Marcação CE de Dispositivos Médicos e Segurança em Software

Célio Eduardo Sousa Cerqueira

Dissertação apresentada no Instituto Superior de Engenharia do Porto para a obtenção de grau de Mestre em Engenharia de Computação e Instrumentação Médica

Orientadores
Doutor António Manuel Cardoso da Costa
Departamento de Informática - ISEP

Engenheiro Filipe Pires de Morais
Engenheiro Ricardo Pinho
Efficientia Management Integration, Consulting, Lda

Porto, 9 de Dezembro de 2012

Aos meus pais, Maria e Albino Cerqueira.

Agradecimentos

A minha primeira palavra de agradecimento dirige-se aos meus orientadores, Doutor António Costa, Engenheiro Filipe Morais e Engenheiro Ricardo Pinho.

À instituição que me acolheu, que fez com que tudo isto fosse possível, a Efficientia Management Integration, Consulting, Lda pelo departamento Medical Solutions.

Aos meus colegas e amigos que me ajudaram sempre que necessitei, Hélder da Silva, António Vaz, Nuno Pereira e especialmente à Diana Barros.

À Cátia por todo o apoio, dedicação e compreensão.

Aos meus pais e irmã dirijo o meu maior agradecimento por me permitirem chegar até aqui.

Resumo

Com o crescente aumento da Teleradiologia, sentiu-se necessidade de criar mais e melhores softwares para sustentar esse crescimento. O presente trabalho pretende abordar a temática da certificação de software e a sua marcação CE, pois para dar entrada no mercado Europeu todos os Dispositivos Médicos (DM) têm de estar devidamente certificados. Para efetuar a marcação CE e a certificação serão estudadas normas e normativos adequados para marcação de DM ao nível Europeu e também dos Estados Unidos da América. A temática da segurança de dados pessoais será também estudada de forma a assegurar que o dispositivo respeite a legislação em vigor. Este estudo tem como finalidade a certificação de um software proprietário da efficientia sysPACS, um serviço online abrangente, que permite a gestão integrada do armazenamento e distribuição de imagens médicas para apoio ao diagnóstico.

Palavras-chave: Certificação de software; Marcação CE; Segurança de dados; Dispositivos Médicos; DICOM; PACS, HL7.

Abstract

With the increasing use of tele-radiology, it is necessary to develop more and better software to support this growth without compromising security and safety. This study addresses the software certification in general and the CE label in particular, because all medical devices related software to be used in the European market must be a priori certified. To achieve CE label and software process certification, legislation, standards and good-practices associated with medical devices in Europe and in the United States of America will be identified and analyzed. The subject of personal data security will be addressed in order to ensure that the medical device complies with current legislation. This study aims at the certification of proprietary software from Efficientia (sysPACS), a comprehensive online web-based information system supporting an integrated storage management and the distribution of medical data for diagnostic purposes.

Keywords: Software certification, CE label, Data Security, Medical Devices, DICOM, PACS, HL7.

Conteúdo

Resumo . . . viii

Abstract . . . x

Conteúdo . . . xii

Lista de Figuras . . . xiii

Lista de Tabelas . . . xv

Lista de Abreviaturas . . . xx

1. Introdução . . . 1
- 1.1 Telemedicina . . . 2
  - 1.1.1 Teleradiologia . . . 4
  - 1.1.2 PACS . . . 6
- 1.2 Objetivos e Motivação . . . 7
- 1.3 Apresentação do Problema e Contribuições . . . 8
- 1.4 Estrutura da Dissertação . . . 8
- 1.5 Planeamento . . . 9

2. Marcação CE de Dispositivos Médicos . . . 11
- 2.1 Dispositivos Médicos . . . 11
  - 2.1.1 Classificação . . . 13
- 2.2 Marcação CE . . . 15
  - 2.2.1 Diretivas aplicáveis . . . 17
  - 2.2.2 Requisitos específicos do produto . . . 19
  - 2.2.3 Organismo Notificado . . . 20
  - 2.2.4 Avaliação da conformidade . . . 21
  - 2.2.5 Documentação técnica . . . 22
  - 2.2.6 Aposição da Marcação CE e declaração de conformidade . . . 22
  - 2.2.7 Qualidade em Saúde . . . 23

3. Segurança em Software . . . 27
3.1 Segurança de Aplicações WEB . . . 29
3.2 Protocolos e Normas de Segurança em Saúde . . . 35
3.2.1 DICOM . . . 35
3.2.2 HL7 . . . 37
3.2.3 Técnicas de segurança - ISO 17799 . . . 38
3.3 Proteção de Dados . . . 40
3.4 Gestão de Risco . . . 42
3.4.1 Gestão de risco em Dispositivos Médicos - ISO 14971:2007 . . . 43
3.4.2 *Failure Modes and Effect Analysis* . . . 46
3.5 Licenciamento em Software . . . 48

4. Implementação do efficientia sysPACS . . . 53
4.1 Medical Image Service . . . 53
4.2 efficientia sysPACS . . . 54
4.2.1 Módulos . . . 55
4.2.2 Ferramentas . . . 58
4.3 Processo de Marcação CE . . . 61
4.3.1 Classificação do Dispositivo Médico . . . 61
4.3.2 Processo . . . 65
4.4 Gestão de Risco - efficientia sysPACS . . . 66
4.5 Avaliação dos aspectos de segurança . . . 71
4.5.1 Comparação do MIS com o sysPACS . . . 72

5. Conclusões e Perspetivas futuras . . . 79

Bibliografia . . . 81

A. Anexos . . . 87
A.1 Requisitos Essenciais . . . 87
A.2 Declaração de Conformidade . . . 104
A.3 Requerimento Avaliação da Conformidade . . . 107
A.4 Declaração de Compromisso . . . 109
A.5 Manual de Utilizador . . . 112
A.6 Processo de Concepção . . . 135
A.7 Checklist - Avaliação dos aspetos de segurança . . . 137
A.8 FMEA . . . 144
A.9 Fluxograma dos Procedimentos de Avaliação de Conformidade . . . 148

Lista de Figuras

1.1 Equipamentos de telemedicina 3
1.2 Esquema de um sistema em teleradiologia 5

2.1 Passos gerais para a marcação CE 16
2.2 Exigência da marcação CE para dispositivos médicos 18
2.3 Marca CE 23
2.4 Modelo Qualidade 24

3.1 AIC Triad 28
3.2 Arquitetura *web*. 29
3.3 Arquitetura *web*. 39
3.4 Processo da Gestão de Risco. 45

4.1 Requisitos Essenciais 66
4.2 efficientia sysPacs. 71
4.3 MIS and efficientia sysPACS 74

A.1 Fluxograma dos Procedimentos de Avaliação de Conformidade 149

Lista de Tabelas

2.1 Sistema de classificação de Dispositivos Médicos 13

3.1 Escala usada no Top 10 das vulnerabilidades 30
3.2 Classificação do Top 10 do OWASP 34
3.3 Mecanismos mínimos para TLS 37
3.4 Probabilidade de ocorrência 45
3.5 Nível de gravidade 46
3.6 Cronograma que delimita o risco aceitável do não aceitável, pela conjugação do dano com a probabilidade. 46
3.7 Sistema de classificação da Gravidade 49
3.8 Sistema de classificação da Ocorrência 49
3.9 Sistema de classificação da Deteção 50
3.10 Escala RPN 50

4.1 Tipos de Licenciamento vs. Sistemas Operativos 62
4.2 Regras para Classificação da Classe do Dispositivo Médico. 63
4.3 Ferramentas a incluir na gestão de risco pós-mercado. 70

Lista de Abreviaturas

ACR	Americam College of Radiology
AES	Advanced Encryption Standard
API	Application Programming Interface
BSD	Berkeley Software Distribution
CE	European Conformity
CERN	European Organization for Nuclear Research
CMS	Content Management System
CNPD	Comissão Nacional de Proteção de Dados
CSRF	Cross Site Request Forgery
DES	Data Encryption Standard
DICOM	Digital Imaging and Communications in Medicine
DM	Dispositivos Médicos
EPL	Eclipse Public License
FDA	Food and Drug Administration
GPL	General Public License
HIS	Hospital Information Systems
HL7	Health Level Seven
HTML	HyperText Markup Language
INFARMED	Autoridade Nacional do Medicamento e Produtos de Saúde, I. P.
IPsec	Internet Protocol Security

ISO	International Organization for Standardization
ISP	Internet sSrvice Provider
JSP	JavaServer Page
MAC	Apple Macintosh
MD5	Message Digest 5
MIS	Medical Image Service
MSW	microsoft windows
NANDO	New Approach Notified and Designated Organisations
NEMA	National Electrical Manufacturers Association
ON	Organismo Notificado
OSI	Open systems Interconnection
OWASP	The Open Web Application Security
PACS	Picture Archiving and Communication Systems
PHP	Hypertext Preprocessor
PPTP	Point-to-Point Tunneling Protocol
RIS	Radiology Information System
RPM	Risk Priority Number
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SSL	Secure Sockets Layer
TAC	Tomografia Axial Computadorizada
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network
WADO	Web Access to DICOM Objects
WWW	World Wide Web
XML	eXtensible Markup Language

XSS Cross Site Scripting

Capítulo 1

Introdução

A grande expansão dos mercados da saúde, juntamente com o grande avanço tecnológico, introduziram no mercado um grande número de DM, com aplicação nas diversas áreas da medicina, abrindo grandes possibilidades para o diagnóstico médico e tratamento de doenças, colocando no entanto algumas questões de segurança.

Com este grande aumento na produção de dispositivos médicos, os países da União Europeia tiverem necessidade de uniformizar as normas, pelo que cada país devia deixar de ter regulamentos próprios e passar a usar os comunitários, designando-se esta abertura constitucional *Nova Abordagem* [1], sobre a qual se tem trabalhado para uma harmonização das diretivas.

Para a sua colocação no mercado, os dispositivos médicos têm de estar de acordo com as regras impostas pela União Europeia. Para tal, tem de existir um organismo que verifique se essas regras são aplicadas de forma correcta. Com o constante aumento da legislação e da sua complexidade, juntamente com a variedade dos dispositivos médicos, começa a ser cada vez mais necessária a existência de profissionais com um grande *know-how* para a realização destas tarefas.

A presente dissertação é desenvolvida no âmbito do Mestrado de Engenharia em Computação e Instrumentação Médica, tendo em conta o estágio realizado na empresa Efficientia Management Integration, Consulting, Lda no departamento Medical Solutions, que está a desenvolver um *software* destinado à teleradiologia, o efficientia sysPACS.

O efficientia sysPACS está a ser desenvolvido com o objetivo de o comercializar no mercado Europeu, devendo por isso ostentar a marcação CE.

A aposição da marcação CE é uma evidência dada pelo fabricante de que o produto está em conformidade com as disposições das diretivas europeias aplicáveis.

Para melhor compreensão dos temas abordados inicialmente, começaremos por explicar temas base com a Telemedicina, Teleradiologia e PACS.

1.1 Telemedicina

A Telemedicina não é propriamente uma novidade, pois é um conceito que já tem alguns anos de história. Segundo [2], a revista *Radio News Magazine* em 1924 mostrou um desenho de um médico que observava um paciente à distância, marcando assim o início desta atividade.

Várias definições foram propostas por diferentes autores [3], mas todas centram-se na premissa de que a telemedicina é a prestação de cuidados de saúde a distância. No entanto para o rigor deste trabalho adoptou-se a definição que é proposta pelo Parlamento Europeu:

"Entende-se por telemedicina a prestação de serviços de saúde através da utilização das tecnologias da informação e das comunicações em situações em que o profissional de saúde e o doente (ou dois profissionais de saúde) não se encontrem no mesmo local. A telemedicina compreende a transmissão segura de informações e dados médicos, necessários para a prevenção, diagnóstico, tratamento e seguimento dos doentes, por meio de texto, som, imagens ou outras vias" [4].

Existem diferentes tipos de telemedicina, como por exemplo: a telemonitorização, a teleconsulta e a teleradiologia. A teleradiologia, o método mais comum, baseia-se no envio de imagem de um centro de imagem médica para o respetivo médico que, através da imagem, efetua o diagnóstico do doente.

O conceito de teleconsulta está relacionado com a realização de uma consulta, por parte do médico, à distância e também com a possível necessidade de uma segunda opinião médica [5, 6].

A telemonitorização, como o próprio nome indica, consiste em monitorizar um doente à distância, como por exemplo registar os batimentos cardíacos no caso de um doente com insuficiência cardíaca [7].

Um sistema como o de telemedicina, que resulta da fusão das tecnologias de informação e comunicação, [8], levanta inúmeras questões de segurança e confiabilidade, colocando em risco a privacidade dos pacientes. Para a resolução destas questões a União Europeia tem clarificado questões jurídicas para que os Estados-Membros avaliem as suas regulamentações e as adaptem para facilitarem o acesso a serviços de telemedicina. Esta clarificação tem incidido sobre questões como a responsabilidade clínica, a privacidade e a proteção de dados [4, 3].

Com o grande aumento da população idosa, o que significa mobilidade reduzida, e também com o aumento do número de pessoas com doenças crónicas, os cuidados médicos de que necessitam têm, muitas vezes, de ser prolongados. No entanto, a telemedicina pode revelar-se uma grande ajuda na resolução da maioria destes problemas, como, por exemplo, facilitar o acesso a cuidados de saúde especializados, a diminuição de dias dos internamento hospitalar devido à telemonitorização dos doentes crónicos. A teleradiologia pode ser utilizada na optimização de recursos, permitindo a diminuição do tempo de resposta.

Este sistema apresenta vantagens, a saber: a prestação de serviços de saúde à distância pode melhorar, tornar mais fácil e rápido o serviço que é prestado às pessoas, melhorando assim alguns dos problemas do sistema de saúde [8].

A telemedicina é uma área que tem ainda alguns problemas técnicos como o acesso à banda larga e a garantia de obtenção de conectividade, que são condições essenciais à difusão da telemedicina. A normalização de todas as disciplinas da telemedicina é fundamental para a sua expansão[4].

Hasan et al realizaram um estudo em 2010 com o objectivo de fornecer cuidados de saúde a zonas isoladas. Pode ver-se na Figura 1.1 um esquema da estrutura utilizada por *Hasan et al* no seu projeto, que serve para demonstrar como é que funciona um sistema de telemedicina [8].

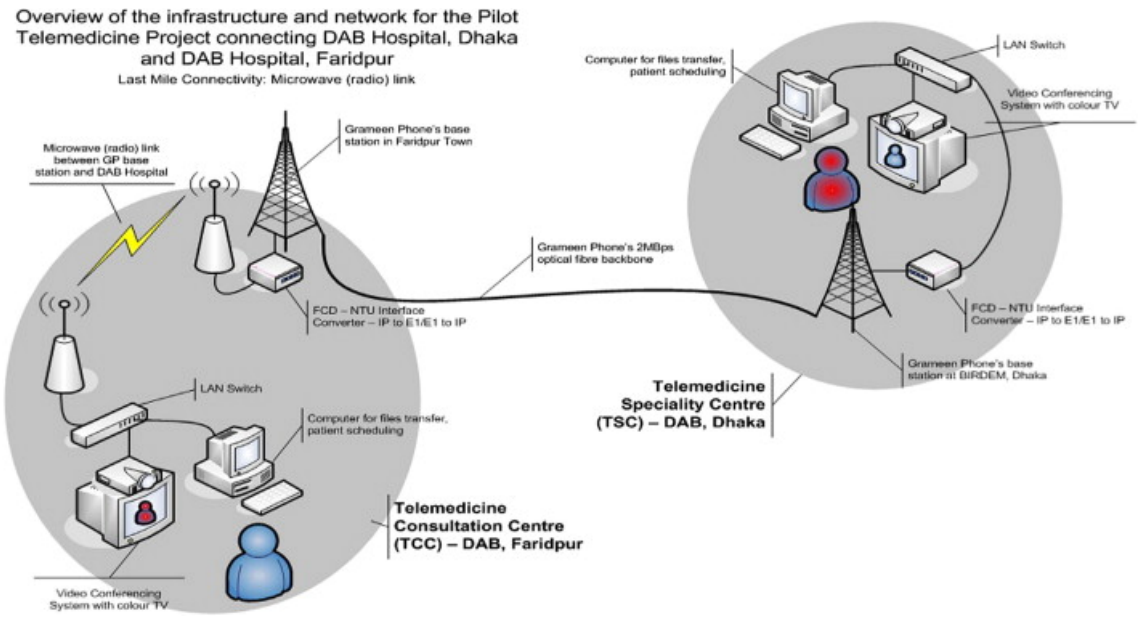


Fig. 1.1: Equipamentos de telemedicina [8]

1.1.1 Teleradiologia

A Teleradiologia não consiste só numa simples transmissão de imagens médicas, envolve também uma partilha de conhecimentos entre os profissionais. Porque este serviço facilita o acesso a relatórios médicos, permite a troca de opiniões entre médicos, bem como a obtenção de uma segunda opinião, entre outros benefícios [9].

Para a teleradiologia poder beneficiar de todas estas vantagens, tem de estar interligada com um sistema Picture Archiving and Communication Systems (PACS), sistema que vai permitir toda esta gestão de ligações.

