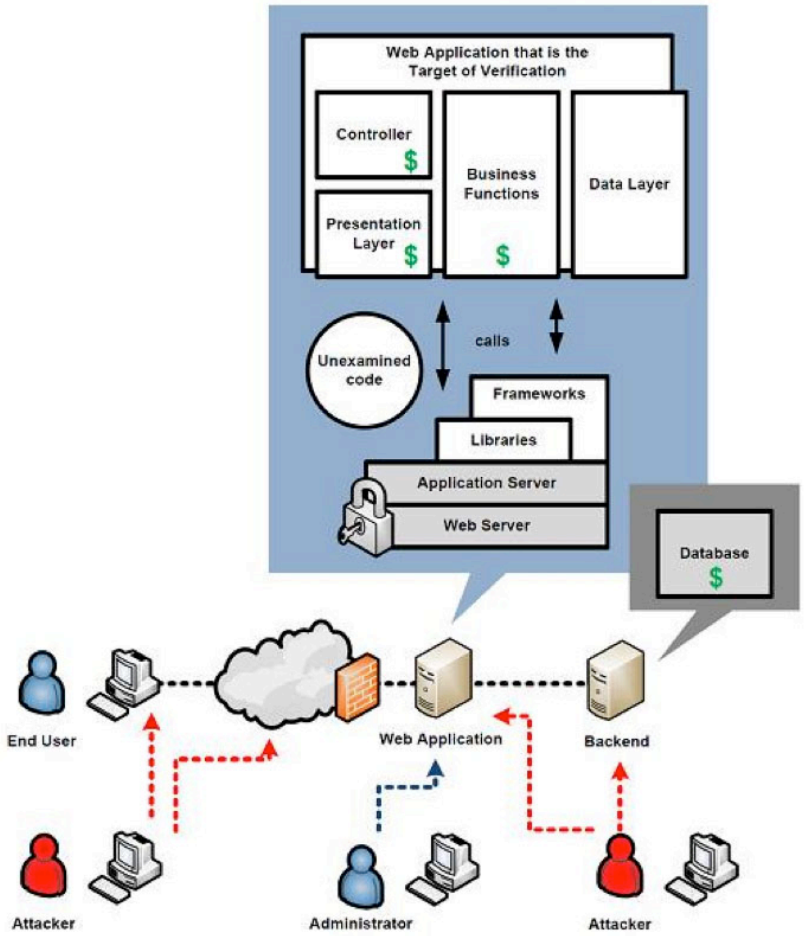

Figura 22 - Representação do nível de verificações no nível 3 retirado de [OWASP, 2009]

4 Situação atual

4.1 Auditoria

Para medir a situação atual nas questões da segurança da informação e na segurança informática, e após análise dos padrões abordados no capítulo 3, optou-se por auditar usando a norma ISO/IEC 27001 e a OWASP ASVS. A ISO/IEC 27001 por ser uma referência amplamente utilizada para a gestão da segurança da informação onde é possível obter certificação e por esta ser referenciada pelo Instituto Português da Qualidade e que oferece uma coerência com as práticas de qualidade e gestão implementadas em instituições portuguesas, e a *framework* OWASP ASVS por estar mais diretamente focada no desenvolvimento e controlo das aplicações *web,* por ser uma comunidade aberta e por toda a documentação e ferramentas serem de acesso gratuito.

4.2 Metodologia

A avaliação consistiu em duas fases subdivididas em várias. Na primeira fase foi feita a análise de literatura sobre o tema e foram também revistas *frameworks* para a gestão da segurança da informação. Na segunda fase, e após as escolhas terem recaído sobre a ISO/IEC 27001 e a OWASP ASVS, fez-se um levantamento de requisitos indicados pelas próprias *frameworks*. A ISO/IEC 27001 propõe um modelo constituído por quatro fases: Planear, executar, verificar e agir. Na fase do planeamento foram identificados os objetivos da organização, definidos os pontos a serem avaliados e definida a classificação para ser atribuída aos pontos de controlo. A correção dos pontos de controlo que não obtiveram um nível aceitável foi realizada na fase de execução. A terceira etapa desta norma (verificar) incentiva à monitorização contínua e análise crítica dos riscos motivados por mudanças organizacionais ou à existência de novos incidentes. Na última fase (Agir) foi executada uma nova auditoria e revistas as políticas para, como indicado pela norma, manter e melhorar o processo de gestão de riscos da segurança da informação.

No que diz respeito à utilização das OWASP ASVS foi definido que nível de verificação iria ser utilizado, escolha que recaiu sobre o nível 1A. Subsequentemente foram determinadas as aplicações *web* que iriam ser alvo de análise. Nesta fase foram também estudadas e decididas que ferramentas seriam usadas para levar a cabo os testes de penetração. Depois de realizados os testes que o nível 1A do OWASP ASVS determina, foram feitas correções a códigos-fonte das aplicações e servidores. Por último, realizou-se uma nova auditoria para verificar se as falhas foram corrigidas.

4.2.1 ISO/IEC 27001:2013 – Objetivos de controlo

4.2.1.1 Política de segurança da informação (A.5)

Este ponto de controlo tem por objetivo dotar a organização de politicas para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Foi feita de acordo com os pontos de controlo da norma ISO/IEC 27001 e tabela 3.

Tabela 3 – Níveis de classificação

Nível	Classificação
0%	Muito Fraco ou inexistente
25%	Insatisfatório
50%	Satisfatório
75%	Bom
100%	Excelente

Tabela 4 - Comentários ao controlo política de segurança da informação

Ref	Comentários	Status
A.5.1.1	Atualmente existem politicas de segurança, previamente aprovadas pela direção. A cada novo funcionário são comunicadas as regras que podem sempre que necessário ser consultadas online.	100%
A.5.1.2	As politicas não são alteradas regularmente. A periodicidade das revisões deveria acontecer mais frequentemente. O documento deveria ser revisto após cada incidente.	50%

4.2.1.2 Organização da segurança da informação (A.6)

Este ponto serve para gerir a segurança da informação dentro da organização.

Tabela 5 - Comentários ao controlo da organização da segurança da informação

Ref	Comentários	Status
A.6.1.1	Encontram-se definidas as responsabilidades pela segurança da informação	100%

A.6.1.2	Existem algumas lacunas na atribuição de deveres, que acarretam acesso indevido a informações.	50%
A.6.1.3	Não existe nenhuma política de contacto com as autoridades.	0%
A.6.1.4	Existe troca de informações entre a reitoria da Universidade do Porto e as unidades orgânicas.	100%
A.6.1.5	Todos os projetos têm em consideração as questões da segurança da informação.	100%
A.6.2.1	Existe uma política para dispositivos móveis que tem a aprovação da direção.	100%
A.6.2.2	Existe uma política para trabalho remoto com a aprovação da direção.	100%

4.2.1.3 Segurança nos recursos humanos (A.7)

Assegura que os funcionários, fornecedores e terceiros entendam as suas responsabilidades e estejam de acordo

Tabela 6 - Comentários ao controlo da segurança nos recursos humanos

Ref	Comentários	Status
A.7.1.1	Não são feitas verificações ao passado profissional e pessoal do candidato. É presumida a veracidade do *curriculum.*	0%
A.7.1.2	Apenas parte reduzida da organização assinou documentos de confidencialidade.	25%
A.7.2.1	Apenas parcialmente.	50%
A.7.2.2	Ainda existe pouco treino e consciencialização em segurança da informação dentro da organização.	25%
A.7.2.3	Não há um processo formal para casos de violação de informação confidencial, nem são comunicados aos restantes funcionários.	0%
A.7.3.1	Na questão da segurança da informação não há um processo formal para o encerramento de atividades.	0%

4.2.1.4 Gestão de ativos (A.8)

Tabela 7 - Comentários ao controlo da gestão dos ativos

Ref	Comentários	Status
A.8.1.1	O inventário existente não é preciso, dado que muitos dos ativos pertencem a grupos de investigação.	75%
A.8.1.2	Existem algumas lacunas na correta atribuição de responsabilidades dos ativos.	75%

A.8.1.3	Não existe classificação da informação.	0%
A.8.1.4	Não existe uma política documentada para a devolução de ativos.	0%
A.8.2.1	Não existe classificação da informação.	0%
A.8.2.2	Não existe tratamento da informação.	0%
A.8.2.3	Não existe uma política para o manuseamento de diferentes tipos de ativos.	0%
A.8.3.1	Não existe uma política para o tratamento de *media* removíveis.	0%
A.8.3.2	Não há procedimentos não que diz respeito à alienação de media removíveis.	0%
A.8.3.3	Não existe uma política para o transporte de ativos que contenham informações.	0%

4.2.1.5 Controlo de acesso (A.9)

Tabela 8 - Comentários ao ponto de controlos de acesso

Ref	Comentários	Status
A.9.1.1	Existem politicas no controlo de acesso.	100%
A.9.1.2	Os utilizadores têm apenas acesso às redes para as quais estão autorizados.	100%
A.9.2.1	Existe um processo para registo e cancelamento de utilizadores.	100%
A.9.2.2	Existe um processo de disponibilização de acesso.	100%
A.9.2.3	Os acesso privilegiados são restritos e controlados.	100%
A.9.2.4	É utilizado um processo formal para atribuição da informação secreta de autenticação.	100%
A.9.2.5	São feitas verificações regulares aos direitos de acesso dos utilizadores.	75%
A.9.2.6	Após cessação de atividades são retirados os acesso, exceto o email que permanece acessível por período suplementar de 30 dias.	75%
A.9.3.1	Apesar de orientados, parte dos utilizadores ainda partilha informação de autenticação secreta.	50%
A.9.4.1	O acesso à informação está de acordo com a política de controlo de acesso.	100%
A.9.4.2	Os sistemas de autenticação usam procedimentos de segurança.	100%
A.9.4.3	Os sistemas de gestão têm mecanismo para criação de senhas seguras (Mais de 8 carateres, letras maiúsculas e minúsculas, números, não conter o nome do utilizador, etc.)	100%
A.9.4.4	Estes programas são de acesso restrito.	100%
A.9.4.5	O acesso ao código-fonte de programas é restrito	100%

4.2.1.6 Criptografia (A.10)

Tabela 9 - Comentários ao controlo da criptografia

Ref	Comentários	Status
A.10.1.1	Não se encontra definido uma política para o uso de controlos criptográficos.	0%
A.10.1.2	Não existe uma política sobre a gestão de chaves criptográficas.	0%

4.2.1.7 Segurança física e do ambiente (A.11)

Tabela 10 - Comentários ao controlo da segurança física e do ambiente

Ref	Comentários	Status
A.11.1.1	Estão definidos os perímetros de segurança física.	100%
A.11.1.2	Estão protegidas parcialmente.	75%
A.11.1.3	Os escritórios e salas têm controlos de acesso parciais.	50%
A.11.1.4	Existem medidas parciais para desastres naturais, ataques maliciosos ou acidentes.	75%
A.11.1.5	As áreas seguras estão devidamente controladas.	100%
A.11.1.6	Os pontos de carga e descarga estão controlados e separados de recursos de processamento de informação.	100%
A.11.2.1	Os equipamentos estão parcialmente protegidos contra perigos ambientais e oportunidades de acesso não autorizado.	75%
A.11.2.2	Os equipamentos estão parcialmente protegidos contra interrupções energéticas e outras falhas	50%
A.11.2.3	A cablagem elétrica e de telecomunicações encontra-se parcialmente protegida.	50%
A.11.2.4	Os equipamentos são mantidos de forma correta.	100%
A.11.2.5	Os equipamentos apenas são retirados com autorização prévia.	100%
A.11.2.6	Os equipamentos que saem das instalações não estão completamente alheios aos riscos fora das instalações da organização.	50%
A.11.2.7	Todos os equipamentos eliminados ou reutilizados são alvo de verificações para que nenhum dado sensível esteja presente.	100%
A.11.2.8	Nem todos os utilizadores asseguram a proteção dos seus equipamentos.	50%
A.11.2.9	Não está instituído uma política	0%