A teleradiolgia teve uma evolução ao longo dos tempos, passando de um simples envio de uma imagem do centro hospitalar para o computador do médico, no início da década de 50 [10], para um sistema de maior complexidade, em que é possível obter um histórico de todas as imagem de um determinado paciente e aceder a informações do Radiology Information System (RIS).

Actualmente os sistemas de teleradiologia já permitem, juntamente com a informação do paciente, obter o ditado ou o relatório que o médico fez do exame [11, 12]. Este avanço tecnológico está relacionado com a aceitação e generalização do protocolo de comunicação de imagens médicas, o *Digital Imaging and Communication in Medicine*, (DICOM) [13].

A teleradiologia apresenta-se como mais valia e consegue dar resposta ao grande fluxo de trabalho dos profissionais da imagiologia médica. No entanto existem questões que se devem colocar antes de se optar por um sistema de teleradiologia:

- Como é que a informação é transmitida e integrada?
- Quem tem acesso à imagem e aos relatórios armazenados?
- A que legislação está sujeito o paciente no país de origem?
- Como se trata a privacidade e integridade dos dados?
- Como é assegurada a comunicação entre médicos e radiologistas?
- Quais os aspetos médico-legais a ter em conta? [11].

Segundo [9], não existem aspetos legais específicos para a teleradiologia, no entanto existe um conjunto substancial de legislação que é transversal, aos diversos países, e que será aprofundada no Capítulo 2.

A União Europeia desenvolveu um conjunto de diretivas que abordam algumas questões relacionadas com esta área, como a Directiva de Protecção de Dados Pessoais [14].

Os aspetos mais sensíveis da teleradiologia estão relacionados com os pacientes, a saber:

- Direitos, confidencialidade, proteção de dados;
- Serviços com o máximo de qualidade;
- Garantir a identidade única de todos os pacientes;
- Serviço com segurança e rastreabilidade [9].

Para uma máxima qualidade no serviço e para que os dados médicos dos pacientes sejam mantidos com segurança, o sistema de telaradiologia deverá garantir níveis adequados de segurança na manutenção da privacidade e na transmissão de dados [9].

Relativamente à segurança, existem várias políticas que podem ser aplicadas ao sistema de telaradiologia, tais como política de segurança física, segurança em rede, juntamente com um conjunto de diretrizes de segurança, como por exemplo criptografia. A confidencialidade pode ser mantida por meio de uma rede VPN, já a integridade pode ser assegurada usando a norma DICOM com compressão sem perdas [11].

Pode ver-se na Figura 1.2 um esquema de um sistema de teleradiologia, muito simples, de uma rede DICOM que permite o acesso às imagens através da internet.

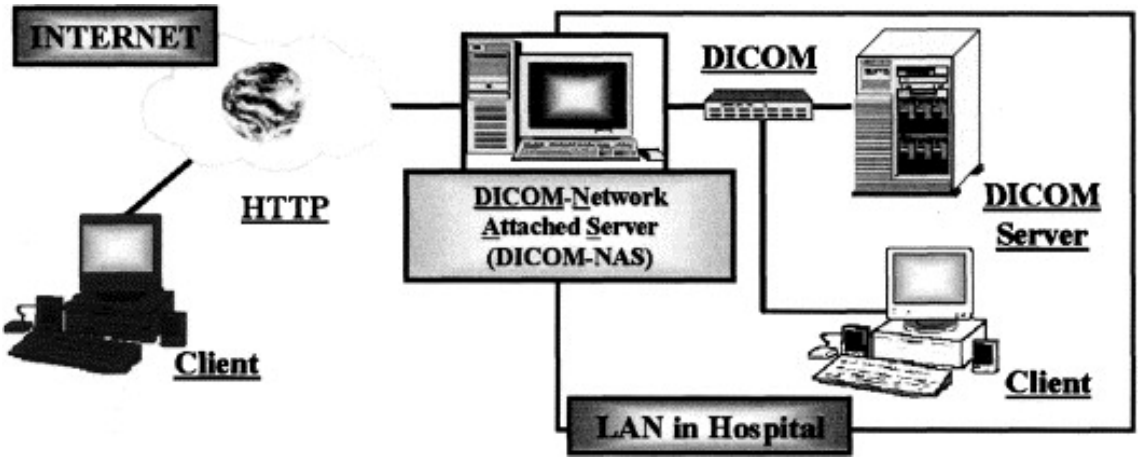


Fig. 1.2: Esquema de um sistema em teleradiologia [15]

1.1.2 PACS

O PACS é um sistema que, por via electrónica, processa, armazena, distribui e recupera imagens médicas [2] procedentes de modalidades de imagiologia médica como Tomografia Computorizada, Ressonância Magnética, entre outras.

A arquitectura geral do PACS consiste na aquisição de uma imagem, um servidor de arquivo e *workstations* integradas na rede (PACS), por sua vez ligados ao sistema de informação do hospital, o *Radiology Information System/Hospital Information Systems* (HIS/RIS) [12].

O servidor PACS é o "motor" do PACS, consistindo em computadores ou servidores, e tem como principais componentes uma base de dados e um sistema de arquivo, que pode armazenar em curto, médio ou longo prazo.

Estes servidores têm como principais funções:

- Receber as imagens dos exames;
- Entender a informação que consta no cabeçalho da imagem DICOM;
- Encaminhar os exames para as *workstations*;
- Permitir o visionamento de imagem antigas.

A segurança da informação contida no PACS é um ponto de extrema importância, devido à confidencialidade dos dados médicos do paciente, que tem de ser preservada.

Arquitetura do PACS

Existem três tipos de arquitecturas PACS, o *stand-alone*, *cliente-servidor* e *Web-based*. [12].

No stand-alone as imagem são enviadas automaticamente para as estações de trabalho, onde se pode fazer *Query/Retrieve*[1] às imagens que estão no servidor.

Na arquitetura cliente-servidor as imagens são armazenadas centralmente no servidor do PACS. Este envia uma lista de trabalho para as *workstations*, onde é possível selecionar os pacientes juntamente com as imagens. Não existe um armazenamento local, pelo que as imagens são descartadas após a leitura.

[1] Query / Retrieve é um serviço DICOM que permite ao utilizador visualizar a lista de exames do doente e transferir as imagens desejadas [13].

Por último, o modelo baseado na web é muito semelhante ao do cliente-servidor, estando a principal diferença no servidor orientado para aplicações *web*. Comparando com o modelo anterior, tem como principais vantagens ser um sistema completamente portátil, permitindo ao médico aceder aos exames em qualquer parte do mundo. O hardware das estações de trabalho pode ser independente, bastando um *web browser* adequado.

No entanto apresenta como desvantagens as limitações do *web browser*: funcionalidade e performance. Estes sistemas têm evoluído nos últimos anos e estão a tornar-se sistemas dominantes [12].

1.2 Objetivos e Motivação

A razão que levou à escolha deste tema foi o facto de permitir estar em contacto com uma solução empresarial de valor crescente no mercado, adquirindo conhecimentos abrangentes na área da imagem médica, certificação, segurança informática e programação *web*.

Com este trabalho pretende-se estudar os métodos existentes para a certificação de software médico como dispositivo médico e questões relacionadas com segurança informática e da informação. Para a obtenção da marcação CE, que será atribuída pela autoridade competente, a Autoridade Nacional do Medicamento e Produtos de Saúde, I. P. (INFARMED), é necessário estudar as normas relacionadas com a certificação de software, juntamente com as boas práticas e normas de segurança. A solução terá de estar de acordo com a entidade que rege a proteção de dados, a Comissão Nacional de Proteção de Dados (CNPD).

O objetivo principal desta dissertação passa então por preparar a documentação do software para a sua marcação. Além deste, outros objetivos podem ser considerados como de grande importância:

- Objetivos
  - Melhorar o sistema atual;
  - Implementar segurança no sistema;
  - Analisar os riscos associados;
  - Estudar e compreender directivas nacionais e internacionais sobre os Dispositivos Médicos;
  - Estudar e compreender normas de segurança e boas práticas em software;

– Compreender, realizar e implementar um sistema de Teleradiologia.

1.3 Apresentação do Problema e Contribuições

O acesso a dados médicos de pacientes através da rede informática é fundamental para optimizar os processos de prestação de cuidados de saúde. Para ser bem aceite este tipo de partilha de informação médica é necessário que o sistema seja seguro.

De forma a permitir esta troca de dados médicos na Internet é necessário criar uma solução que cumpra todas as recomendações e boas práticas de segurança. A solução deve ser preparada para marcação CE, com vista à comercialização no mercado Europeu.

As grandes contribuições deste trabalho passaram pela preparação de uma solução de teleradiologia para marcação CE bem como a respetiva implementação de segurança informática de toda a solução. O grande benefício é o fabrico de um sistema que permite a troca de informação médica de uma forma segura na Internet.

Este sistema vem trazer uma maior confíança aos utilizadores pois irá permitir que sejam trocados dados clínicos na Internet com segurança quer para o utilizador quer para os utentes.

1.4 Estrutura da Dissertação

O presente trabalho encontra-se dividido em 5 capítulos. No Capítulo 1 é apresentada a problemática teórica e é feito o seu enquadramento, bem como aquilo que se pretende alcançar com este trabalho. Apresenta-se ainda o modo para atingir esses objetivos.

No Capítulo 2 são apresentadas noções teóricas de dispositivos médicos juntamente com a legislação associada, assim como a descrição do processo de marcação CE.

No Capítulo 3 é apresentada a problemática da segurança, bem como processos a adaptar para a implementação de um sistema seguro.

No Capítulo 4 é apresentado o sistema que foi desenvolvido, juntamente com os processos associados à marcação e classificação entre outros.

Finalmente, no Capítulo 5 são apresentadas as ideias mais importantes que foram alcançadas com a elaboração deste trabalho, bem como algumas propostas para trabalho futuro.

1.5 Planeamento

O planeamento deste projeto foi estruturado em quatro fases, sendo elas:

1. Requisitos
    - Levantamento de requisitos;
    - Estado da arte;
    - Requisitos do sistema;
2. Implementação
    - Implementação de todo sistema;
    - Preparação para a Marcação CE;
3. Verificação
    - Testes ao sistema;
4. Elaboração da dissertação.

Capítulo 2

Marcação CE de Dispositivos Médicos

Os Dispositivos Médicos são instrumentos que se destinam a ser utilizados para fins como diagnóstico, prevenção ou tratamento de uma doença. Esta definição inclui uma gama muito vasta de produtos, que podem ir de um simples termómetro até uma Ressonância Magnética.

Segundo o estudo da *Acmite Market Intelligence*, [16], os DM apresentam um crescimento anual de 6 a 9%, sendo este um mercado que movimenta muitos milhões de euros na Europa.

A marcação CE dá-nos a garantia de que um produto está de acordo com a legislação da União Europeia, pois esta marcação permite que o produto circule de forma segura no mercado Europeu.

Para um DM ostentar a marcação CE deve estar em conformidade com os requisitos legais que fazem parte integrante do Decreto-Lei n.º145/2009. Para tal, deve ser submetido junto do Organismo Notificado (INFARMED) a uma avaliação de conformidade. Para essa avaliação, o fabricante tem de elaborar uma declaração CE de Conformidade com a respetiva documentação técnica [17].

2.1 Dispositivos Médicos

O Artigo 3.º do Decreto-Lei 145/2009, que transpõe internamente as Diretivas Europeias sobre Dispositivos Médicos, define como dispositivo médico "*qualquer instrumento, aparelho, equipamento, software, material ou artigo utilizado isoladamente ou em combinação, incluindo o software destinado pelo seu fabricante a ser utilizado especificamente para fins de diagnóstico ou terapêuticos e que seja necessário para o bom funcionamento do dispositivo médico, cujo principal efeito pretendido no corpo*

humano não seja alcançado por meios farmacológicos, imunológicos ou metabólicos, embora a sua função possa ser apoiada por esses meios, destinado pelo fabricante a ser utilizado em seres humanos" .

O artigo anterior define também os fins dos dispositivos médicos, que são:

i) *"Diagnóstico, prevenção, controlo, tratamento ou atenuação de uma doença;"*

ii) *"Diagnóstico, controlo, tratamento, atenuação ou compensação de uma lesão ou de uma deficiência;"*

iii) *"Estudo, substituição ou alteração da anatomia ou de um processo fisiológico;"*

iv) *"Controlo da concepção."*

Uma outra definição a considerar para este trabalho é a de Dispositivo médico ativo, que se define como: "*qualquer dispositivo médico cujo funcionamento depende de uma fonte de energia eléctrica, ou outra não gerada directamente pelo corpo humano ou pela gravidade, e que actua por conversão dessa energia, não sendo considerados como tal os dispositivos destinados a transmitir energia, substâncias ou outros elementos entre um dispositivo médico activo e o doente, sem qualquer modificação significativa e sendo que o software, por si só, é considerado um dispositivo médico activo;*" [17].

Nos Estados Unidos da América, a Food and Drug Administration (FDA) é a entidade que regula os dispositivos médicos, segundo Diretivas próprias como a *FD&C Act*.

Uma definição de Dispositivos Médicos segundo essa Diretiva é:

A medical device is an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

- *recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,*
- *intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or*
- *intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of it's primary intended purposes through chemical action within or on the body of man or other animals and*

which is not dependent upon being metabolized for the achievement of any of its primary intended purposes. Pode ser consultada no site da FDA.[1]

2.1.1 Classificação

Não é comercialmente viável submeter todos os dispositivos médicos a procedimentos de avaliação muito rigorosos, é mais viável dividir em grupos e submeter cada grupo aos testes mais adequados.

Para assegurar que a avaliação é bem feita o fabricante deve ser capaz de determinar a classificação do dispositivo do modo mais preliminar possível [18]. Desta feita foi acordada a criação de um sistema de classes, para que cada fabricante possa classificar os seus dispositivos.

A classificação é baseada no risco que tem por base a vulnerabilidade do corpo humano, tendo em conta os potenciais riscos associados ao próprio dispositivo [19]. Desta abordagem surgem alguns critérios que combinados permitem a classificação dos dispositivos.

Os dispositivos médicos podem ser classificados de várias formas, sendo que, a determinação da classe do dispositivo é preponderante para a marcação CE. É com base neste tópico que vai assentar todo processo [17]. O sistema de classificação geral proposto pela Diretiva Europeia 93/42/EEC e pelo Decreto-Lei 145/2009 está representado na tabela 2.1.

Tab. 2.1: Sistema de classificação de Dispositivos Médicos.

Classe	Nível de Risco	Exemplo
A	Baixo	Termómetro
C	Baixo-Moderado	Ressonância Magnética
C	Moderado-Alto	Sacos de sangue
D	Alto	Válvula Cardiaca

De seguida os níveis de requisitos regulamentares que aumentam a classe de risco.

- sistema da qualidade;
- dados técnicos;
- testes ao produto;

[1] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm

- evidência clínica;
- auditoria externa independente;
- revisão externa independente dos dados técnicos.

A classificação tem como base os potenciais riscos que pode causar ao ser humano e depende de alegações feitas pelo fabricante e aplicação pretendida. De acordo com o Artigo 4º do Decreto - Lei 145/2009, está dividida em 4 classes [20, 18]:

- Classe I;
- Classe IIa;
- Classe IIb;
- Classe III.

A classificação é obtida através da aplicação de 18 regras que são definidas pelo Decreto-Lei 145/2009. As regras estão subdivididas em 4 grupos: Dispositivos não invasivos, Dispositivos Invasivos, Dispositivos activos e Dispositivos especiais [18]. A classificação dos dispositivos médicos está relacionada com vários factores determinantes:

- a duração de contato com o corpo;
- invasibilidade (invasivo, não invasivo);
- área do corpo afetada;
- riscos da conceção técnica e de fabrico;
- fim a que se destina [19, 17].

É aceitável dizer-se que as normas existentes em alguns casos são inadequadas para a classificação dos dispositivos. Estes casos incluem em especial os casos limítrofes entre as duas classes. Para além destes podem existir dispositivos de natureza incomum, isto é, não tipificados.

Para uma boa classificação o fabricante deve proceder de acordo com os quatro pontos seguintes.

- o produto é realmente um dispositivo médico;

- documentação específica do produto;
- aplicação de todas as regras, optando pela classificação mais elevada;
- verificar a aplicação de regras nacionais específicas [19].

2.2 Marcação CE

O grande crescimento de produtos ligados à tecnologia médica e as inconsistências legais no mercado Europeu levaram a que a União Europeia adoptasse a *"nova abordagem"* na harmonização técnica, descrita na *Resolução do Conselho 85/C136/01, de 7 de Maio de 1985*. Esta abordagem introduziu um conjunto de normas comuns a toda a União. Os fabricantes dispõem assim de um mercado único, permitindo a livre circulação dos produtos. Anteriormente a esta *nova abordagem*, as principais barreiras eram as leis nacionais e normas associadas à segurança dos produtos [21].

Os estados membros foram obrigados a harmonizar as suas regulamentações de acordo com as regulamentações comunitárias, sendo esta mudança apelidada de *"nova abordagem"*. Com ela os Estados designaram Autoridades Competentes que por sua vez designaram Organismos Notificados. Essencialmente a *"nova abordagem"* obriga a que as Diretivas contenham requisitos essenciais que os produtos devem respeitar [21].

Nem todos os produtos que circulam no mercado Europeu têm de ostentar a Marcação CE esta só é obrigatória para produtos que pertencem a categorias abrangidas por Diretivas específicas. Os Dispositivos médicos pertencem a esta categoria, como nos dizem as Diretivas 93/42/EEC e 2007/47/CE, transpostas para o Decreto-Lei 145 de 2009 [22].

A Marcação CE não é uma marca atribuída a produtos fabricados na Europa, mas sim a um produto que está em conformidade com as normas impostas pela Comunidade Europeia e respeita todas as disposições legais. Significa isto que o fabricante comprovou perante o ON (Organismo Notificado) os requisitos essencias das diretivas aplicáveis.

O processo de Marcação CE é da total responsabilidade do fabricante, que deve fazer a avaliação da conformidade, elaboração da ficha técnica, emissão da declaração CE de conformidade e aposição da marcação CE no produto. Já os distribuidores têm de provar a existência da marcação CE com a documentação de apoio.

Existem procedimentos que têm de ser cumpridos independentemente do produto, podendo dividir-se em 6 passos, como se pode ver na Figura 2.1, os quais

serão posteriormente explicados.

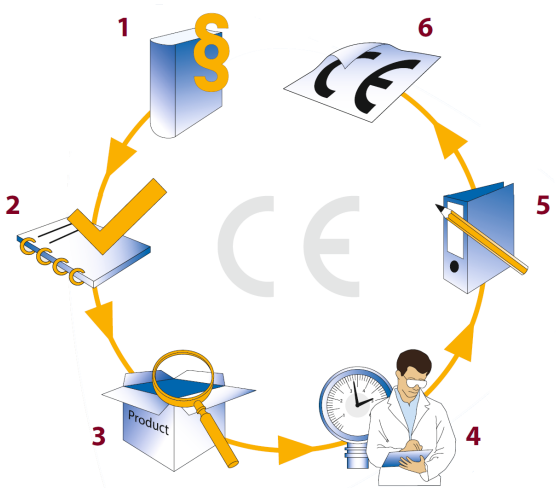


Fig. 2.1: Passos gerais para a marcação CE[2] [23]

1. **Identificar as diretivas aplicáveis**

   Existem aproximadamente 20 diretivas que definem as categorias dos produtos que devem ter Marcação CE. No caso dos dispositivos médicos essa diretiva é a 93/42/EEC, que sofreu ao longo dos anos várias modificações. A última versão pode ser consultada na diretiva 2007/47/EC ou no site da ec.europa[3]. Posteriormente, as diretivas publicadas como normas europeias harmonizadas baseadas nas diretivas, onde são especificados tecnicamente os requisitos essenciais[4].

2. **Identificar a aplicabilidade dos requisitos ao produto**

   Cada diretiva tem métodos diferentes de conformidade, dependendo da classificação dos produtos, por exemplo, as diferentes classes de dispositivos médicos. Dependendo da classificação, cada diretiva tem um número de requisitos essências que o produto tem de satisfazer. Para se cumprir os requisitos essenciais de uma boa prática é necessário satisfazer uma norma harmonizada aplicável[5].

3. **Identificação do Organismo Notificado**

[3] http://ec.europa.eu/enterprise/policies/european-standards/harmonised-standards/medical-devices/index_en.htm
[4] http://www.ce-marking.org/list-of-standards.html
[5] http://ec.europa.eu/enterprise/policies/european-standards/harmonised-standards/medical-devices/index_en.htm

Cada diretiva especifica, se for necessário, recorrer a uma terceira entidade autorizada a realizar a avaliação de conformidade. Para os dispositivos médicos em Portugal, a autoridade competente é o INFARMED o que pode ver-se no site da ec.europa[6]ec.europa.

4. **Avaliação da conformidade do produto**

   Quando todos os requisitos essenciais estiverem definidos, é preciso garantir que são cumpridos, bem como todos os requisitos das normas harmonizadas aplicáveis e uma avaliação dos riscos [17].

5. **Elaboração da documentação técnica**

   A documentação técnica relativa ao produto deve abranger todos os aspetos relacionados com a conformidade.

6. **Aposição da Marcação CE e declaração de conformidade**

   A Marcação CE tem de ser aposta pelo fabricante ou representante. Por conseguinte cabe ao fabricante elaborar a declaração CE de conformidade e certificar que os produtos cumprem os requisitos [17].

Estes 6 passos para a marcação CE, que incorporam de forma direta ou indireta as exigências da marcação CE para dispositivos médicos como os da Figura 2.2, são temas a abordar nas seções seguintes.

2.2.1 Diretivas aplicáveis

O passo inicial para a marcação CE é a garantia de que o produto que pretende certificar é abrangido por Diretivas Europeias. Os dispositivos médicos, como seria expectável, estão abrangidos por um grande número de legislação aplicável. As diretivas que estão diretamente relacionada com a marcação CE de dispositivos médicos são:

- Diretiva n.º 90/385/CEE, de 20 de Junho, relativa a Dispositivos Médicos Implantáveis Activos.
- Diretiva n.º 93/42/CEE, de 14 de Junho, relativa a Dispositivos Médicos.
- Diretiva n.º 98/79/CE, de 27 de Outubro de 1998, relativa aos Dispositivos Médicos para Diagnóstico *In Vitro*.

[6] http://ec.europa.eu/ent

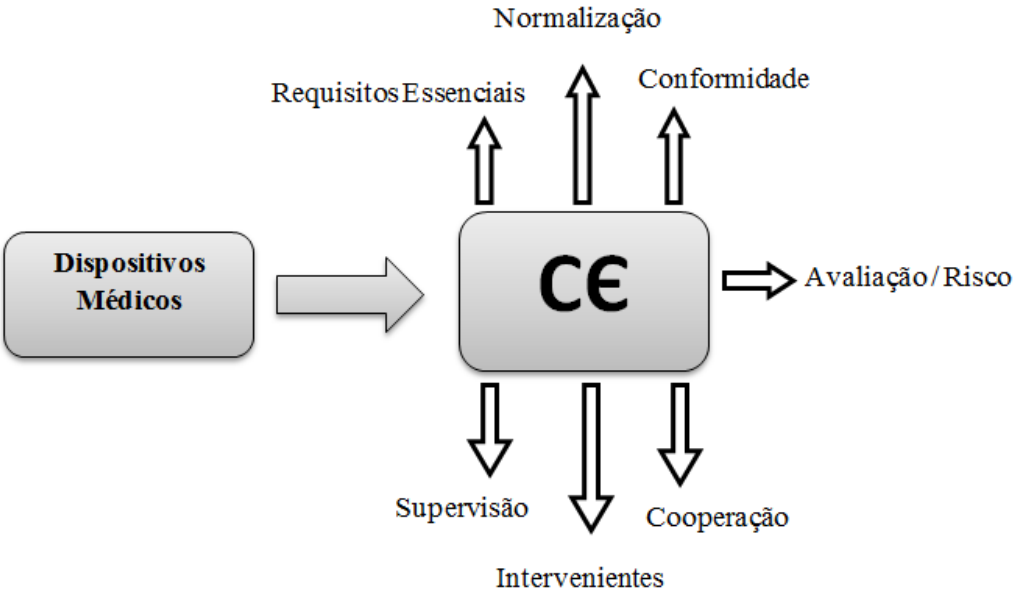


Fig. 2.2: Exigência da marcação CE para dispositivos médicos

- Diretiva n.º 2000/70/CE, de 16 de Novembro, relativa a Dispositivos Médicos que incorporam na sua composição derivados estáveis do sangue e plasma humanos.

- Diretiva n.º 2003/32/CE, de 23 de Abril, que introduz especificações pormenorizadas relativamente aos requisitos estabelecidos na Diretiva 93/42/CEE na sua actual redação, no que diz respeito a dispositivos médicos fabricados mediante a utilização de tecidos de origem animal.

- Diretiva n.º 2007/47/CE, de 5 de Setembro, que altera a Diretiva n.º 90/385/CE e Diretiva 93/42/CEE.

- Decreto-Lei nº 145/2009, de 17 de Junho: este decreto-lei estabelece as regras a que devem obedecer a investigação, o fabrico, a comercialização, a entrada em serviço, a vigilância e a publicidade dos dispositivos médicos e respetivos acessórios. Este decreto-lei transpõe para a lei interna a diretiva 2007/47/CE, 90/385/CEE, 93/42/CEE, 2000/70/CE, 2003/32/CE [17].

Como já foi referido, o Decreto-Lei nº 145 de 2009 tem com principal objetivo transpor para a ordem jurídica interna a Diretiva nº 2007/47/CE, do Parlamento Europeu e do conselho, de 5 de Setembro de 2007, alterando a Diretiva nº 93/42/CEE

relativa aos dispositivos médicos e assegurando a coerência legislativa entre as Diretivas 93/42/CEE e 90/885/CEE.

Estabelece que a Autoridade Competente deve ser notificada do exercício da atividade de fabrico e distribuição por grosso de dispositivos médicos, que o fabricante deve dispor de um responsável técnico que tem como principal função assegurar a qualidade das atividades desenvolvidas, bem como a manutenção dos requisitos de segurança e desempenho dos Dispositivos Médicos.

Está dividido em 18 capítulos com um total de 20 anexos, em que os mais relevantes para a este trabalho são os anexos de I a IX [17].

Depois de identificadas as Diretivas, deve verificar-se se o produto está de acordo com a definição de dispositivo médico, de acordo com o Artigo nº 3 do Decreto-Lei 145 de 2009 ou com o Artigo nº 1 da Diretiva 93/42/CEE. É necessário verificar se o dispositivo está abrangido pelas Diretivas 90/385/CEE e 98/79/CE. Cumpridas estas tarefas, conclui-se que a Diretiva 93/42/CEE é aplicável e pode avançar para a segunda fase.

2.2.2 Requisitos específicos do produto

Este segundo passo é de extrema relevância para o processo da marcação CE, pois para a obtenção da marcação os dispositivos médicos têm de cumprir todos os requisitos aplicáveis, que se encontram no Anexo A.1, sendo estes baseados no Anexo I do Decreto-Lei 145 de 2009 e fornecidos pelo INFARMED para os dispositivos médicos. Estes requisitos destinam-se a proporcionar um bom nível de segurança aos dispositivos médicos.

No entanto, o fabricante tem de estar atento a outras Diretivas, pois existem casos onde se aplica mais do que uma diretiva.

Os requisitos têm como principal objetivo definir os resultados a atingir. Os fabricantes, para os alcançarem, terão de recorrer a soluções técnicas que não são especificadas pela diretiva [17]. Esta flexibilidade tem como finalidade permitir que os fabricantes escolham o método mais recente e que melhor se adequa à obtenção da conformidade.

Os dispositivos devem ser produzidos de tal modo que, quando usados em condições normais, eles cumpram o seu objetivo e que não coloquem em risco os seus utilizadores. As soluções adoptadas pelo fabricante na concepção devem respeitar os requisitos juntamente com o estado da arte.

Aquando da elaboração dos requisitos, se se identificar que o risco é elevado, o

fabricante deve aplicar os seguintes princípios pela ordem indicada:

- *Identificar os perigos conhecidos ou previsíveis e estimar o risco associado;*
- *Eliminar os riscos na medida do razoável através de uma concepção segura;*
- *Reduzir tanto quanto possível os riscos e tomar medidas de protecção, por exemplo alarmes;*
- *Informar os utilizadores dos riscos associados* [24].

2.2.3 Organismo Notificado

O Organismo Notificado (ON) é uma entidade ligada ao Estado-Membro que tem como função efetuar a avaliação da conformidade de dispositivos médicos com o objetivo da marcação CE. O Organismo Notificado é responsável por:

- Efetuar os procedimentos de avaliação da comformidade dos dispositivos médicos, no quadro da legislação nacional e comunitária;
- Autorizar a aposição da marcação CE dos dispositivos médicos;
- Emitir os certificados CE de conformidade dos dispositivos médicos;
- Assegurar que o fabricante cumpre corretamente com as obrigações decorrentes do sistema de qualiade aprovado.

Segundo o Decreto-Lei nº 145/2009, a definição de Organismo Notificado é: *o organismo designado para avaliar e verificar a conformidade dos dispositivos com os requisitos exigidos no presente decreto-lei, bem como aprovar, emitir e manter os certificados de conformidade.*

No Artigo 22.º do Decreto-Lei nº 145/2009 são designados os deveres do Organismo Notificado, que passam por analisar a documentação da concepção a fim de garantir que o fabricante do dispositivo médico está a cumprir todas as disposições aplicáveis. Esta análise deve ser tão mais cuidadosa quanto maior for a classe de risco do dispositivo[17].

Depois da seleção deste organismo para a avaliação de conformidade, deve ser enviada toda a documentação que é referida no Decreto-Lei nº 145/2009.

O Organismo Notificado avaliará toda a documentação enviada, fará uma auditoria às instalações do fabricante, ensairá o produto e, por fim, elaborará um relatório

da avaliação. Caso o parecer seja positivo, será emitido um certificado CE de conformidade, que tem um acompanhamento anual pelo Organismo Notificado. Após a realização da auditoria e caso sejam detetadas não conformidades críticas, o ON aguarda pela sua resolução e posteriormente emitirá o certificado CE de conformidade.

2.2.4 Avaliação da conformidade

Os dispositivos médicos são abrangidos pelo diretiva 93/42/CEE, na sua atual redação, transposta para o direito interno pelo Decreto-Lei nº 145/2009 de 17 de Junho. Para a avaliação da conformidade o fabricante pode escolher um dos procedimentos de avaliação previstos no Artigo 8º e descritos nos anexos II a VIII do Decreto-Lei nº 145/2009 de 17 de Junho.

Para a marcação de dispositivos de classe I, a aposição da marcação CE é da total responsabilidade do fabricante, sendo este obrigado a elaborar uma declaração de conformidade, notificar a autoridade competente, e sujeitar-se a fiscalização por parte da referida autoridade.

Para os dispositivos de classes IIa, IIb e III o fabricante deve escolher o organismo notificado para a intervenção, que é obrigatória, ao qual deve ser dirigido um pedido de avaliação da conformidade. O organismo, perante a avaliação, emite um certificado de conformidade.

De acordo com o Decreto-Lei nº 145/2009, os fabricantes de dispositivos médicos de classe I devem proceder de acordo com o Anexo VII - *Declaração CE de conformidade*, como descrito na alínea d) do Artigo 8º. No Anexo VII são descritas as obrigações do fabricante ou do mandatário, que passam por assegurar e declarar que os produtos em questão satisfazem as disposições do Decreto-Lei nº 145/2009 que lhes são aplicáveis. O procedimento de avaliação descrito no Anexo VII-*Declaração CE de Conformidade* pode ser conjugado com um dos procedimentos de avaliação de conformidade descritos no anexo V-*Garantia da Qualidade da Produção* ou VI-*Garantia da Qualidade dos Produtos*, tendo em conta a natureza do dispositivo médico, com função de medição ou estéril [17].

O fabricante deve elaborar a documentação técnica sobre a qual será feita a avaliação da conformidade do produto com as exigências do Decreto-Lei nº 145/2009, designadamente: uma descrição geral do produto; desenhos de concepção e descrição dos métodos de fabrico; resultados da análise de risco, bem como uma lista de normas harmonizadas cujas referências tenham sido publicadas no Jornal Oficial da União

Europeia; e os resultados dos cálculos da concepção, e das inspeções efetuadas, entre outros.

2.2.5 Documentação técnica

A documentação técnica deve ser elaborada pelo fabricante do Dispositivo Médico e tem como finalidade demonstrar a conformidade dos dispositivos médicos com os requisitos essenciais que lhes são aplicáveis.

A descrição dos requisitos essenciais encontra-se no Anexo I do Decreto-Lei 145/2009, que diz o seguinte: *Os dispositivos devem ser concebidos e fabricados por forma que a sua utilização não comprometa o estado clínico nem a segurança dos doentes, nem, ainda, a segurança e a saúde dos utilizadores ou, eventualmente, de terceiros, quando sejam utilizados nas condições e para os fins previstos, considerando-se que os eventuais riscos associados à utilização a que se destinam constituem riscos aceitáveis quando comparados com o benefício proporcionado aos doentes e são compatíveis com um elevado grau de proteção da saúde e da segurança.*

Para dar cumprimento aos requisitos essenciais foi utilizada uma tabela disponibilizada pelo INFARMED, que se enquadra com as exigências do Decreto-Lei 145/2009 e que pode ser consultada no Anexo A.1.

Para além dos requisitos essenciais, o requerente, depois de escolher um procedimento de avaliação de conformidade previsto na diretiva, deve preencher o modelo de *Requerimento para Avaliação da Conformidade*, juntamente com toda a documentação técnico científica necessária para a avaliação da conformidade. O fabricante deve manter cópias da documentação por um período de 5 anos.