4.2.1.8 Segurança nas operações (A.12)

Tabela 11 - Comentários ao controlo da segurança nas operações

Ref	Comentários	Status
A.12.1.1	Os procedimentos de operação encontram-se documentados e disponibilizados	100%
A.12.1.2	São parcialmente geridas as alterações na organização.	75%
A.12.1.3	Existe separação dos ambientes de desenvolvimento, teste e produção.	100%
A.12.1.4	A utilização dos recursos é monitorizada e ajustada para assegurar o desempenho dos sistemas.	100%
A.12.2.1	Existem mecanismo de deteção e prevenção.	75%
A.12.3.1	Dado o crescimento da instituição apenas é possível garantir parcialmente cópias de segurança das informações.	25%
A.12.4.1	Existe registo de eventos, no entanto a análise apenas é feita após incidente.	75%
A.12.4.2	O acesso ao registo de eventos é restrito.	100%
A.12.4.3	São registadas as atividades de administradores e operadores de sistema.	100%
A.12.4.4	Não existe sincronização de relógios.	0%
A.12.5.1	Existem procedimentos de controlo de instalação de software nos sistemas de produção.	100%
A.12.6.1	O departamento de sistemas de informação vai-se mantendo atualizado sobre vulnerabilidades. Os períodos de avaliação sobre os riscos associados para a organização deveriam ser encurtados.	75%
A.12.6.2	Existem regras definidas para instalação de software pelos utilizadores.	100%
A.12.7.1	As auditorias são previamente planeadas.	100%

4.2.1.9 Segurança nas comunicações (A.13)

Tabela 12 - Comentários ao controlo da segurança nas comunicações

Ref	Comentários	Status
A.13.1.1	As redes são controladas e geridas.	100%
A.13.1.2	Estão identificados os mecanismos de segurança nos serviços de rede.	100%
A.13.1.3	Tanto utilizadores como ativos contendo informações estão divididos.	100%
A.13.2.1	Nem todos os meios de comunicação possuem procedimentos para proteger a transferência da informação.	50%
A.13.2.2	Nem todos os prestadores de serviços têm acordos de	50%

	confidencialidade.	
A.13.2.3	As mensagens eletrónicas que tratam dados sensíveis são encriptadas.	100%
A.13.2.4	Estão parcialmente identificados e revistos os documentos de confidencialidade.	50%

4.2.1.10 Aquisição, desenvolvimento e manutenção de sistemas (A.14)

Tabela 13 - Comentários ao controlo da aquisição, desenvolvimento e manutenção de sistemas

Ref	Comentários	Status
A.14.1.1	Todos os novos sistemas ou melhorias são alvo de controlo de requisitos de segurança da informação.	100%
A.14.1.2	Nas redes públicas os serviços são parcialmente protegidos.	75%
A.14.1.3	A informação envolvida nas transações encontra-se protegida.	100%
A.14.2.1	As aplicações desenvolvidas na organização possuem regras de desenvolvimento seguro.	100%
A.14.2.2	O registo de alterações aos sistemas estão pouco documentados.	25%
A.14.2.3	Deveriam ser feitas mais revisões técnicas após modificações das plataformas em produção.	25%
A.14.2.4	As alterações em pacotes de software são controladas.	100%
A.14.2.5	São mantidos parcialmente princípios de engenharia de sistemas seguros.	75%
A.14.2.6	Existe um ambiente de desenvolvimento seguro.	100%
A.14.2.7	Existe pouco supervisionamento das atividades subcontratadas.	25%
A.14.2.8	São realizados poucos testes das funcionalidades durante o desenvolvimento.	25%
A.14.2.9	Não estão definidos teste de aceitação e respetivos critérios.	0%
A.14.3.1	Os dados de teste estão normalmente protegidos e controlados.	100%

4.2.1.11 Relações com fornecedores (A.15)

Tabela 14 - Comentários ao controlo das relações com os fornecedores

Ref	Comentários	Status
A.15.1.1	Poucos contratos com os fornecedores incluem diretrizes para a segurança da informação.	25%
A.15.1.2	Não existe uma política forte de estabelecimento de requisitos de segurança da informação com os fornecedores.	25%
A.15.1.3	Os acordos com os fornecedores muito raramente incluem requisitos para a assegurar a segurança da informação.	25%

A.15.2.1	Os fornecedores não são alvo de auditorias.	0%
A.15.2.2	As mudanças para a prestação de serviços não incluem uma avaliação de segurança e risco.	0%

4.2.1.12 Gestão de incidentes de segurança da informação (A.16)

Tabela 15 - Comentários ao controlo gestão de incidentes de segurança da informação

Ref	Comentários	Status
A.16.1.1	Não se encontra instituído uma política eficaz de responsabilidades e procedimentos.	25%
A.16.1.2	Os eventos de segurança da informação não são tratados com celeridade.	25%
A.16.1.3	Não existem procedimentos para reportar pontos fracos da segurança da informação.	0%
A.16.1.4	Existe avaliação parcial sobre eventos de segurança da informação.	25%
A.16.1.5	A resposta a incidentes não segue um processo formal.	25%
A.16.1.6	Existe aprendizagem com os incidentes. Deve no entanto existir mais celeridade e documentação.	75%
A.16.1.7	Existe recolha de evidências.	75%

4.2.1.13 Aspetos da segurança da informação na gestão da continuidade do negócio (A.17)

Tabela 16 - Comentários ao controlo aspetos da segurança da informação na gestão da continuidade do negócio

Ref	Comentários	Status
A.17.1.1	Não existe um planeamento de continuidade.	0%
A.17.1.2	Não estão documentados processos de continuidade.	0%
A.17.1.3	Não existem processos de continuidade.	0%
A.17.2.1	Existe redundância parcial em alguns serviços.	50%