2.2.6 Aposição da Marcação CE e declaração de conformidade

A última fase da marcação CE é a colocação no mercado do produto [17]. Para esta fase ser bem sucedida, todos os processos anteriores têm de ser cumpridos com sucesso. Imediatamente antes da colocação no mercado ocorre a aposição e declaração de conformidade.

A Declaração de Conformidade é o documento que o fabricante apresenta perante o Organismo Notificado, no qual onde declara que mantém um sistema de qualidade adequado para a produção de dispositivos médicos. Garante ainda que os dispositivos médicos estão em conformidade com os requisitos essenciais presentes

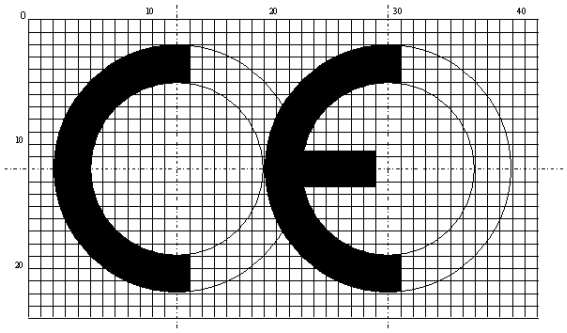


Fig. 2.3: Marca CE [1]

na diretiva que lhe é aplicável.

Neste documento, como se pode ver no Anexo A.2, têm de constar algumas informações do fabricante, juntamente com informações referentes aos produtos, tais como classe do produto e normas aplicadas no processo de certificação.

Para a aposição da marcação CE num dispositivo médico, Figura 2.3, é necessário que esteja em conformidade com os requisitos essenciais. Após esta fase e se todo o processo está conforme, o Organismo Notificado atribui a marcação CE ao dispositivo.

De forma a resumir este Capítulo, pode ver-se no Anexo A.9 um fluxograma dos procedimentos de avaliação de conformidade para marcação CE de todas as classes de dispositivos médicos, previstos na Diretiva 93/42/CE, o qual pode ser consultado no anexo 8 do Guia Nova Abordagem [1].

2.2.7 Qualidade em Saúde

Depois de analisar os requisitos do Decreto-Lei 145/2009 conclui-se que, para a aposição de marcação CE, os dispositivos médicos de classe I devem estar de acordo com a conjugação dos anexos V,VI e VII. Tal conjugação leva à implementação de um sistema de qualidade.

Os sistemas da qualidade em saúde são implementados normalmente pelas normas NP EN ISO 9001:2008 ou EN ISO 13485:2003 [25, 26]. Esta seção tem como finalidade dar uma visão geral da normas focando o sistema de concepção da NP EN ISO 9001:2008.

A qualidade é definida pela NP EN ISO 9000:2005 como sendo *"grau de satisfação de requisitos dado por um conjunto de caraterísticas intrínsecas"* [27].

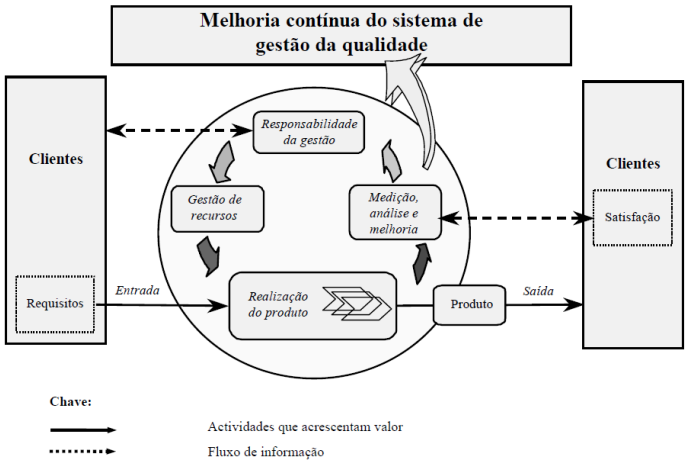


Fig. 2.4: Esquema do modelo da gestão da qualidade baseado em processos [27].

NP EN ISO 9001:2008

Com a implementação desta norma as organizações definem um sistema de qualidade em que têm de mostrar aptidão para proporcionar produtos que vão ao encontro dos requisitos do cliente e regulamentações aplicáveis. Implementa ainda uma visão focada no cliente, incluindo processos para uma melhoria contínua do sistema.

Esta norma internacional implementa uma abordagem por processos. Uma das vantagem desta abordagem *"é o controlo passo-a-passo que proporciona sobre a interligação dos processos individuais dentro do sistema de processos, bem como sobre a sua combinação e interação"* [27].

Pode ver-se na Figura 2.4 um modelo de um sistema de gestão da qualidade baseado em processos.

Um dos processos do sistema da qualidade mais relevantes para este trabalho é o processo de concepção, que pode ser consultado no Anexo A.6. Esse processo é apresentado na cláusula 7.3 da norma ISO 9001:2008, onde são descritos os requisitos.

O processo está dividido em 4 fases Especificação para o projeto, Conceção Inicial, 1º Fornecimento e Lançamento, sendo também descritas as entradas e quais as saídas.

Este processo é referido porque é a base de toda a conceção de qualquer produto de uma empresa certificada pelo norma 9001:2008.

EN ISO 13485:2003

A norma ISO 13485:2003 tem como finalidade especificar os requisitos para o sistema da gestão da qualidade nas áreas de concepção e desenvolvimento, produção, instalação e assistência técnica de dispositivos médicos [28].

Auxilia na harmonização da regulamentação mundial de dispositivos médicos. Tem como base a norma ISO 9001, com algumas modificações, e requisitos específicos para dispositivos médicos.

Capítulo 3

Segurança em Software

O problema da segurança informática surgiu muito antes da expansão da internet [29, 30]. O estudo da segurança informática foi crescendo e foram surgindo conceitos e mecanismos basilares, tais como princípios do projeto de sistemas seguros, controlo de acesso, segurança multinível, modelos de segurança, núcleos de segurança, entre outros.

Com a grande expansão da internet, a segurança de computadores e de redes torna-se indispensável [29].

As principais razões para a insegurança na internet devem-se a um número enorme de potenciais vítimas que ficou exposta na rede à invisibilidade e ao anonimato que a internet proporciona aos atacantes. Para colmatar esta exposição dos utilizadores a possíveis, ataques surgiram mecanismos que permitem aumentar a segurança tais como: comunicação segura, *firewalls*, detetores de intrusão e chaves criptográficas.

Hoje sabe-se que grande parte dos problemas de segurança existente no software estão relacionados com a vulnerabilidade do software, isto é, com erros de projecto que o deixam sujeito ao ataque de piratas informáticos [29, 31].

A segurança é baseada fundamentalmente em três conceitos conhecidos como *AIC triad*, como pode ver-se na Figura 3.1 [32].

- **Confidencialidade** é caraterizada como a ausência da divulgação não autorizada de informação [33, 32]. Sempre que há uma libertação não intencional de informação o sigilo é perdido.

- **Integridade** significa que os dados não são modificados ou alterados sem autorização prévia [29]. A integridade deve também impedir a alteração dos

Fig. 3.1: AIC Triad

dados durante o armazenamento ou quando são transmitidos pela rede [32].

- **Disponibilidade** está relacionada com o acesso confiável e em tempo útil aos dados e recursos que se tem autorização para usar. Um exemplo de perda de disponibilidade é um ataque DoS, que não dá acesso ao criminoso mas impede a utilização normal do sistema [32].

A avaliação de risco é um processo de extrema importância para as organizações, permitindo identificar e dar prioridade a riscos inerentes ao negócio. Esta avaliação vai permitir projetar uma boa política de segurança e procedimentos para defender os pontos fracos da empresa, protegendo assim os seus ativos [32].

A identificação de risco tem como objetivo reduzir o risco a que a organização está sujeita. Mas esta diminuição terá um custo que tem de ser medido e não faz sentido gastar-se milhares de euros a proteger um computador pessoal, no entanto será lógico proteger, ao mais alto nível, um software onde as falhas de segurança levam a perda de utilizadores e consequentemente de dinheiro [29].

A gestão de risco tem como finalidade avaliar as ameaças que uma organização enfrenta. Tem de ser capaz de identificar e analisar as vulnerabilidades para saber como lidar com o risco. Alguns dos processos mais importantes da gestão de risco passam por nomear uma equipa de gestão de risco, identificar as vulnerabilidades e determinar medidas para colmatar os riscos encontrados [32]. Os conceitos de ameaça, vulnerabilidade e controlo são importantes para se efetuar uma boa análise de risco.

- **Ameaça** é um acontecimento natural ou induzido que poderá ter algum tipo de impacto na organização.

- **Vulnerabilidade** é um defeito do sistema relevante para efeitos de segurança, que pode ser explorada por um atacante para subverter a política de segurança. Existem vários tipos de vulnerabilidades de projeto, de codificação e operacional.

- **Controlos** são mecanismos para regular ou reduzir as vulnerabilidades.

3.1 Segurança de Aplicações WEB

A *World Wide Web* (WWW) surgiu por volta dos anos 90 no CERN, na Suíça, e desde então aumentou exponencialmente tanto ao nível de aplicações como vulnerabilidades [34, 35].

A internet é um sistema cliente-servidor, no qual os servidores contêm dados multimédia que podem ser acedidos através do *browser*. O sistema evoluiu com o passar dos anos, passando de uma simples representação de HTML para aquilo que hoje em dia se chama de aplicações *web*. Estas aplicações recorrem a diversas tecnologias que oferecem um comportamento altamente dinâmico.

Do lado do cliente é usado um *browser*, como por exemplo o *Mozilla Firefox*, e do lado do servidor é usado um servidor *web*, como por exemplo o *Apache*. Do lado do Cliente, as tecnologias presentes são o HTML o *JavaScript*, *Ajax*, entre outras, enquanto que no lado do servidor temos o PHP, JSP, entre outras, ver Figura 3.2.

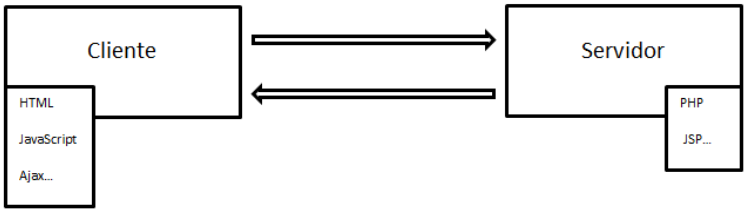


Fig. 3.2: Arquitetura *web* [29].

Com a conjugação de inúmeras tecnologias aumenta a probabilidade de vulnerabilidades. Para tentar diminuir essas falhas é importante conhecer minimamente as mais perigosas e mais usadas nos dias de hoje. Em seguida apresentam-se um resumo das 10 principais vulnerabilidades e uma breve explicação de cada uma delas.

A *Open Web Application Security Project* (OWASP) é uma organização que visa melhorar a segurança do software. Tem vindo a acompanhar a evolução das vulnerabilidades ao longo do tempo e publica periodicamente a sua visão sobre o assunto [36]. Existem outras organizações que também fazem a avaliação dessas

vulnerabilidades tais como a *Web Application Security Consortium* (WASC), no entanto é apresentada a metodologia da OWASP, mais propriemente a OWASP Top 10 [37].

Relativamente às vulnerabilidades que constam nesta lista, foram tidos em conta o nível de ameaça, grau de vulnerabilidade, impacto e deteção. Os níveis de ameaça são medidos de acordo com a Tabela 3.1.

Tab. 3.1: Escala usada no Top 10 das vulnerabilidades[37].

Fatores	Escala
Dificuldade de ataque	Fácil, Médio, Difícil
Grau de vulnerabilidade	Bastante comum, comum, incomum
Detectabilidade da vulnerabilidade	Fácil, Média, Difícil
Impacto técnico	Severo, Moderado, Menor

O Top 10 é composto pelas seguintes vulnerabilidades:

1. Injeção SQL;
2. *Cross Site Scripting (XSS)*;
3. Autenticação e gestão de secções;
4. Referência direta a objetos;
5. *Cross Site Request Forgery (CSRF)*;
6. Configuração insegura;
7. Armazenamento criptográfico inseguro;
8. Falha na restrição de acesso a URL‘s;
9. Comunicação insegura;
10. Redireccionamentos não validados.

Para cada uma das vulnerabilidades apresentadas será apresentada uma explicação e como previnir.

Injeção SQL

A injeção pode ser de diversos tipos como SQL, XML, HTML ou mesmo comando do sistema operativo. As injecções de pedaços de código podem ser entendidas pelo interpretador e dar acesso a informação confidencial a atacantes, sendo a mais perigosa a própria injeção de SQL [37, 29].

A prevenção da injeção passa por prevenir que comandos ou *Queries*[1] possam ser contaminados com dados não confiáveis [29]. Para obter essa proteção devem ser usadas *Application Programming Interface* (APIs) seguras que possam evitar que o código seja contaminado com dados não confiáveis.

Uma boa prática para a proteção contra ataques deste tipo é codificar os carateres especiais, metacarateres e para ir mais longe pode-se criar uma lista de carateres confiáveis [37].

Cross Site Scripting (XSS)

O *Cross Site Scripting* é um ataque muito perigoso e bastante comum, que permite ao atacante executar um *script* no *browser* da vítima, podendo assim copiar dados da secção ou redirecionar a vítima para um site malicioso.

Este tipo de ataque pode ser prevenido com a validação do *input* e codificação de *output*. Uma boa prática para prevenir este ataque passa também pela codificação de carateres usados [37].

Autenticação e gestão de secções

Este tipo de ataque prende-se com o problema de não ser possível manter um sessão ativa entre o servidor e o cliente. Deve-se ao facto do protocolo HTML não manter o estado, pois é *stateless*, em que o servidor não relaciona os pedidos efetuados pelo utilizador, abrindo assim possibilidades ao atacante.

Para prevenir este tipo de ataque, a organização deve adaptar um conjunto de boas práticas que podem ser:

- Utilização de HTTPS nas comunicações entre o servidor e o cliente.
- Definir um número máximo de tentativas de autenticação.
- As credencias devem respeitar um formato que deve ser o mais complexo possível.

[1] Linguagem para pesquisa em base de dados

- Deve ser exigida re-autenticação antes de serem efetuadas operações que possam por em causa o bom funcionamento do sistema.
- As credencias devem expirar ao fim de um período de tempo prédefinido.
- O ficheiro de registo de eventos deve incluir a autenticação.
- As passwords devem ser encriptadas.
- A sessão deve ser terminada quando o utilizador faz logout.
- A sessão deve expirar após um período de inatividade.

Referência direta a objetos

A vulnerabilidade encontra-se quando uma aplicação *web* expõe objetos que serão usados internamente. Isto acontece quando se expõe referências diretas via URL, ou no próprio código HTML, como por exemplo passar um variável por URL que será utilizada numa pesquisa à base de dados.

No caso de ser necessário fazer uma referência direta a um objeto, essa informação deve ser encriptada e deve ser verificado se o utilizador pode aceder à informação pretendida.

Cross Site Request Forgery (CSRF)

Este tipo de vulnerabilidade está presente em aplicações *web* que autenticam o utilizador com base em credenciais estáticas e persistentes, por exemplo o *cookie*.

Esta vulnerabilidade pode ser contornada de duas formas a partir da criação de um terceiro campo que não é guardado junto do *cookie*, como um número aleatório; usando a re-autenticação aquando de ações mais críticas.

Configuração insegura

Uma boa segurança implica uma configuração segura de todos os componentes que contribuem para a aplicação, como por exemplo o servidor *web*, sistema de base de dados, sistema operativo, entre outros.

A prevenção passo por boas práticas tais como a criação de um guia para a correta manutenção de todos os sistemas que estão relacionados com a aplicação *web*.

Armazenamento criptográfico inseguro

As aplicação *web*, ao manipularem informação sensível, devem ter como suporte um sistema que permita a correta encriptação dessa informação, protegendo-a, pelo menos contra leitura ou alteração por utilizadores não autorizados.

Há algoritmos que mantêm a confidencialidade, por exemplo RSA[2], e integridade, como por exemplo SHA e MD5, que podem ser usados para prevenir este tipo de vulnerabilidade.

Falha na restrição de acesso a URL

Em aplicações *web* existem páginas que só podem ser visualizadas por quem está autenticado, e dentro destas, há ainda uma distinção de perfis de utilizadores, pois nem todos podem ter acesso a tudo. É portando necessário estarem protegidas de acordo com a informação que guardam.

As aplicações *web* normalmente falham em páginas como:

- Administração da aplicação.
- Ficheiros de dados XML.
- Ficheiros temporários.
- *Backup* e *logs*.
- Ficheiros de configuração [29].

A melhor prática para evitar este tipo de vulnerabilidade passa por colocar em todas as páginas um mecanismo de controlo de, acesso. Deve ainda ser definida um política de controlo de acesso.

Comunicação insegura

A comunicação entre um o cliente e o servidor deve ser feita através da utilização do protocolo HTTPS. Mesmo com a ausência de vulnerabilidades, é possível a um atacante capturar as credenciais de um utilizador [29].

Uma aplicação *web* pode utilizar o protocolo HTTPS na autenticação e posteriormente trocar dados com o servidor, com o protocolo HTTP. Após autenticação, e

[2] Algoritmo criptográfico de dados,que tem como nome as iniciais dos seus criadores,Adi Shamir e Leonard Adleman.

utilizando o protocolo HTTP, pode ser capturada informação confidencial do utilizador.

De modo a prevenir esta vulnerabilidade deve usar-se em toda e qualquer comunicação com o servidor o protocolo HTTPS.

Redirecionamentos não validados

O redirecionamento entre página, é comum neste tipo aplicações, o que por si só não representa um vulnerabilidade. No entanto é comum a passagem de parâmetros de *input* que podem ser manipulados pelo utilizador.

A solução mais simples é evitar redirecionamento entre páginas. No caso de ser estritamente necessário, os parâmetros devem estar encriptados para que não seja percetível ao utilizador. É vital que os parâmetros sejam validados antes de serem processados.

Na Tabela 3.2 encontram-se as classificações de cada vulnerabilidade, admitindo os fatores da Tabela 3.1.

Tab. 3.2: Classificação do Top 10 do OWASP [29].

Vulnerabilidades	Ataque	Grau	Deteção	Impacto
Injeção SQL	Fácil	Comum	Média	Severo
XSS	Média	Muito Comum	Fácil	Moderado
Autenticação e gestão de seções	Média	Comum	Média	Severo
Referência direta a objetos	Fácil	Comum	Fácil	Moderado
CSRF	Média	Muito Comum	Fácil	Moderado
Configuração insegura	Fácil	Comum	Fácil	Moderado
Armazenamento criptográfico inseguro	Difícil	Incomum	Difícil	Severo
Falha na restrição de acesso a URL‘s	Fácil	Incomum	Média	Moderado
Comunicação insegura	Difícil	Comum	Fácil	Moderado
Redirecionamento não validados	Média	Incomum	Fácil	Moderado

Das vulnerabilidades apresentadas, aquela que pela sua posição e impacto na lista merece mais atenção é a injeção de SQL.

3.2 Protocolos e Normas de Segurança em Saúde

Neta secção são apresentadas duas das normas mais relevantes no âmbito hospitalar, DICOM e HL7, focando os pontos de segurança que elas recomendam para uma utilização segura dos dados de saúde.

3.2.1 DICOM

O protocolo DICOM foi concebido por uma comissão formada pela *Americam College of Radiology* (ACR) e a *National Electrical Manufacturers Association* (NEMA) e foi desenvolvido com a finalidade de tornar a imagiologia médica independente de dispositivos desenvolvidos por fabricantes particulares [38, 13].

Este protocolo estabelece um conjunto de regras que faz com que sejam trocadas informações médicas entre equipamentos de imagiologia médica de marcas diferentes e providencia todas as ferramentas necessárias para a correta representação e processamento de dados provenientes da imagiologia. Regula a transferência, armazenamento e exibição de dados relacionados com a imagem médica. Estes procedimentos encontram-se divididos por 20 capítulos que hoje formam o protocolo e que estão em constante evolução [13].

A implementação do protocolo DICOM pelos fabricantes de equipamentos e entidades hospitalares abriu uma nova perspectiva sobre a qualidade dos serviços, aumentando a rapidez de reposta e a segurança [39].

O DICOM diferencia-se de outros protocolos de imagens por apresentar a informação de forma estruturada, isto é, armazena a imagem médica juntamente com informações relativas ao paciente, que são armazenadas com etiquetas, denominadas de tags, que indicam e delimitam as informações. Esta forma de guardar os dados permite uma leitura coerente e íntegra da informação dos pacientes [13].

O protocolo DICOM especifica um conjunto de boas práticas referentes a perfis para a gestão de sistemas e segurança na *Part 15: Security and System Management Profiles* [40],que podem ser resumidas em:

- Aplicação da assinatura digital;
- Técnicas para comunicação segura;
- Segurança na troca de dados [40, 39].

Assinatura digital

A assinatura digital é baseada em técnicas tais como funções de Hash ou chaves públicas [41, 42, 39].

O protocolo DICOM suporta algumas funções *Hash* como o Secure Hash Algorithm (SHA) e *Message Digest 5* (MD5) [40], sendo estes algoritmos considerados seguros por ser praticamente impossível em tempo útil obter-se o mesmo conjunto de bits com duas palavras diferentes.

O MD5 é um algoritmo unidireccional de 128 bits que foi desenvolvido em 1991 por Ronald Rivest. O princípio dos algoritmos unidireccionais é depois de transformar um texto não haver forma de voltar a ter o texto original [43].

No entanto, há um ponto fraco, que é a possibilidade de ser gerado um *hash* idêntico para valores diferentes [39].

O MD5 é também útil para verificar a integridade de um ficheiro, recorrendo a programas próprios, em que é criado um *hash* do ficheiro original, que depois é comparado com o *hash* após o download.

O SHA é também um algoritmo unidireccional. É usado em protolos de segurança como TLS, SSL, IPSec, entre outros. O SHA-2, variante mais atual, tem uma capacidade de saída superior às anteriores, enquanto que o SHA-0 e SHA-1 podem usar desde 224 bits até 512 bits [41].

As chaves públicas são um método de criptografia que usa dois tipos de chaves: a pública, que é cedida, e a chave privada, que deve ser guardada em segurança pelo utilizador.

Este tipo de algoritmo é mais usado em contestos de rquisitos elevados de autenticidade e confidencialidade. O seu método de funcionamento é simples. Depois de cifrar uma mensagem com a chave pública, esta só pode ser descodificada com a chave privada, sendo o contrário também válido.

O protocolo DICOM recomenda o algoritmo RSA, o qual deve o seu nome aos três inventores (Rivest, Shamir, Adleman), atualmente ainda considerado um dos algoritmos mais seguros.

Comunicação segura

O Transport Layer Security (TLS) é um protoloco criptográfico que fornece segurança em comunicações na Internet. Possibilita que aplicações cliente servidor possam comunicar de forma a garantir que os dados não são alterados nem escutados na rede.

O TLS inicia a comunicação pela troca de certificados. Posteriormente existe uma troca de chaves assimétricas (chave pública e chave privada) e inicia-se a troca de dados.

O protocolo DICOM sugere alguns requisitos mínimos para as comunicações segundo o protocolo TLS, como se pode ver na Tabela 3.3.

Tab. 3.3: Mecanismos mínimos para TLS [40].

Índice	Gravidade
Autenticação	*RSA based certificates*
Exchange of Master Secrets	RSA
Integridade dos Dados	SHA
Privacidade	*Triple DES*, AES

Armazenamento do ficheiro DICOM

Para o armazenamento de um ficheiro DICOM deve ser garantida a integridade e a confidencialidade.

A criptografia dos ficheiros DICOM é recomendada pelo protocolo DICOM na parte 15, através dos algoritmos AES ou *Triple-DES*.

O Triple-DES é um algoritmo de codificação simétrica com uma chave de 192 bits, considerado seguro. Os dados codificados podem ser fornecidos com assinaturas digitais como o RSA [40, 41].

3.2.2 HL7

A *Health Level Seven* (HL7) é uma organização que tem como objetivo produzir normas, na área da saúde, para troca, integração, partilha e recuperação de informação eletrónica, assim como na prática médica e administrativa [44].

O termo Level Seven vem do nível mais elevado do modelo de comunicação OSI (Open Systems Interconnection), a camada de aplicação [45].

O objetivo da HL7 é normalizar a troca de informação entre sistemas hospitalares através do uso de uma linguagem própria, que pode ser encontrada atualmente em duas versões, V2.x ou V3.

Esta norma especifica algumas boas práticas e aconselha o uso de mecanismos de segurança disponíveis [44].

3.2.3 Técnicas de segurança - ISO 17799

A norma ISO 17799 *Information technology - Security techniques - Code of practice for information security management* é um "standard" orientado para a gestão de segurança da informação, definido informação como um ativo que pode existir em diversas formas e que tem valor para a organização. A segurança da informação tem como objetivo a implementação de um sistema que permite proteger os ativos da organização, a fim de garantir a continuidade do negócio [46].

De acordo com esta norma, a segurança da informação é caraterizada pela preservação da confidencialidade, integridade e disponibilidade. De modo a garantirem-se estas caraterísticas, é necessário implementarem-se processos de controlo que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de software.

Os requisitos de segurança, segundo a mesma norma, são definidos pela organização e devem ser baseados em três fontes principais [33]:

1. Avaliar os ativos da organização.
2. Avaliar a legislação vigente e estatutos.
3. Desenvolver um conjunto de princípios, objetivos e requisitos para apoiar as operações da organização [33].

Os controlos essenciais para uma organização são:

- Proteção de dados e privacidade de informação pessoal.
- Salvaguarda de registos organizacionais.
- Gestão de propriedade intelectual [33].

Os controlos relacionados com as melhores práticas para a segurança de informação são:

- Documento da política de segurança da informação.
- Definição das responsabilidades na segurança da informação.
- Educação e treino em segurança da informação.
- Relatório dos incidentes de segurança.

- Continuidade de negócio [33].

Os controlos devem ser adequados de acordo com as capacidades da organização e um que deve ser referido é o método de autenticação apropriado para utilizadores que tenham acesso remoto.

Para a autenticação de utilizadores remotos deve ser usada uma técnica baseada em criptografia, como por exemplo uma *Virtual Private Network* (VPN) [33].

Em teleradiologia é comum usar-se esta técnica para proteção de dados [47]. A *Virtual Private Network* consiste em estabelecer uma ligação encriptada sobre uma infraesstrutura pública, a Internet. Este protocolo pode garantir que a comunicação é feita de uma forma segura, pois oferece grande confiabilidade, integridade e disponibilidade [48].

Os processos para a implementação da norma ISO 17799 são apresentados na Figura 3.3 e descritos posteriormente [33].

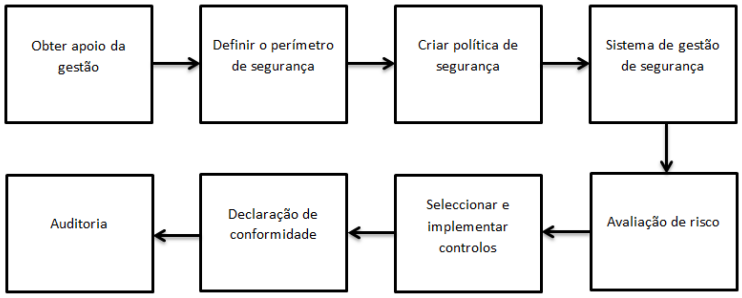


Fig. 3.3: Arquitetura *web* [46].

Obter apoio da Gestão

Para o sucesso da implementação da ISO 17799 é necessário obter o apoio da gestão, a qual deverá incutir na organização a noção que um sistema de segurança que deve partir do topo.

Definir domínio de segurança

A organização deve definir o domínio de segurança, sendo esta uma tarefa difícil. Esse domínio pode não abranger toda a organização, mas deve estar sobre total controlo.

Criar política de segurança

A política de segurança tem como objetivo fornecer à gestão uma orientação e apoio na segurança da informação.

Possuir sistema de gestão da segurança da informação

Para um sistema de gestão de segurança, deve implementar, gerir, manter e executar o processo de segurança da informação.

Efetuar periodicamente a avaliação de risco

Devem ser identificadas as vulnerabilidades a que os ativos da organização estão expostos e calcular o risco proporcional. Os controlos devem ser implementados para minimizar os riscos para um nível aceitável. Este assunto será abordado com mais detalhe na seção Gestão de Risco 3.4.

Seleccionar e implementar controlos

A seleção dos controlos é feita de acordo com a disponibilidade de aceitação do risco por parte da gestão, no qual se deve dar atenção ao valor do risco.

Elaborar declaração de Aplicabilidade

Esta declaração deve documentar os riscos identificados na avaliação de risco.

Efetuar auditorias

A auditoria permite fazer uma revisão das infra-estrutura de segurança.

3.3 Proteção de Dados

No decorrer do estudo do processo de marcação CE constatou-se que é necessário o parecer da autoridade que regula o tratamento de dados.

A Comissão Nacional de Proteção de Dados Pessoais (CNPD) é a autoridade, em Portugal, que controla e fiscaliza o processamento de dados pessoais. Tem como orientação a Lei da Proteção de Dados Pessoais, que transpõe para a ordem jurídica Portuguesa a diretiva 95/48/CE, cujo princípio é a transparência no processamento de dados pessoais.

Segundo a Lei número 67/98 de 26 de Outubro, os dados pessoais são: *"qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;"* [49].

Para que conste, a presente lei define tratamento de dados pessoais como: *"qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;"* [49].

Na Lei da Proteção de Dados Pessoais, no Artigo 7, pode ler-se que é proibido tratar dados relativos à saúde. O tratamento dos dados de saúde só pode ser efectuado se a Comissão Nacional de Proteção de Dados Pessoais der uma autorização prévia. No entanto é necessário que sejam garantidas medidas adequadas de segurança da informação [49, 50].

A Lei nº 67/98 na secção III "segurança e confidencialidade do tratamento", define as medidas às quais o processo deve obedecer. No Artigo nº 14 - "Segurança do tratamento" é dito que o responsável deve por em prática medidas de segurança para proteger os dados de destruição, alteração e difusão. Realça-se o facto da difusão quando os dados são transmitidos em rede. O responsável deve implementar um nível de segurança adequado para a natureza dos dados que se estão a proteger.

No Artigo nº 15 - "Medidas especiais de segurança" são expostas as medidas a tomar no tratamento, tais como:

- Impedimento da entrada a pessoas não autorizadas às instalações utilizadas para o tratamento;
- Controlo de suportes de dados, de forma a impedir que sejam lidos, alterados ou copiados;
- Controlo de inserção;
- Controlo de utilização;

- Controlo de acesso;
- Controlo da transmissão;
- Controlo de introdução, quem e quando introduziu os dados;
- Controlo de transporte para impedir que os dados sejam lidos, copiados, alterados ou eliminados. [49, 50]

No mesmo artigo, no ponto 3, é referido que os sistemas devem garantir a separação lógica dos dados sensíveis tais como dados de saúde, dos restantes dados. É dito que se a CNPD, assim o entender, a circulação dos dados em rede deverá ser cifrada.

Relativamente a este tema, foi também estudada a Lei nº 12/2005 de 26 de Janeiro, "Informação genética pessoal e informação de saúde". No entanto não se inclui neste documento por não acrescentar nada de relevante para este trabalho [51].

3.4 Gestão de Risco

Os dispositivos médicos devem ser concebidos de forma a desempenharem as suas funções em completa segurança e sem comprometer a saúde dos utilizadores. Um bom conhecimento dos riscos associados a um dispositivo médico, em todas as fases do seu ciclo de vida, aumenta a segurança para os seus utilizadores. A identificação dos perigos dos eventuais riscos e a tentativa de os eliminar constituem a gestão de risco.

No anexo I do Decreto-Lei 145 de 2009 encontram-se os requisitos essenciais que fazem referência à análise de risco, tornando-a numa obrigação regulamentar. No ponto 1.1 pode ler-se: *"os eventuais riscos apresentados constituem riscos aceitáveis se forem menores do que o benefício"*; o ponto 2.1 refere que é necessário *"eliminar ou reduzir os riscos ao mínimo possível"*; e, por fim no ponto 2.3, pode ler-se *"informar os utilizadores dos riscos residuais"* [17].

Pela consulta da literatura e da documentação disponibilizada no site do INFARMED, surgem aplicações das normas IEC 60812 *Analysis techniques for system reliability - Procedure for failure mode and effects analysis* (FMEA) e ISO 14971 *Medical devices - Application of risk management to medical devices* para a avaliação de risco de dispositivos médicos [52, 52, 53].

3.4.1 Gestão de risco em Dispositivos Médicos - ISO 14971:2007

A norma ISO 14971:2007 *Medical devices - Application of risk management to medical devices* especifica as linhas de orientação a fornecer aos fabricantes para que desenvolvam um processo de gestão de riscos associados à utilização de dispositivos médicos.

Esta norma é específica para riscos associados a dispositivos médicos e permite a identificação dos riscos, benefício/risco, implementação de medidas de correção e prevenção.

É aceitável dizer-se que o conceito de risco tem duas componentes:

- *Probabilidade de ocorrência do dano;*
- *Gravidade do dano;* [54]

Para melhor compreensão da aplicação é importante ter em conta algumas definições tais como:

- **Análise de Risco** - uso sistemático de informações disponíveis para identificar perigos e estimar o risco;
- **Dano** - lesões físicas ou prejuízos para a saúde de pessoas, para propriedade ou para o ambiente;
- **Perigo ou Ameaça** - potencial fonte de dano;
- **Risco** - combinação da probabilidade de ocorrência de dano e da gravidade desse dano;
- **Estimativa do risco** - processo utilizado para atribuir valores de probabilidades de ocorrência do dano e de relevância do dano;
- **Avaliação do risco** - processo de comparar o risco estimado com base em critérios de risco identificados para determinar a aceitabilidade do risco;
- **Controlo de risco** - processo no qual as definições são tomadas e as medidas implementadas para que os riscos sejam reduzidos ou mantidos dentro de níveis específicos e aceitáveis;
- **Risco residual** - risco remanescente após terem sido tomadas as medidas;

- **Segurança** - inexistência de risco para além do aceitável;
- **Gravidade** - Medida das possíveis consequências de um perigo;
- **Verificação** - confirmação, por exame e fornecimento de evidências objetivas, de que os requisitos especificados foram satisfeitos;
- **Ciclo de vida** - todas as fase da vida de um dispositivo médico, desde a concepção inicial até a eliminação.