4.2.1.14 Conformidade (A.18)

Tabela 17 - Comentários ao controlo da conformidade

Ref	Comentários	Status
A.18.1.1	Existe pouca identificação da legislação aplicável e de requisitos	25%

	contratuais.	
A.18.1.2	Existem procedimentos apropriados para assegurar a conformidade com os direitos de propriedade intelectual.	100%
A.18.1.3	Existem procedimentos contra a perda, eliminação, falsificação, acesso não autorizado e divulgação não autorizada de registos.	100%
A.18.1.4	Existem politicas para a privacidade e proteção de dados pessoais.	100%
A.18.1.5	Não existem regulamentação de controlos criptográficos.	0%
A.18.2.1	Não existe revisão regular e independentes de controlos, politicas, processos e procedimentos de segurança da informação.	0%
A.18.2.2	Não existe revisão regular dos procedimentos e processamento da informação.	0%
A.18.2.3	Não existem auditorias aos sistemas de informação.	0%

4.2.2 OWASP ASVS

Para realização de testes de vulnerabilidades em aplicações foi usado o nível 1A do OWASP ASVS. Neste nível são usadas ferramentas automatizadas para a deteção dessas vulnerabilidades. Com este método é possível fazer a avaliação das aplicações quer internas quer externas do LA IBMC-INEB, simulando testes de penetração para determinar se o ataque é viável ou não e qual o seu impacto.

Os testes foram feitos em 30 aplicações *web*, usando as seguintes ferramentas:

- **Sqlmap** é uma ferramenta *open-source* que automatiza o processo de deteção e exploração de falhas de SQL injection;
- **Burpsuite** é uma plataforma integrada para a realização de testes de segurança de aplicações *web*. Possui diversos componentes como: *proxy* que interceta e modifica o tráfego entre o browser e o servidor; *spider* que procura conteúdos existentes, *scanner* faz pesquisas automáticas por vulnerabilidades; *intruder* que permite executar ataques customizados; *repeater* que permite manipular e reenviar pedidos individuais;
- **OWASP ZAP** muito semelhante ao programa Burpsuite, permite realizar testes de segurança, encontrando vulnerabilidades em aplicações *web*;
- **Wireshark** é um analisador de protocolos de rede Permite capturar e analisar todo o tráfego;
- **Tcpdump** funciona de maneira semelhante ao wireshark e não possui interface gráfica;
- **w3af** é uma ferramenta de auditoria para aplicações *web*. Automatiza a deteção de vulnerabilidades em aplicações *web*;
- **Nikto** é uma ferramenta *open-source* que realiza testes de vulnerabilidades contra servidores *web*.

4.2.2.1 Tabela de verificação do nível 1A

Tabela 18 - Número de ocorrências no nível 1A do OWASP ASVS

	Requisito	Número de ocorrências
V1.1	Verificar se todos os componentes da aplicação que estão presentes estão identificados.	0
V2.1	Verificar se todas as páginas e recursos requerem a autenticação e exceto aquelas que especificamente devem ser públicas.	0
V2.2	Verificar se todos os campos de senha não retornam a senha do utilizador quando ela é submetida, e se os campos da senha estão com o recurso de autocompletar desabilitado.	5
V2.3	Verificar se um número máximo de tentativas de autenticação for excedido, a conta é bloqueada por um período de tempo suficiente para deter os ataques de força bruta.	2
V3.1	Verificar se a implementação padrão da gestão de sessões do *framework* é utilizada pela aplicação.	0
V3.2	Verificar se as sessões são invalidadas quando o utilizador sai da aplicação.	3
V3.3	Verificar se as sessões expiram após um período especificado de inatividade.	3
V3.5	Verificar se todas as páginas autenticadas têm links de *logout*.	2
V4.1	Verificar se os utilizadores podem aceder somente funções protegidas para as quais eles possuem autorização especifica.	4
V4.2	Verificar se os utilizadores podem aceder somente *URLs* para as quais eles possuem autorização especifica.	2
V4.3	Verificar se os utilizadores podem aceder somente arquivos para os quais eles possuem autorização especifica.	1
V4.4	Verificar se referências diretas a objetos são protegidas, de tal forma que somente objetos autorizados sejam acessíveis para cada utilizador.	1
V4.5	Verificar se a navegação pelos diretórios está desabilitada a menos que explicitamente desejada.	2
V5.1	Verificar se o ambiente não é susceptivel a *buffer overflows*, ou se os controlos de segurança previnem *buffer overflows.*	0
V5.2	Verificar se um padrão de validação positiva é definido e aplicado para todas as entradas.	0
V5.3	Verificar se todas as falhas na validação de entradas resultam na rejeição ou sanitização da entrada.	4
V9.1	Verificar se todos os formulários que contenham informações sensíveis têm desabilitado o cache do lado do cliente, incluindo recursos de auto completar	0

V10.1	Verificar se um caminho pode ser construído a partir de uma CA confiável para cada certificado de servidor TLS, e se cada certificado de servidor é válido.	0
V11.1	Verificar se redireccionamentos não incluem dados que não foram validados.	0
V11.2	Verificar se a aplicação aceita somente um conjunto definido de métodos de requisição HTTP, tais como GET e POST.	1
V11.3	Verificar se toda a resposta HTTP contém um cabeçalho tipo de conteúdo (contente type header) especificando um conjunto seguro de carateres (por exemplo UTF-8)	0

4.2.3 Análise de resultados ISO 27001

Figura 23 – Resultados por secção da auditoria usando a norma ISO 27001

Após análise dos resultados em termos da segurança da informação usando a norma ISO 27001:2013, a organização deve melhorar nos seguintes aspetos:

- As politicas de segurança da informação devem ser revistas em intervalos regulares ou sempre que há modificações significativas;
- Deve ser reduzido o risco de uso acidental ou deliberada de ativos fazendo uso da segregação de funções;
- Contactos com entidades, como por exemplo fornecedores telecomunicações (FCCN), devem ser implementados para prever e preparar futuras mudanças de leis ou regulamentos;
- Devem ser feitas verificações aos candidatos, de acordo com as leis e ética, que irão ocupar cargos que têm acesso a informações confidenciais, como por exemplo informações financeiras;
- Todos os funcionários e prestadores de serviços com acesso a informações sensíveis devem perceber as suas responsabilidades e as da organização e devem também assinar um documento de confidencialidade;
- A organização deve realizar regularmente ações de sensibilização paras as questões da segurança da informação;
- O processo para a cessação de funções deve ser revisto;
- Os suportes de dados, quando já não são necessários, devem ser eliminados de forma a que a recuperação de dados não seja possível;
- A organização deve sensibilizar os funcionários de que as credenciais de autenticação são pessoais e intransmissíveis;
- Deve-se adotar uma política de secretária limpa, na qual os documentos sensíveis em papel ou em suporte digital devem estar guardados em locais seguros para que não haja acesso não autorizado. De igual modo as sessões dos computadores devem ser bloqueadas sempre que o utilizador se ausentar;
- É necessário investimento por parte da organização para a solução de backups, de modo a que toda a informação seja salvaguardada;
- Deve haver um servidor NTP para sincronizar todos os servidores e computadores dentro da organização como forma dos registos de eventos serem mais fidedignos;
- Durante o processo de desenvolvimento devem ser realizados testes de segurança padronizados;
- Os prestadores de serviços devem ser identificados definindo em que áreas dentro da organização atuam, fazendo uma revisão dos direitos de acesso;
- Os funcionários e prestadores de serviços que utilizam sistemas e serviços de informação da organização devem ser incentivados a observar e relatar quaisquer falhas de segurança de informações observadas ou suspeitos nos sistemas ou serviços;
- O departamento de sistemas de informação deve alertar a comunidade para vulnerabilidades existentes;
- A organização deve determinar as suas necessidades de segurança da informação e continuidade de gestão de segurança da informação em situações adversas, como por exemplo durante uma crise ou desastre;

- Manter a consciência de políticas para proteger os direitos de propriedade intelectual dando conhecimento da intenção de tomar medidas disciplinares contra o pessoal que não os cumpre.

4.2.4 Análise de resultados OWASP ASVS

- Devem ser melhorados os aspetos da gestão e tratamento de credenciais de contas;
- A gestão de sessões das aplicações devem ser verificadas;
- Os controlos de acesso a *URLs*, dados, diretórios devem ser revistos;
- As entradas de dados nas aplicações devem ser validadas para que sejam usadas de forma segura;
- Melhorar a segurança dos requisitos e respostas HTTP.

4.3 Análise de risco

A análise de risco é um elemento-chave do processo de gestão de segurança de sistemas de informação. Possibilita a identificação e avaliação do que tem de ser controlado, minimizado ou aceite. [Rot, A., 2008]

Existem dois métodos de análise de risco: quantitativo e qualitativo.

4.3.1 Análise de risco quantitativa

Segundo [Tregear, 2001] uma abordagem quantitativa estima geralmente o custo monetário de risco e técnicas de redução de risco, baseadas em:

- A probabilidade de um evento danoso ocorrer;
- O custo de perdas potenciais;
- A probabilidade do evento danoso trazer perdas potenciais.

Este método é algo complexo de ser realizado dado que:

- O cálculo dos custos de interrupção é difícil;
- É difícil estimar as probabilidades de ocorrências;
- Tem um maior consumo de tempo.

4.3.2 Análise de risco qualitativa

É o método mais usado para a realização de análises de risco. Neste método não é requerida a atribuição de valores monetários para componentes e perdas. As análises qualitativas usam

habitualmente questionários, listas de verificação, questionários e entrevistas. Neste método, diferentes elementos da organização classificam diferentes tipos de ameaças.

4.3.3 Resultados à analise de risco qualitativa

Foi realizado um questionário a cinco elementos da organização, representando as diferentes áreas profissionais existentes. Para cada uma das dez ameaças foi classificado utilizando a seguinte escala:

Tabela 19 - Nível de classificação da análise qualitativa para as ameaças

Nível	Classificação
1	Muito baixo
2	Baixo
3	Médio
4	Alto
5	Muito alto

Tabela 20 – Resultados da análise de risco qualitativa

	Sistemas de informação	Investigador	Técnico administrativo	Técnico de laboratório	Técnico
Incêndio/Inundação	2	2	2	2	2
Falhas de energia	3	3	3	3	3
Falhas de hardware	3	2	3	3	3
Acesso não autorizado	1	3	3	2	2
Roubo de propriedade intelectual	2	3	1	2	2
Vírus	3	3	2	2	2
Sabotagem	1	1	2	1	1
Privacidade	2	2	1	2	2
Não realização de cópias de segurança	4	4	4	3	3
Não alteração da password regularmente	4	2	2	2	2
Resultado	**2,5**	**2,5**	**2,3**	**2,2**	**2,2**

5 Implementação da solução

Após análise feita no capítulo anterior, foram aplicadas medidas com vista à correção e ou melhoria dos pontos de controlo da norma ISO 27001 e OWASP ASVS. Optou-se por usar a norma ISO 27001 por ser uma norma de referência internacional para a gestão da segurança da informação e a OWASP ASVS por estar mais diretamente focada no desenvolvimento e controlo das aplicações *web*. Dado que foi usado o nível 1A do OWASP ASVS, isso significa que foram usados mecanismos automatizados para encontrar vulnerabilidades. Dada a sua rapidez de deteção de pontos críticos, e uma vez que está virada para o departamento de sistemas de informação isso acaba por facilitar o atingir de alguns pontos de controlo da norma ISO 27001, mais virados para os SI.

Neste caso de estudo optou-se por usar a norma ISO 27001 mais como modelo de referência para a gestão da segurança da informação do que norma certificadora, no entanto o objetivo de certificar a organização não está posta de parte, dado que a certificação traz vantagens tais como:

- **Redução de custos** – As normas Internacionais ajudam a otimizar as operações e, portanto, melhorar a linha de fundo;
- **Diferenciação** – A certificação significa estar num grupo restrito de organizações que são capazes de assegurar um conjunto de obrigações padronizadas;
- **Credibilidade** – Garantir a integridade dos dados e sistemas, significa o reconhecimento de fornecedores, clientes ou outras partes interessadas no que diz respeito à proteção da informação, o que pode também levar a abertura a novos mercados de negócio;
- **Conformidade legal e regulatória** – Garante a conformidade com as leis do país;

5.1 Resultados

5.1.1 OWASP ASVS – Resultados

O resultado da auditoria feita no capitulo anterior mostraram existir 27 falhas em 21 pontos de controlo, em 30 aplicações diferentes. (Tabela 16) Em conjunto com os restantes elementos do departamento de sistemas de informação do LA IBMC-INEB, foi levado a cabo as correções das vulnerabilidades encontradas. A tabela seguinte mostra o resultado das correções.