A avaliação de risco é um processo que deve acompanhar o dispositivo médico durante o seu ciclo de vida e deve incluir análise, avaliação, controlo e produção de informação.

A norma encontra-se dividida em 6 passos principais, como se pode ver no esquema apresentado na Figura 3.4.

A Figura 3.4 resume a norma ISO 14791:2007, onde se encontram presentes todos os requisitos especificados na norma. Podemos ler, no anexo F da norma ISO 14791:2007, que os requisitos mínimos para a gestão de risco são os que se encontram no ponto 3.4 - *"Planeamento da gestão de risco"* sendo eles:

a) Âmbito das atividades de risco planeadas, identificação e descrição do dispositivo médico, incluindo as fases do ciclo de vida;

b) Atribuição de responsabilidades;

c) Requisitos para a revisão das atividades de gestão de risco;

d) Critérios para a aceitabilidade de riscos, com base na política do fabricante para determinar o risco aceitável;

e) Atividades de verificação;

f) Atividades relacionadas com a recolha de informação de produção e pós produção.

A identificação dos perigos associados ao produto pode ser encontrada nas respostas às questões que se encontram no anexo C da norma ou em respostas a questões colocadas a caraterísticas do dispositivo e métodos de concepção.

A norma ISO 14791:2007 propõe 2 parâmetros para a estimativa do risco, que são a probabilidade de ocorrência, ver Tabela 3.4, e o nível de gravidade, ver Tabela 3.5.

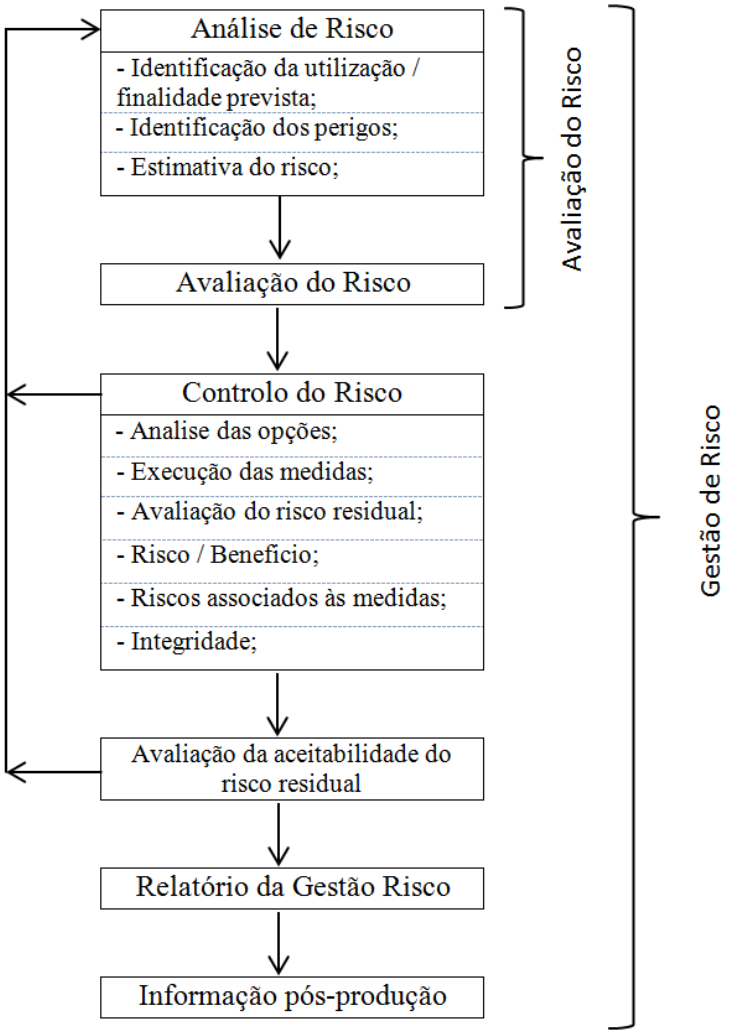


Fig. 3.4: Processo da Gestão de Risco [54].

Tab. 3.4: Probabilidade de ocorrência [54].

Índice	Ocorrência	Critério
1	Frequente	> 10^3
2	Provável	10^4 a 10^3
3	Ocasional	10^5 a 10^4
4	Remota	10^6 a 10^5
5	Improvável	<10^6

Tab. 3.5: Nível de gravidade [54].

Índice	Gravidade	Critério
1	Catastrófico	Morte do paciente
2	Crítico	Resulta na incapacidade permanente ou risco de vida
3	Grave	Resulta em lesão
4	Baixo	Resulta em lesão temmporária
5	Desprezível	Inconveniência ou desconforto temporário

Tab. 3.6: Cronograma que delimita o risco aceitável do não aceitável, pela conjugação do dano com a probabilidade.

Nível	Desprezível	Baixo	Grave	Crítico	Catastrófico
Improvável	X	X	X	X	X
Remota	X	X	X	X	X
Provável	X	X	X	X	X
Frequente	X	X	X	X	X

A aceitabilidade do risco, resultante da multiplicação dos factores das tabelas, será feita segundo dois critérios: risco aceitável e risco inaceitável confome sugerido na norma ISO 14792:2007, como se pode ver na Tabela 3.6.

Na Tabela 3.6 pode ver-se a verde o risco aceitável e a vermelho o inaceitável, o qual ser comparado com o resultado da conjugação da Tabela 3.4 e da Tabela 3.5.

3.4.2 *Failure Modes and Effect Analysis*

Segundo *Stamits*, o *Failure Modes and Effect Analysis* (FMEA) é uma técnica de engenharia usada para definir, identificar e eliminar falhas, problemas e erros conhecidos e/ou potenciais de sistemas, projectos, processos e/ou serviços antes que eles cheguem ao consumidor [55].

O FMEA é um método sistemático de identificação e prevenção de problemas de produto e processo antes da sua ocorrência. Os métodos do FMEA estão focados na prevenção de defeitos, aumento da segurança e, consequentemente, no aumento da satisfação do cliente. Idealmente o FMEA é iniciado no projeto do produto ou nos estágios de desenvolvimento do processo [56]. Usado tanto na conceção como em processos de fabricação, principal objetivo é reduzir substancialmente os custos através da identificação do problema numa fase inicial do processo de desenvolvimento, pois é nesta fase que fazer as mudanças tem um custo menor, e conseguindo-se assim aumentar a sua confiabilidade.

Tipos de FMEA

A classificação dos tipos de FMEA não é uniforme, e dependendo da fonte bibliográfica os tipos podem variar, mas o modo de realizar as etapas é equivalente [57].

Stamatis [55] classifica o FMEA em quatro tipos: FMEA do projeto, FMEA do processo, FMEA do sistema FMEA do serviço. O FMEA pode ser também dividido em dois, FMEA do produto e FMEA do processo, segundo *McDermott, et al.* [56].

FMEA de produto

O objetivo do FMEA do produto é descobrir antecipadamente possíveis falhas de segurança ou mau funcionamento do produto. Deve ser aplicado a cada fase no processo de concepção, sempre com a pergunta: "Como é que o produto pode falhar?" [56].

FMEA de processo

O FMEA do processo tem como objetivo descobrir os problemas relacionados com o fabrico do produto. É útil orientar a análise de um processo de FMEA para os principais elementos pessoas, materiais, equipamentos, métodos e meio ambiente, sempre com a pergunta: "Como é que a falha do processo pode afectar o produto, a eficiência do processo ou a segurança do operador e cliente?" [56].

Etapas de FMEA

Passos para o FMEA do Processo/Produto [56]:

1. Rever o processo do produto - Nesta fase deve estar presente um fluxograma de todo o processo para garantir que a equipa de trabalho entenda, de forma coerente, o processo de trabalho;

2. Possíveis modos de falha - Depois da compreensão do processo (ou produto), a equipa está pronta para começar a reflectir sobre os possíveis modos de falha;

3. Listar potenciais efeitos dos modos de falha - Identificar os efeitos para os possíveis modos de falha que podem variar. Uma pergunta para ajudar a completar este passo é: *Se a falha ocorrer, quais são as principais consequências?*;

4. Classificação de gravidade para cada efeito - É uma estimativa de quão grave podem ser os efeitos se uma determinada falha ocorrer. Podem obter-se mais informações na Tabela 3.7;

5. Ocorrência de cada falha - A melhor forma de determinar a ocorrência é a utilização de dados reais ou de produtos/processos similares, ver Tabela 3.8;

6. Deteção do modo de falha ou efeito - É preciso identificar os controlos atuais para deteção de falhas ou efeitos de falhas. Se não existirem controlos, a probabilidade de detecção será baixa, o que eleva a classificação da falha. Primeiramente devem-se listar todos os controlos dos modos de falha e posteriormente atribuir o ranking de deteção, ver Tabela 3.9;

7. Calcular o número de ocorrência para cada efeito - O *Risk Priority Number* (RPN) é calculado multiplicando a gravidade pela deteção e ocorrência;

8. Ordenar os modos de falha por ação - Depois de classificar os modos de falha é necessário atuar sobre eles, para tal ordena-se do maior para o menor e inicia-se o processo pelo que tem um RPN mais elevado. A organização deve decidir qual é o RPN aceitável e baixar os que se encontram acima desse nível, ver Tabela 3.10;

9. Acionar medidas para eliminar ou reduzir os riscos dos modos de falha - Recorrendo a um processo de resolução de problemas, é importante identificar e implementar ações de modo a eliminar ou a reduzir os modos de falha mais elevados;

10. Calcular o RPN - Por fim e depois de aplicados todos os métodos para resolução de falhas, deve ser calculado novamente o RPN. Deve ainda ser verificado se nos modos de falhas onde foram tomadas medidas existe uma redução significativa do RPN.

3.5 Licenciamento em Software

Existem essencialmente dois tipo de licenças de software, *Open Source* ou software proprietário, ambos geralmente regidos por direitos de autor. O *Open Source* é regido por um grade número de licenças, tais como *General Public License*, *Berkeley Software Distribution*, Apache, *Eclipse Public License*, entre outras, sendo estas a mais relevantes para este trabalho [60].

Tab. 3.7: Sistema de classificação da Gravidade [56, 58, 59].

Índice	Gravidade	Critério
1	Nenhum	Sem efeito perceptível
2	Muito Menor	Falha notada somente por clientes muito atentos (menos de um quarto)
3	Menor	Falha notada por parte dos clientes (50%)
4	Muito Baixo	Falha notada pela maioria dos clientes
5	Baixo	Produto operacional, mas com defeito ao nível do desempenho
6	Moderado	Produto operacional, mas com partes não funcionais
7	Alto	Produto operacional, mas com nível de desempenho reduzido
8	Muito Alto	Produto operacional, necessidade de reparo
9	Perigoso com Aviso Prévio	O grau de risco é muito elevado para o efeito da falha, com aviso prévio. Afecta a segurança na operação do produto ou envolve o não cumprimento da legislação
10	Perigoso sem Aviso Prévio	O grau de risco é muito elevado para o efeito da falha, sem aviso prévio. Afecta a segurança na operação do produto ou envolve o não cumprimento da legislação

Tab. 3.8: Sistema de classificação da Ocorrência.[56, 58, 59]

Índice	Gravidade	Critério
1	Extremamente Remota	1:1.000.000
2	Remota	1:20.000
3	Mínima	1:4.000
4	Probabilidade Baixa	1:1.000
5	Baixa	1:400
6	Moderadamente	1:80
7	Moderadamente Alta	1:40
8	Alta	1:20
9	Muito Alta	1:8
10	Extremamente Alta	1:2

Tab. 3.9: Sistema de classificação da Deteção[56, 58, 59].

Índice	Gravidade	Critério
1	Quase Certa	Possibilidade quase certa que o controlo de projeto irá detetar a causa
2	Muito Alta	Possibilidade muito alta que o controlo de projeto irá detetar a causa
3	Alta	Possibilidade alta que o controlo de projeto irá detetar a causa
4	Moderadamente Alta	Possibilidade moderadamente alta que o controlo de projeto irá detetar a causa
5	Moderada	Possibilidade moderada que o control de projeto irá detetar a causa
6	Baixa	Possibilidade baixa que o controlo de projeto irá detetar a causa
7	Muito Baixa	Possibilidade muito baixa que o controlo de projeto irá detetar a causa
8	Remota	Possibilidade remota que o controlo de projeto irá detetar a causa
9	Muito Remota	Possibilidade muito remota que o controlo de projeto irá detetar
10	Certeza Absoluta de não Detectar	Controlo de projeto certamente não deteta a causa

Tab. 3.10: Escala RPN [58].

Índice	RPN	Critério
> 100	Alta	Prioridade zero, requer ações preventivas
50 a 100	Médio	Prioridade 1, requer ações preventivas ou corretivas
1 a 50	Baixo	Prioridade 2, pouco vulnerável

General Public License

A licença *General Public License* (GPL) é das mais usadas no mundo do *Open Source* [60] e permite a:

- Cópia e distribuição do código fonte.
- Modificação do código fonte e redistribuição do mesmo.
- Distribuição de versões compiladas do programas modificadas ou não
- Todas as cópias devem ser acompanhadas da respectiva identificação *copyright*.
- Todas as cópias são distribuídas sobre a licença GPL.
- Disponibilização ao publico do código fonte de todas as cópias distribuídas [61, 60].

Berkeley Software Distribution

A *Berkeley Software Distribution* (BSD) é das mais simples no domínio do *open source*, tornando-se assim aquela que menos inconsistências tem ao nível jurídico [62, 60].

Esta licença permite a redistribuição do código, com ou sem modificações, desde que se cumpram as seguintes exigências:

- A redistribuição do código fonte deve manter o *copyright*.
- A redistribuição em formato binário deve manter o aviso de direitos de autor.
- Os nomes dos colaboradores não devem ser usados para promover produtos derivados.

Apache

A licença Apache permite que o software seja usado por qualquer pessoa para qualquer propósito, incluindo a possibilidade de incluir código proprietário sem a necessidade de revelar o código fonte e resumidamente permite:

- Alteração do código fonte e redistribuição.
- Utilização por parte de qualquer pessoa.
- Não obriga à distribuição de uma cópia do código fonte.

Eclipse Public License

O *Eclipse Public License* EPL permite que o código fonte seja de uso livre, modificado, copiado e distribuído. Mudanças ao código original obrigam à disponibilização do mesmo conteúdo. Se adicionar novos componentes não é necessário disponibilizar o código fonte. Esta licença não é compatível com a GPL [63].

Capítulo 4

Implementação do efficientia sysPACS

Os capítulos anteriores permitiram entender quais os passos essenciais para a marcação CE de um dispositivo médico, quais as principais falhas de um software e quais as principais preocupações na programação segura.

Neste capítulo será feita a apresentação do efficientia sysPACS e alguns dos seus principais componentes. É também apresentada a aplicação do processo de marcação CE, a gestão de risco do efficientia sysPACS e, por fim, irá fazer-se uma comparação entre o sistema MIS e o efficientia sysPACS.

4.1 Medical Image Service

O Medical Image Service (MIS) é um sistema de teleradiologia que foi a base para o efficiencia sysPACS. O MIS funciona como uma plataforma Web em que auxilia o fluxo interno de trabalho de uma clínica hospitalar. Permite a visualização de imagens médicas através de um visualizador DICOM associado, o Weasis[1] [64, 65].

O serviço MIS tem como principais funções a comunicação com os equipamentos de imagiologia e o armazenamento das imagens DICOM por um período de tempo pré-definido, permitindo envio dos estudos para outros dispositivos remotos, como é o caso de um computador pessoal do médico para que este possa relatar o exame, e incorpora um sistema multi-idioma com o apoio de um ficheiro XML.

Esta solução engloba no seu conjunto quatro módulos referentes aos vários intervenientes no processo clínico, sendo eles: Médico relator, Transcrição, Atendimento e Utentes.

[1] http://www.dcm4che.org/confluence/display/WEA/Home

Toda a solução foi desenvolvida recorrendo a uma *Content Management System* (CMS), o *Joomla*, o que foi posto de lado na desenvolvimento do efficientia sysPACS.

4.2 efficientia sysPACS

O efficientia sysPACS é o sistema de teleradiologia que irá substituir o MIS, no entanto as principais funções são mantidas.Este é um serviço que permite, através da web, fazer uma gestão integrada do armazenamento e da distribuição de imagem médicas para o apoio ao diagnóstico.

Os dois principais objetivos deste serviço são:

- Reduzir o tempo de diagnóstico do médico relator, fornecendo-lhe ferramentas de diagnóstico, transcrição e/ou gravação.
- Permitir ao utente aceder às suas imagens médicas, como por exemplo TAC, e fazer o *download* com o visualizador e o respetivo relatório.