Tabela 21 - Resultados das correções das vulnerabilidades encontradas usando o modelo de verificação OWASP ASVS

Requisito	Número de ocorrências	Requisito	Número de ocorrências
V1.1	0	V4.4	**0**
V2.1	0	V4.5	**1**
V2.2	**0**	V5.1	0
V2.3	**0**	V5.2	0
V3.1	0	V5.3	**1**
V3.2	**1**	V9.1	0
V3.3	**2**	V10.1	0
V3.5	**0**	V11.1	0
V4.1	**0**	V11.2	**0**
V4.2	**2**	V11.3	0
V4.3	**0**		

Após as correções verificou-se uma melhoria de 74% em relação à auditoria feita anteriormente. As 7 falhas não corrigidas deveram-se aos seguintes fatores:

- Falta de tempo, dada a pequena dimensão da equipa de desenvolvimento;
- Espera por decisão superior (V4.5).

É expectável num futuro próximo que os 7 pontos em falta sejam corrigidos, elevando assim para 100% as correções das vulnerabilidades.

5.1.2 ISO 27001 – Resultados

No que diz respeito aos resultados da implementação da norma ISO 27001, a auditoria anteriormente feita (Fig. 20) mostrou que 7 das 14 secções de controlo da norma ISO 27001 atingiram 50% ou menos dos objetivos propostos.

Figura 24 - Resultados da implementação da norma ISO 27001

Depois da implementação e apesar de haver algumas melhorias, estas acabaram por não ser significativas. O facto de que num futuro próximo o LA IBMC-INEB e o IPATIMUP juntar-se-ão, criando o I^3S, acaba por provocar alguma incerteza no futuro no que diz respeito à aceitação deste tipo de políticas para a segurança da informação, dado que é necessário envolver todos os departamentos e direções.

Foi também notado resistência à mudança de processos, tanto organizacional como individual. Essa resistência por ser motivada por diversos fatores, desde medo do não cumprimento com clientes, fornecedores ou parceiros passando por fatores psicológicos onde os indivíduos não se sentem motivados para alterar os seus processos habituais.

Os pontos de controlo que foram melhorados acabaram por estar mais ligados ao departamento de sistemas de informação.

5.1.3 Análise de risco – Discussão de resultados

O resultado à análise de risco realizada a alguns membros da organização apresenta globalmente um resultado de nível baixo. Isso significa que alguns dos riscos possuem valores suficientemente baixos para serem considerados aceitáveis de acordo com a política da organização. Todavia, alguns dos riscos, como por exemplo "a não realização de cópias de segurança", terão de ser revistos para serem colocados num nível aceitável.

5.1.4 Metodologias organizacionais e tecnológicas

[Siponen, 2000] refere que as organizações não costumam a agir enquanto tudo corre bem, mas apenas quando as coisas correm mal, as organizações despendem uma grande quantidade de esforço para recuperar da situação. A partir do estudo realizado, conclui-se que existem um conjunto de falhas que devem ser mitigadas para que a organização atinja um nível de maturidade satisfatório no que diz respeito á segurança da informação. Medidas quer sejam organizacionais ou tecnológicas devem ser implementadas para mitigar os riscos identificados e devem estar em conformidade com as necessidades de segurança e objetivos de negócio da organização.

No âmbito dos processos organizacionais, muitos dos riscos foram minimizados através da aplicabilidade dos requisitos, processos e pontos de controlo existentes na norma ISO/IEC 27001, como a consciencialização dos utilizadores por meio de realização de palestras e colocação de um curso básico de segurança da informação na plataforma de *e-learning* da instituição. Ainda no que diz respeito à educação dos utilizadores para este tema, todos os novos funcionários serão informados das políticas existentes e das consequências das suas violações. De igual modo o papel do Departamento de Sistemas de Informação (DSI) será mais ativo para esta temática, criando uma plataforma de resposta a incidentes. Como resultado, tanto os funcionários como o Departamento de Sistemas de informação passaram a agir em uniformidade ou seja, os utilizadores estavam mais atentos para os riscos, sendo capazes de os identificar e reportar, e o DSI mais eficiente nos tempos de resposta e alerta das ameaças. Dado que muita da informação existente na organização pode ser considerada sensível, tanto por ser relevante para a investigação e futuras criações de patentes, como também para assegurar a competitividade, será dada atenção às políticas de confidencialidade dos membros da organização, como também os prestadores de serviços externos.

A nível de desenvolvimento de aplicações, o DSI adotou um conjunto de medidas tais como a utilização de *frameworks* de desenvolvimento que, para além de acelerarem o processo de criação das aplicações, também oferecem maior proteção contra falhas mais comuns em ambientes *web,* como definido no documento OWASP Top 10. O ciclo de desenvolvimento também inclui a realização de testes de segurança. Também a nível de servidores o DSI implementou processos de minimização dos riscos (*hardening*), como a utilização de canais seguros e encriptados sempre que existam transições de dados privados como palavras-passe ou informação pessoal, remoção de informações que possam identificar que aplicação e versão de determinadas aplicações [Cód. 25 e Cód. 26] e aplicação e manutenção de *patches*.

```
atorres$ telnet 193.137.38.111 80
Trying 193.137.38.111...
Connected to e-training.ibmc.up.pt.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 302 Found
Date: Thu, 4 Sep 2014 22:31:25 GMT
Server: Apache/2.4.7 (Fedora) OpenSSL/1.0.1e-fips PHP/5.5.9
Location: http://e-training.ibmc.up.pt
Connection: close
Content-Type: text/html; charset=iso-8859-1

Connection closed by foreign host.
```

Código 25 – Exemplo de reconhecimento de um servidor onde são apresentadas as versões das aplicações.

```
atorres$ telnet 193.137.38.111 80
Trying 193.137.38.111...
Connected to e-training.ibmc.up.pt.
Escape character is '^]'.
HEAD / HEAD/1.0

HTTP/1.1 302 Found
Date: Thu, 4 Sep 2014 22:48:36 GMT
Server: Apache
Location: http://e-training.ibmc.up.pt
Connection: close
Content-Type: text/html; charset=iso-8859-1

Connection closed by foreign host.
```

Código 26 – Exemplo de reconhecimento de um servidor após remoção das informações sobre as aplicações

Uma vez que a organização tem uma política de BYOD, muitas das ameaças encontravam-se nos computadores pessoais dos funcionários. Para além de serem incentivados a instalarem antivírus, foi implementado um IDS *open-source* (*Snort*) para deteção de *malware* e *botnets* na rede, o que trouxe uma identificação e correção das falhas mais célere. A organização fazia também uso de VPN PPTP, que se encontrava vulnerável [Schneier, Wagner, 1999]e que se encontra atualmente a ser migrada para OpenVPN. O DSI pretende ainda no futuro centralizar todos os *logs* e fazer uso de um servidor NTP para garantir a exatidão dos acontecimentos.

Em suma, um dos requisitos que a norma ISO/IEC 27001 aborda é a da melhoria contínua, isto significa que toda a organização deve ser periodicamente avaliada como forma de garantir que os riscos sejam minimizados e que a integridade, disponibilidade e confidencialidade sejam garantidas.

6 Conclusões

A informação é um ativo que todas as organizações dependem para o seu ambiente de negócio. Com o advento das tecnologias e sistemas de informação, a informação fica mais exposta a uma ampla variedade de ameaças e vulnerabilidades, o que põe em risco a manutenção da integridade, confidencialidade e disponibilidade. A gestão de segurança da informação pode ser elaborada para eliminar ou minimizar os riscos e devem ser feitas utilizando normas padronizadas.

Existem várias normas relacionadas com a questão da segurança informacional, algumas das quais desenvolvidas especificamente para determinados setores de negócio e que para serem corretamente implementadas dependem do esforço de todos os elementos da organização. Esta questão da segurança não é um problema exclusivo do departamento de sistemas de informação, mas sim de todos os elementos que compõe a organização e que deve ser reforçada pela direção.

A auditoria realizada revelou diversas lacunas nos processos e politicas da organização e que, embora de forma não muito significativa, foram colmatadas. No entanto, ficaram-se a conhecer os pontos fracos e fortes da organização que até então eram desconhecidos. A implementação da norma ISO 27001 revelou-se difícil de ser executada dada a resistência à mudança que normalmente as organizações sofrem. O facto de o IBMC, INEB e IPATIMUP virem a formar uma parceria dentro de pouco tempo (meados de 2015) fez com que alguns dos objetivos propostos ficassem em espera.

6.1 Trabalho futuro

Existe a promessa de retomar a implementação da norma ISO 27001 no futuro I3S com vista à certificação, até porque os desafios do futuro consórcio serão maiores. Serão criadas logo inicialmente politicas de acordo com a norma ISO 27001, para que depois a sua implementação seja menos complicada de ser executada.

Referências

[Abawajy, 2008]	Abawajy, J. H., Thatcher, K. and Kim, T.-h. Investigation of Stakeholders Commitment to Information Security Awareness Programs. IEEE, 2008.
[Acunetix, 2013]	Acunetix Cross-site Scripting (XSS) Attack. https://www.acunetix.com/websitesecurity/cross-site-scripting/ [ultimo acesso: Jan 2014]
[Alonso, Bordón, Béltran e Guzman, 2008]	Alonso, J. M., Bordón, R., Beltrán, M. and Guzmán, A. LDAP Injection & Blind LDAP Injection. 2008
[Anderson, 2008]	Anderson, R. Security engineering. John Wiley & Sons, 2008.
[Arce, 2003]	Arce, I. The weakest link revisited [information security]. Security & Privacy, IEEE, 1, 2 2003), 72-76.
[BBC, 2013]	BBC Edward Snowden documents show NSA broke privacy rules, http://www.bbc.com/news/world-us-canada-23721818 [último acesso: Mar 2014]
[Campos, A., 2006]	Campos, A. Sistema de segurança da informação. Florianópolis: Visual Books, 2006.
[Citrix, 2010]	Citrix How to use NetScaler Application Firewall to defend against CSRF attacks. http://blogs.citrix.com/2010/04/29/how-to-use-netscaler-application-firewall-to-defend-against-csrf-attacks/ [último acesso: Set 2014]
[CNN, 2013]	CNN WikiLeaks Fast Facts. http://edition.cnn.com/2013/06/03/world/wikileaks-fast-facts/ [último acesso: Dez 2014]
[Commoncriteriaportal, 2014]	Commoncriteriaportal Common Criteria. http://www.commoncriteriaportal.org/cc/ [último acesso: Set 2014]
[Dias, 2000]	Dias, C. Segurança e auditoria da tecnologia da informação. Axcel Books, 2000.
[Emarketer, 2013]	Emarketer Ecommerce Sales Topped $1 Trillion for First Time in 2012. http://www.emarketer.com/Article/Ecommerce-Sales-Topped-1-Trillion-First-Time-2012/1009649 [último acesso: Dez 2013]
[Gartner, 2010]	Gartner 20 years of phishing. http://blogs.gartner.com/jay-heiser/2010/05/03/phishing/ [útimo acesso: Set 2014]
[Guardian, the, 2014]	Guardian, The. Apple tightens iCloud security after celebrity nude

photo hack. http://www.theguardian.com/technology/2014/sep/05/apple-tightens-icloud-security-after-celebrity-nude-photo-hack [último acesso: Set 2014]

[Guardian, the, 2014] Guardian, T. Bradley Manning's sentence: 35 years for exposing us to the truth. http://www.theguardian.com/commentisfree/2013/aug/21/bradley-manning-sentence-birgitta-jonsdottir [último acesso: Set 2014]

[Halfond, Viegas, Orso, 2006] Halfond, W., Viegas, J. and Orso, A. A classification of SQL-injection attacks and countermeasures. 2006.