Este sistema possibilita alertar o médico relator, através do correio eletrónico, mensagens escritas para o telemóvel (sms)/mensagens instantâneas, baseado em escalas médicas e num sistema de prioridades que fazem parte do serviço. A finalidade dos alertas é ajudar o médico relator a gerir melhor o seu tempo, visando-se diminuir o período de espera do diagnóstico em cada estudo.

Utilizam-se alguns dos mais importantes protocolos utilizados em ambientes hospitalares, como é o caso do DICOM e HL7 v2 ou v3, os quais permitem a integração com os mais diferenciados sistemas disponíveis nestes ambientes.

O efficientia sysPACS tem como principais funções:

- Comunicar com os equipamentos de imagiologia e armazenar as imagens DICOM por um período de tempo pré-definido;
- Realizar de forma automática backups da informação localmente e em sistemas separados;
- Permite o envio dos estudos para outros dispositivos remotos desde que estejam dentro da rede VPN;
- Permitir a utilização de visualizadores tais como o Osirix e o iQ-VEW.
- Suportar um sistema multi-idioma.

Podem obter-se mais informações sobre o sistema no Anexo A.5 no Manual de Utilizador.

4.2.1 Módulos

Para uma melhor compreensão da solução, foi necessário estudar os módulos que a constituem para proceder à identificação de eventuais falhas presentes na aplicação, bem como as licenças usadas por cada componente dos módulos.

O efficientia sysPACS está dividido em vários módulos distintos em que a divisão serve para separar as diferentes funcionalidades de cada utilizador do sistema e permite uma melhor gestão, por parte da administração do sistema, constituindo uma boa prática de segurança.

Módulo Recepção

O módulo de recepção tem como objetivo iniciar o processo clínico, criando o paciente, e apresenta como principais funcionalidades:

- Registar um novo estudo a ser realizado;
- Definir prioridades do estudo para serem enviados alertas ao médico relator;
- Gerar a senha para o utente poder aceder, via web, às imagens médicas e relatório.

Módulo de Utente

Este módulo permite consultar o exame e o respetivo diagnóstico. O processo é iniciado quando se regista o utente no sistema no RIS (sistema hospitalar). Posteriormente ao registo é enviada uma mensagem HL7 para o servidor online, onde é atualizada a lista de trabalho.

O recepcionista no efficientia sysPACS gera a password de acesso para o utente, que lhe dá acesso ao sistema onde pode ver as suas imagens e o respetivo relatório. Posteriormente é definida a prioridade do estudo e, com recurso à escala médica, o médico relator será alertado da existência de um novo estudo para relatar.

Módulo *GateWay*

O módulo *GateWay* é um módulo que possibilita o envio de imagens médicas que se encontram na clínica, de forma segura para sistema web. Tem como principais

caraterísticas:

- Enviar para o serviço online as novas imagens;
- Efetuar localmente ou remotamente backups das imagens armazenadas.

Após a conclusão do estudo do qual resultam imagens no formato DICOM, estas são enviadas para o módulo *GateWay*, que as reencaminha para o servidor online (efficientia sysPACS). Neste momento considera-se que as imagens estão no arquivo *online*.

É possível através de um visualizador aceder localmente às imagens e é também nesta fase que é feito um backup das imagens, as quais são enviadas para o servidor online através um canal seguro (VPN), ficando prontas para serem visualizadas.

Módulo Médico Relator

O módulo médico relator é o de maior importância para este sistema por nele serem disponibilizadas as principais funções do sistema, como são os casos de relatar e permitir que as imagens sejam visualizadas. Neste módulo o médico relator pode:

- Aceder à sua lista de trabalho;
- Visionar imagens médicas através de um visualizador;
- Escrever o relatório médico;
- Ditar o relatório médico;
- Validar a transcrição médica.

O médico relator, após receber a notificação de que tem estudos pendentes, acede, através de um web browser, à sua lista de trabalho. O acesso à informação é feito através do protocolo HTTPS, dando acesso a um conjunto de ferramentas para este efetuar o diagnóstico tais como:

- Processador de texto com relatórios tipo;
- Interface de gravação áudio, formato *.spx*;
- Visualizador de imagens médicas, Weasis, apenas para apoio à visualização e não de diagnóstico.

Terminado o diagnóstico e após a transcrição, caso tenha optado pela gravação, o médico relator valida o relatório e este fica pronto a ser consultado pelo utente.

Módulo Transcrição

O módulo transcrição dá acesso ao ditado médico e permite escrever esse ditado num editor de texto integrado no sistema. Apresenta como funções:

- Transcrição do ficheiro de áudio enviado pelo médico relator;
- Criação de relatórios tipo;
- Submissão do relatório para validação.

Módulos Prioridade e Alertas

O módulo prioridade e alertas tem como principais funções:

- Escalonar o serviço dos médicos relatores;
- Gerir prioridades;
- Enviar alertas para os médicos relatores.

Módulo de Administrador

Este módulo ocupa-se com a gestão do sistema e apenas deve ser usado pelo responsável da clínica. Tem como principais funções:

- Gestão de utilizadores;
- Gestão de acessos de segurança;
- Gestão das definições DICOM;
- Distribuição de exames pelos médicos relatores;
- Gestão de acessos e permissões de utilizadores;
- Escalas médicas;
- Lista de prioridades;
- Definições gerais do centro clínico.

Módulo de Backups

Neste módulo é possível efetuar o backup das imagens mais antigas que se encontram online, passando as imagens para um estado de offline.

4.2.2 Ferramentas

Nesta secção são apresentadas as principais ferramentas para a construção do efficientia sysPACS, algumas delas já usadas no sistema anterior. Foi necessário estudar estas ferramentas para identificação das licenças que as regem e deteção de eventuais problemas associados.

Conquest DICOM

O PACS usado foi o Conquest que se trata de um servidor DICOM, utilizado para armazenar e distribuir as imagens médicas, o qual foi desenvolvido por Mark Oskin[2].

Este mini-PACS tem a vantagem de ser Open Source e tem como principais funções:

- Pesquisa de imagens;
- Arquivo de imagens;
- Encaminhamento e compressão das imagens;
- Acesso Web a imagens DICOM (WADO).

Weasis

O Weasis [3] é um visualizador de imagens médicas não certificado, que permite visionar imagens a partir da Web de acordo com o protocolo *Web Access to DICOM Objects* (WADO). Trata-se de um software Open Source desenvolvido na linguagem java e contém as funções base dos visualizadores DICOM como zoom, alteração do brilho e contraste entre outros. Uma das caraterísticas mais relevantes é a possibilidade de se ligar a um PACS que suporte ligações WADO via um portal Web.

[2] http://ingenium.home.xs4all.nl/dicom.html
[3] http://www.dcm4che.org/confluence/display/WEA/Home

Mirth Connect HL7

No meio hospitalar existem varios sistemas de informação que usam diferentes protocolos de comunicação, mas quando existe a necessidade de comunicar é preciso recorrer a ferramentas intermédárias.

O Mirth Connect HL7 [4] é baseado em padrões HL7, sendo um motor de integração em serviços de saúde. Este sistema facilita o encaminhamento, filtragem e a transformação de mensagens entre sistemas de informação em saúde. O software permite também a monitorizaçãoda da conexão em tempo real, reprocessamento de mensagens e suporta uma variedade de protocolos de mensagens padrões como o caso de HL7 v2.x, HL7 v3 e DICOM.

Joomla

Com o objetivo de facilitar o desenvolvimento do MIS, recorreu-se a um CMS, o Joomla, por ser uma ferramenta de fácil utilização e de código aberto (licença GNU/GPL). O Joomla é desenvolvido em PHP e pode ser executado num servidor *Web Apache* usando uma base de dados MySQL. O Joomla facilita a criação de funções base para sites como identificação/autenticação de utilizadores, criação, edição e publicação do conteúdo, entre outros. Estes recursos estão já pré-programados, sendo esta a principal vantagem de qualquer CMS [5].

O Joomla apresenta junto da sua comunidade de utilizadores alguns problemas de segurança, apesar do código da componente CMS ser relativamente seguro, pois é desenvolvido pelos programadores do Joomla. O mesmo não se aplica às extensões que são desenvolvidas pela comunidade, que nem sempre respeitam as regras de segurança [6] [35].

Por motivos de segurança e de administração do sistema, foi decidido abandonar o Joomla, o que levou à elaboração do efficientia sysPACS.

CKEditor

O editor de texto escolhido foi o CKEditor, um editor em páginas Web. Tem funcionalidades que fazem parte de aplicações como o *Microsoft Word* ou o *OpenOffice* e trata-se de um software Open Source e de fácil integração.

[4] http://www.mirthcorp.com/products/mirth-connect
[5] http://pt.wikipedia.org/wiki/Joomla
[6] http://www.webmaster.pt/joomla-tutorial-seguranca-4.html

Nanogong

Para o médico relatar o exame recorreu-se a um gravador de voz integrado na própria interface, para assim facilitar o uso do mesmo. O gravador usado foi o Nanogong [7], que é um applet utilizado para gravar e reproduzir som numa página web. Trata-se de um *applet open source* com a licença do tipo Apache v2.

mPDF

O mPDF [8] é um conversor de HTML para PDF. É compativel com os standards CSS 2 e 3, e suportando HTML 4.0. É uma applet open source que com licença GNU Lesser GPL.

VPN pptp

Point-to-Point Tunneling Protocol [9] (PPTP) é adequado para aplicações de acesso remoto do tipo VPN, e opera na segunda camada de OSI, *data link*. A transmissão de dados é feita de forma encriptada e comprimida. Os túneis VPN são criados em 2 passos [66]:

- O cliente PPTP liga-se ao provedor de internet, denominado ISP;
- Cria uma ligação TCP entre o servidor e o cliente, estabelecendo assim um túnel VPN.

O PPTP apresente caraterísticas de segurança tais como:

- Autenticação através de métodos tais como EAP-TLS, CHAP e PAP;
- Criptografia de 128 bits;
- Filtro de pacotes através de *firewall*.

Licenças

Por motivos comerciais foi necessário fazer um levantamento das licenças de todas as ferramentas que fazem parte do efficientia sysPACS, como comprova a figura 4.1, pois algumas dessas licenças apresentam caraterísticas especiais, como por exemplo a

[7] http://gong.ust.hk/nanogong/index.html
[8] http://www.mpdf1.com/
[9] http://pptpclient.sourceforge.net/

impossibilidade de comercialização. As principais caraterísticas de todas as licenças presentes na aplicação podem ser consultadas na Secção 3.5.

4.3 Processo de Marcação CE

Nesta secção será feita a descrição do processo de marcação CE aplicada ao sysPACS. Este processo será descrito de acordo com os passos identificados no Capítulo 2.

O primeiro passo dar é definir que o produto é um dispositivo médico, sendo para isso preciso ter em atenção a definição de dispositivo médico que se encontra no Decreto-Lei 145 de 2009. Nesta definição define-se que o *software*, por si só, é um dispositivo médico quando destinado pelo fabricante a ser utilizado especificamente para fins de diagnóstico. Para além de abrangido pela definição de dispositivo médico, o produto referido é considerado na definição de *Dispositivo médico ativo* do mesmo decreto.

4.3.1 Classificação do Dispositivo Médico

Para que desde o princípio se proceda considerando a classe do dispositivo, devem ser aplicadas as regras do decreto para obter a dita classificação. O resultado da aplicação das regras pode ser consultado na Tabela 4.2.

Aplicando as 18 regras verifica-se que duas abrangem o efficientia sysPACS, classificando-o como dispositivo médico de classe I.

A regra nº 1 classifica os dispositivos não invasivos como pertencentes à classe I. Apesar de ser um dispositivo ativo, não respeita as regras 9, 10 e 11 e consequentemente é classificado, pela regra nº 12, como dispositivo da classe I.

Regra 1 - *"Todos os dispositivos não invasivos pertencem à classe I, excepto no caso de se aplicar uma das regras seguintes."* [17].

Regra 12 - *"Todos os restantes dispositivos ativos pertencem à classe I."*.

No entanto, a Regra 16 levantou algumas dúvidas quanto à sua aplicabilidade a esta classificação. Para tal foi necessário recorrer-se a outro tipo de documentação relacionada com este tema, descrita de seguida. A dúvida remetia para a definição de *"registo de imagens radiográficas"*, como se pode ver na definição da regra 16.

Regra 16 - *"Os dispositivos especificamente destinados ao registo de imagens radiográficas de diagnóstico pertencem à classe IIa."*

Tab. 4.1: Tipos de Licenciamento vs. Sistemas Operativos

Software	GPL	BSD	Apache	EPL	SP	PHP	Ver.	MSW	Linux	MAC
Conquest		X					X	X	X	X
Weasis				X			X	X	X	X
MC HL7			X				X	X	X	X
MySQL	X						X	X	X	X
Wonder Shaper	X								X	
EffMis GW					X			X		
Apache			X				X	X	X	X
PHP						X	X	X	X	X
Joomla	X						X	X	X	X
CKEditor	X						X	X	X	X
Nanogong			X				X	X	X	X
DomPDF	X						X	X	X	X
PHPmailer	X						X	X	X	X
Luxcalendar	X						X	X	X	X
vpn pptp	X						X	X	X	X

Tab. 4.2: Regras para Classificação da Classe do Dispositivo Médico.

Regra	Aplicável	Classe
1	Sim	I
2	Não	—
3	Não	—
4	Não	—
5	Não	—
6	Não	—
7	Não	—
8	Não	—
9	Não	—
10	Não	—
11	Não	—
12	Sim	I
13	Não	—
14	Não	—
15	Não	—
16	Não	—
17	Não	—
18	Não	—

Recorrendo ao *Manual on borderline and classification in the community regulatory framework for medical devices*[10], determina-se uma classificação mais adequada para o sysPACS.

Existem vários tipos de sistemas PACS:

a) PACS usado para visualização, arquivo e transmissão de imagens.

b) Sistema onde se pode fazer o pós-processamento da imagem para fins de diagnóstico, tais como:

   1. Funções de processamento de imagem que alteram os dados da imagem, como por exemplo filtros, reconstrução multiplanar e reconstrução 3D.
   2. Funções quantitativas complexas, como por exemplo avaliação arterial, cálculo do volume ventricular e deteção automática de lesões.

c) Controlo da aquisição de imagem.

No caso em que o PACS é abrangido pela definição de um dispositivo médico, ou seja, é especificamente destinado pelo fabricante a ser utilizado para uma ou mais das finalidades médicas estabelecidas na definição de dispositivo médico, as seguintes situações podem ser consideradas:

i Relativamente ao PACS (a) considera-se que a aplicação da regra 12 pode ser adequada e portanto este tipo de PACS é geralmente classificado como dispositivo médico de classe I.

ii Ao PACS (b) é aplicada a regra 2.3 que o classifica como um dispositivo médico de classe IIa ou IIb. Se o PACS não conduzir ou influenciar o uso da fonte de irradiação, pode ser classificado ao abrigo da regra 10, diagnóstico direto, definindo-o como classe IIa.

iii Se o PACS é destinado a controlar a fonte de aquisição, deve cair na mesma classe que o dispositivo de origem, pela regra 2.3 "comandam um dispositivo ou influenciam o uso de um dispositivo, cai automaticamente na mesma classe". Esta classificação permite que este tipo de PACS possa ser classificado como dispositivos médicos classe IIa ou IIb, de acordo com a classificação do próprio dispositivo.

[10] $http://ec.europa.eu/health/medical-devices/index_en.htm$

Esta classificação vem esclarecer todas as dúvidas, pois separa todos os tipos de PACS em classes distintas. A que melhor define o sysPACS é a "*a*", logo é classificado, segundo o item "*ii*", como classe I.

4.3.2 Processo

Nesta secção será descrito o que foi elaborado para cada um dos 6 passos do processo de marcação CE do sysPACS, descrita na Secção 2.2.

1 Identificar as diretivas aplicáveis. Como já foi possível observar, os dispositivos médicos encontram-se abrangidos por diretivas Europeias. Consultando a legislação Nacional, constatou-se que o Decreto-Lei 145 de 2009 é o indicado para o processo de marcação CE do efficientia sysPACS, porque é o que internamente trata de questões relacionadas com os dispositivos médicos. Para este processo também foi tida em conta a Diretiva Europeia 93/42/CEE, pois esta é a base do Decreto-Lei 145 de 2009.

2 Os requisitos essenciais são um ponto muito importante de todo o processo de marcação. A verificação dos requisitos essenciais foi efetuada através de um documento fornecido no site do INFARMED, que está de acordo com os requisitos do anexo VII do Decreto-Lei n.º 145/2009 de 17 de Junho. Esse documento encontra-se devidamente preenchido, como se obsera na Figura 4.1, e pode ser consultado no Anexo A.1.

3 Para se determinar o Organismo Notificado, recorreu-se ao Decreto-Lei nº 145/2009, que aponta o INFARMED como Autoridade Competente e Organismo Notificado para a marcação CE de Dispositivos Médicos [17]. Foi também verificado no site do *New Approach Notified and Designated Organisations*[11] (NANDO) que é uma organização que divulga aos estados membros qual o organismo que foi designado para a avaliação da conformidade dos requisitos de uma determinada diretiva, pode constatar-se, que para a diretiva 93/42/EEC Medical Devices, em Portugal o INFARMED é o Organismo Notificado.