[Halfond, Orso, 2005] Halfond, W. G. and Orso, A. AMNESIA: analysis and monitoring for Neutralizing SQL-injection attacks. ACM, 2005.

[Harris, S., 2005] Harris, S. All in one CISSP exam guide. McGraw-Hill., 2005.

[UMIC, 2010] IP, U.-A. p. a. S. d. C. A Sociedade da Informação em Portugal.

[ISACA, 2012] ISACA Business Framework for the Governance and Management of Enterprise IT. http://www.isaca.org/COBIT/Pages/default.aspx [último acesso: Set 2014]

[ISECOM, 2012] ISECOM Open Source Security Testing Methodology Manual. http://www.isecom.org/research/osstmm.html [último acesso: Set 2014]

[ITIL, 2011] ITIL What is ITIL ?. http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx [último acesso: Set 2014]

[ITSEC, 1991] ITSEC Information Technology Security Evaluation Criteria. 1991

[Kevin, M., Williams, S. and Steve, W., 2002] Kevin, M., Williams, S. and Steve, W. The art of deception. Wiley Publishing, 2002.

[Loch, K. D., Carr, H. H. and Warkentin, M. E., 1992] Loch, K. D., Carr, H. H. and Warkentin, M. E. Threats to information systems: today's reality, yesterday's understanding. MIS Quarterly 1992), 173-186.

[Mashable, 2012] Mashable Anonymous Hacks Department of Justice. http://mashable.com/2012/05/22/anonymous-department-justice/ [último acesso: Dez 2013]

[Mitrović, P., 2005] Mitrović, P. Handbok i IT-säkerhet (4: e uppl.). Falun: Pagina Förlags AB 2005).

[Net-security, 2012] Net-Security Criminals stole $3.4B from online revenues in 2011. http://www.net-security.org/secworld.php?id=12273 [último acesso: Set 2014]

[Networkworld, 2008] Networkworld Morris worm turns 20: Look what it's done. http://www.networkworld.com/article/2268919/lan-wan/morris-worm-turns-20--look-what-it-s-done.html [último acesso: Set 2014]

[NP27001, 2013] Norma Portuguesa para “Tecnologia da Informação. Técnicas de segurança. Sistemas de Gestão de Segurança da Informação – Requisitos”. Instituto Português da Qualidade. Ministério da Economia. 2013

[OWASP, 2013] OWASP OWASP Top 10. 2013. https://www.owasp.org/index.php/Top_10_2013-Top_10 [último acesso: Set 2014]

[OWASP, 2009] OWASP Application Security Verification Standard 2009. 2009.

[Pcisecuritystandards, 2010] pcisecuritystandards PCI - Requirements and Security Assessment Procedures. 2010.

[Pfleeger, et al, 2006] Pfleeger, C. P. P. a. S. L. Is There a Security Problem in Computing? , 2006.

[Portalgsti, 2013] Portalgsti Guia para certificação ITIL Foundation. 2013.

[RR, 2013] Renascença, R. Ataque visa sites de partidos e forças de segurança.

2013.http://rr.sapo.pt/informacao_detalhe.aspx?fid=25&did=105281 [último acesso: Set 2014]

[Rot, A., 2008] Rot, A. IT risk assessment: quantitative and qualitative approach. Resource, 2832008), 284.

[Santos, J., 2011] Santos, J. Contributos para uma melhor governação da cibersegurança em Portugal. Universidade Nova de Lisboa, 2011.

[Schneier, B., Wagner, D., 1999] B. Schneier, and D. Wagner, "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)," Secure Networking—CQRE [Secure]'99, pp. 192-203: Springer, 1999.

[Schneier, B., 2013] Schneier, B. People, Process, and Technology. 2013.

[Schneier, B., 2008] Schneier, B. IT Attacks: Insiders vs. Outsiders. 2008.

[Schultz, E., 2005] Schultz, E. The human factor in security. Computers & Security, 24, 6 2005), 425-426.

[Security, 2014] Security, E.-E. U. A. f. N. a. I. Glossary. 2014.

[Sêmola, M., 2003] Sêmola, M. Gestão da Segurança da informação. Elsevier Brasil, 2003.

[Silva, J. A. d., 2001] Silva, J. A. d. Os desafios da sociedade da informação. 2001.

[Siponen, Mikkto T.,2000] A conceptual foundation for organizational information security awareness." *Information Management & Computer Security* 8.1 (2000): 31-41.

[Sol, 2012] Sol Hacktivistas divulgam dados de 1 milhão de contas de 100 sites. 2012. http://www.sol.pt/noticia/57830 [último acesso: Set 2014]

[Sol, 2012] Sol Anonymous ataca sites do Governo do Reino Unido. 2012. http://www.sol.pt/noticia/57294 [último acesso: Set 2014]

[Straub, D. W. and Welke, R. J., 1998] Straub, D. W. and Welke, R. J. Coping with systems risk: security planning models for management decision making. Mis Quarterly1998), 441-469.

[Tanenbaum, A. S., 2003] Tanenbaum, A. S. Computer Networks, 4-th Edition. Prentice Hall, 2003.

[Technology, 2002] Technology, N.-N. I. o. S. a. Risk Management Guide for Information Technology Systems. 2002.

[Toffler, A. 1980] Toffler, A. A terceira onda. Record, 1980.

[Tregear, J., 2001] Tregear, J. Risk assessment. Information Security Technical Report, 6, 3 2001), 19-27.

[Veracode, 2013] Veracode LDAP Injection Guide: Learn How to Detect LDAP Injections and Improve LDAP Security. 2013. https://www.veracode.com/security/ldap-injection [último acesso: Set 2014]

[Verizon, 2013] Verizon 2013 Data Breach Investigations Report. 2013. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf [último acesso: Set 2014]

[Wadlow, T. A., 2000] Wadlow, T. A. The process of network security: designing and managing a safe network. Addison-Wesley Professional, 2000.

[Whitman, M., Mattord, H., 2011] Whitman, M. and Mattord, H. Principles of information security. Cengage Learning, 2011.

[Young, E., 2013] Young, E. Under cyber attack - EY's Global Information Security Survey 2013. http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf [último acesso: Set 2014]