4 A avaliação da conformidade, no caso de dispositivos de classe I, é feita de acordo com o anexo VII do Decreto-Lei n.º 145/2009 de 17 de Junho, na

[11] $http : //ec.europa.eu/enterprise/newapproach/nando/index.cfm?fuseaction = na.detailna_id = 164905$

qual deve constar uma descrição geral do produto, bem como desenhos de concepção e uma descrição dos métodos de fabrico. Foi também elaborado um requerimento de avaliação da conformidade, Anexo A.3, uma declaração de compromisso, Anexo A.4 e uma declaração de conformidade CE, Anexo A.2

5 A documentação técnica sobre o efficientia sysPACS encontra-se em anexos e resume-se ao Manual de Utilizador, Anexo A.5 e Manual Técnico.

6 Esta fase tem como finalidade dar cumprimento a todas as fases anteriores. No caso do produto estudado, esta fase representa a apresentação da documentação perante o INFARMED.

	Aplicável	
	Sim 1) Método(s) encontrado(s) para garantir cumprimento (indicar qual(is)) 2) Documento(s) do SGQ relacionado(s)	**Não** 1) Justificação
Grupo I - Requisitos gerais		
1.2.1 A redução, na medida do possível, dos riscos derivados de erros de utilização devido às características ergonómicas do dispositivo ou ao ambiente que está previsto para a utilização do produto (conceção tendo em conta a segurança do doente);	1) Concepção 2) ISO 9001:2008	
1.2.2 A consideração dos conhecimentos técnicos, da experiência, da educação e da formação e, se for caso disso, das condições clínicas e físicas dos utilizadores previstos (conceção para utilizadores não profissionais, profissionais, portadores de deficiência ou outros utilizadores);	1) Concepção 2) ISO 9001:2008	
2.1 Eliminar ou reduzir os riscos ao mínimo possível (conceção e construção intrinsecamente seguras);	**1) Gestão de Risco** **2) Concepção**	

Fig. 4.1: Requisitos Essenciais.

4.4 Gestão de Risco - efficientia sysPACS

O processo de desenvolvimento de um dispositivo médico deve ser feito de tal forma que a saúde de utilizadores ou de terceiros nunca seja posta em causa. Este facto requer que o todo o processo tenha a segurança adequada.

A gestão de risco tem como finalidade aperfeiçoar o processo de desenvolvimento, identificando eventuais perigos que possam estar presentes.

Para o processo de análise de eventuais falhas foi tida em conta a norma ISO 14971, descrita anteriormente, e o FMEA. Estas duas normas da gestão de risco foram usadas em conjunto, de modo a aproveitar o que de bom cada uma pode oferecer.

A norma ISO 14971, está mais ligada à identificação dos perigos, e o FMEA, mais ligado à quantificação, no entanto, são idênticas em muitos aspetos. O FMEA é referido na ISO 14971 como uma boa técnica para identificar problemas específicos e contribui para o amadurecimento de um projeto [54].

Finalidade prevista

Como referido anteriormente, o efficientia sysPACS tem como finalidade aumentar a produtividade de clínicas que prestam serviços de imagiologia médica e que pretendam utilizar a teleradiologia para facilitar o processo de relato de exames. Visa ainda permitie ao utente, através de uma senha gerada no atendimento, aceder às imagens pela web, fazendo o download do ficheiro com um visualizador e o respetivo relatório.

Identificação dos perigos

A identificação e a aceitação dos perigos serão baseados no Capítulo 3, onde foram apresentados os riscos inerentes à utilização e construção de software.

Na análise que se segue serão identificados os perigos que dizem respeito à utilização do efficientia sysPACS. Para melhor compreensão dos resultados apresentados, deve ter-se em atenção as tabelas do FMEA apresentadas no Anexo A.8.

FMEA de Projecto - Falha no controlo de acesso

Má utilização: Falha no controlo de acesso (Anexo A.8)

Perigo: Perda de informação confidencial, perda de dados de saúde, introdução errada de dados no sistema. Para este perigo foi atribuída uma gravidade de 10.

Risco: Injeção SQL é um perigo muito comum nos dias de hoje, com um impacto muito severo, pois permite ao atacante contornar o controlo de acesso, copiar ou mesmo manipular informações da base de dados. Inicialmente este perigo apresentava um RPN de 560.

As recomendações para este tipo de perigo passam pela codificação de caracteres e tags, tais como SELECT (tag SQL) ou mesmo tags HTML.

Controlo: Tendo em conta as ações recomendadas, foram criadas medidas para proteger contra este tipo de ataque, através da criação de uma lista de caracteres que podem ser ”mal interpretados” pela aplicação como:

```
"/(PHPSESSID|isnull|cast|substring|ascii|db_name|OR|AND|from|select
|insert|delete|where|drop table|show tables|#|\*|--|\\\\)/"
```

Estas medidas, depois de implementadas, fizeram com que a deteção diminuísse e, por conseguinte, o RPN baixasse drasticamente para 70.

Risco: Autenticação e gestão de sessões são alvos de ataques frequentes que podem causar graves dados na aplicação. Inicialmente foi identificado com um RPN de 300.

As recomendações para este risco passam por fazer com que a sessão expire após um determinado tempo, registar num ficheiro de logs as tentativas de acesso, ao efetuar operações de maior responsabilidade pedir novamente ao utilizador que se re-autentique, ligação através do protocolo HTTPS ao servidor e bloquear o acesso após um número máximo de tentativas (solução suscetível de causar indisponibilidade).

Controlo: Recorrendo às boas práticas apresentadas foram implementados mecanismos que expirassem as sessões, desenvolvidos ficheiros de registo log e usada uma implementação do protocolo HTTPS. Faltou a implementação de um método que bloqueasse o acesso ao fim de um determinado número de tentativas o qual seria interessante para combater ataques de "força bruta" ao sistema.

Após melhoria, o RPN baixou para o limiar do aceitável, 100.

Risco: Falha na restrição de acesso a URLs. Este risco prende-se com o facto de, por vezes, se criar ou usar ficheiros sem um controlo autorização adequado. Inicialmente este risco foi calculado com um RPN de 350.

Embora este tipo de risco seja incomum, devem ter-se preocupações tais como criar níveis de autorização e definir o que cada um pode fazer e encriptar os dados passados por URL.

Controlo: As recomendações para proteção contra este perigo foram implementadas dividindo os utilizadores em diferentes perfis de acesso e usando funções para encriptar os URLs. Estas medidas fizeram baixar o RPN para 100. Este valor mantém-se um pouco alto porque as funções de encriptação são funções base.

Risco: Roubo de credenciais de acesso. Este tipo de risco pode ser bastante prejudicial para a aplicação, pois pode permitr o acesso indevido a informações confidenciais. Inicialmente foi calculado um RPN de 480.

Uma boa prática, comum em aplicações muito conhecidas da Internet, é a verificação da autenticação através de uma mensagem enviada para o telemóvel do utilizador.

Controlo: Nada foi feito para mitigar este risco, principalmente porque o sistema de mensagens tem um custo associado.

FMEA de Projecto - Introdução de dados errados no sistema

Má utilização: Introdução de dados errados no sistema (Anexo A.8)

Perigo: Erros que podem levar à quebra do sistema, introdução de dados médicos errados, troca de dados médicos dos utentes. Para este perigo foi atribuída uma gravidade de 7.

Risco: Referência direta a objetos, que pode permitir que utilizadores autenticados possam alterar os URLs e aceder a informações de outros utilizadores. Inicialmente com um RPN de 441.

Uma boa prática para proteção deste risco passa por encriptar os URLs e posteriormente fazer uma validação dos dados que vão ser processados pelas funções.

Controlo: As boas práticas apresentadas foram implementadas, contudo o valor de RPN mantém-se elevado, 98, pelo facto de as funções de encriptação serem as funções base.

Risco: Redirecionamento não validados. Este perigo está relacionado com o facto dos utilizadores poderem alterar os URLs. Inicialmente calculado com um RPN de 392.

As recomendações contra este tipo de problema passam pela validação de dados e encriptação dos parâmetros.

Controlo: o controlo feito para este risco é muito idêntico ao do risco anterior, mantendo-se o RPN elevado pelo mesmo motivo.

Risco: Validação de input e output de funções. Este perigo, como o nome indica, passa por validar os valores de entrada e saída de uma função. Inicialmente o RPN foi de 294.

A precaução contra este tipo de risco consiste em validar todos os valores de entrada e saída de uma função.

Controlo: As ações tomadas as recomendadas: validação dos valores. No entanto, o RPN manteve-se elevado, 126, e a precisar de novas medidas tais como limitar a saída das funções aos valores de verdadeiro ou falso.

FMEA de Projecto - Perda de informação

Má utilização: Perda de informação (Anexo A.8)

Perigo: Perda de informação, falta de confiança por parte dos clientes, problemas legais. Para este perigo foi atribuída uma gravidade de 10.

Risco: Comunicação insegura, consiste em trocar dados com o servidor às "claras", sem qualque garantias de confidencialidade. Inicialmente o RPN era de 280.

Uma boa prática para proteção dos dados em trânsito é o uso do protocolo HTTPS juntamente com uma rede VPN.

Controlo: A implementação das boas práticas levou a que o RPN diminuísse para o valor 100.

Risco: Armazenamento criptográfico inseguro passa por armazenar dados críticos como palavras chave com um nível de encriptação não adequado. Inicialmente o RPN era de 560.

A melhor precaução é usar uma função de encriptação mais sofisticada e robusta.

Controlo: O controlo implementado passa pela encriptação dos dados com a função SHA o que fez diminuir o RPN para 80.

Informação Pós produção

A informação de pós-produção é apresentada na Tabela 4.3, devendo ser processadas e aplicadas Às conclusões que se possam retirar da sua análise.

Tab. 4.3: Ferramentas a incluir na gestão de risco pós-mercado.

Ferramentas Pós-mercado
Inquéritos aos Utentes
Inquéritos aos profissionais
Não conformidades identificadas
Tratamento de reclamações

De referir que a análise de risco e as medidas de controlo implementadas, juntamente com os resultados obtidos, devem fazer parte da documentação técnica. A gestão de risco deve ser uma atividade periódica do fabricante.

Os testes de monitorização de risco devem ser realizados periodicamente e atualizados de acordo com o estado da arte, dando assim garantia da continuidade da segurança do efficientia sysPACS.

4.5 Avaliação dos aspectos de segurança

Nesta secção será apresentada uma comparação entre o MIS e o efficientia sysPACS, focando a evolução ao nível da programação, juntamente com vários processos de boas práticas.

Os melhoramentos feitos ao software ao longo do tempo tiveram como base as normas apresentadas no capítulo anterior, sendo aqui dada a evidência do cumprimento de boas práticas para a programação segura.

Para uma melhor compreensão do efficientia sysPACS será apresentada uma breve descrição do sistema. Na Figura 4.2 pode ver-se um esquema dos várias componentes que constituem o sistema.

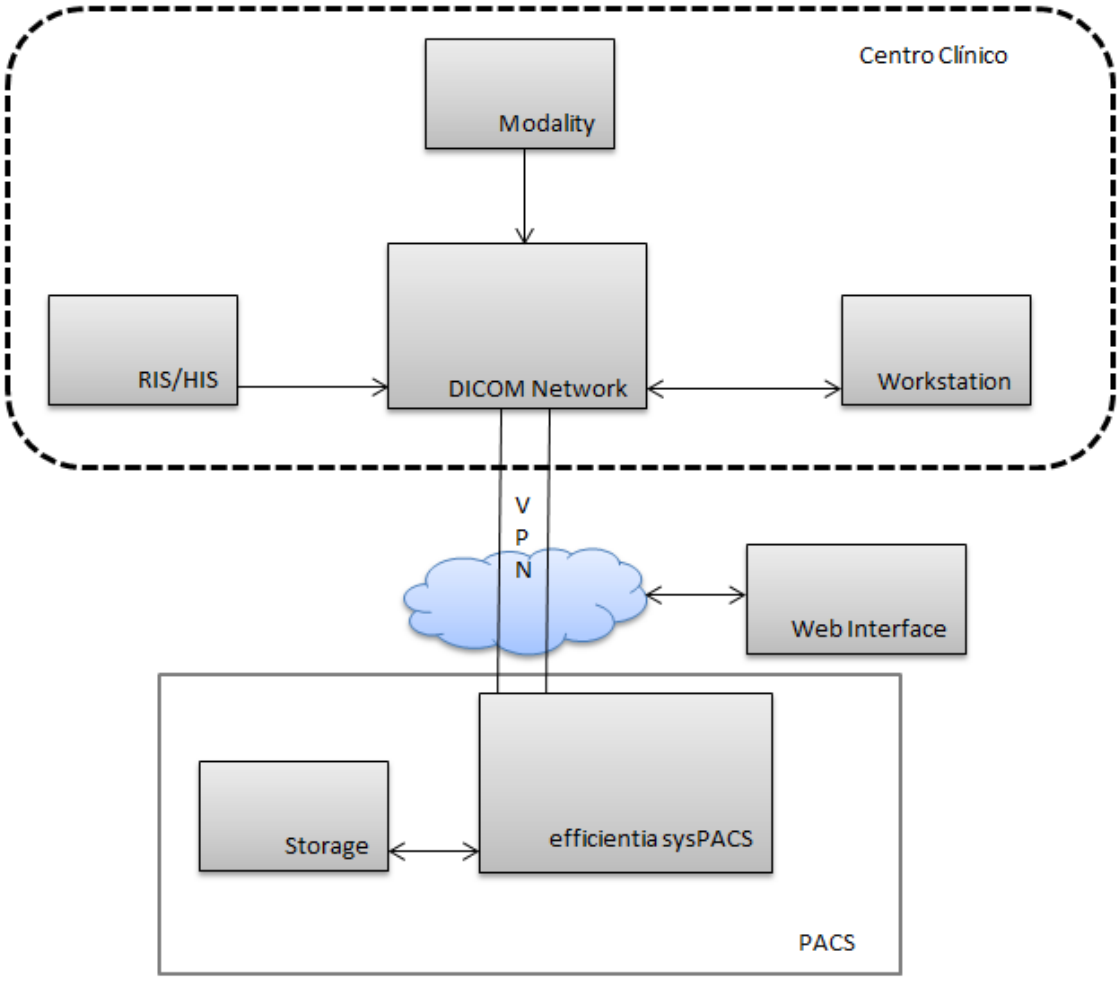


Fig. 4.2: efficientia sysPacs.

O PACS está alojado num servidor dedicado, que se encontra representado na figura pelo efficientia sysPACS e *storage* onde serão efetuadas todas as operações

possíveis através dos módulos anteriormente apresentados.

A rede DICOM engloba o que normalmente se encontra dentro dos centros hospitalares, o HIS/RIS, as Workstation e as modalidades.

As modalidades representam na Figura 4.2 todos os equipamentos que produzem imagens médicas que podem dar origem a um relatório, tais como RM, TAC, entre outros. Estas imagens são enviadas para a rede DICOM, que por sua vez envia as mesmas imagens para o PACS, efficientia sysPACS.

O RIS/HIS representa o sistema de informação do hospital ou clínica sistema esse que envia para o efficientia sysPACS os dados do utente, os quais posteriormente usados pelo efficientia sysPACS para identificar os utentes e gerar passwords.

As Workstation são estações de trabalho onde os médicos podem aceder às imagens para realizar o relatório, que podem estar dentro do centro hospitalar ou noutro local desde que tenha acesso a Internet. Esta é a principal vantagem do efficientia sysPACS, disponibilizar imagens em qualquer lugar.

O médico relator poderá também aceder diretamente às imagens (com um visualizador Osirix e iQ-VEW), com os parâmetros DICOM introduzidos no PACS (AET, IP e porta). Estes parâmetros terão de ser configurados pelo administrador do sistema. Por questões de segurança, foi implementada uma rede VPN, que permitirá que as imagens médicas sejam descarregadas do PACS para o visualizador do médico relator por um canal seguro. No entanto a rede VPN levanta o problema da velocidade de download, uma vez que as imagens terão de ser encriptadas antes de serem enviadas pelo canal seguro.

Por essa razão, foi criada a possibilidade do médico relator descarregar as imagens sem estar conectado à rede VPN, sendo que essa permissão terá de ser dada pelo administrador do sistema.

Esta funcionalidade apenas está disponível mediante duas condições: se o administrador do sistema permitir e definir que o médico pode aceder a imagens externamente.

4.5.1 Comparação do MIS com o sysPACS

Para se poder comparar a evolução da aplicação após o processo de reengenharia, foi aplicada a *checklist* que se encontra no Anexo A.7, baseada em documentos internos da Efficientia e na referência [67].

Essa *checklist* foi aplicada em dois momentos diferentes do desenvolvimento: a primeira aplicação foi efetuada no início da reformulação da aplicação no dia 31

de Janeiro de 2012 ao MIS, mostrando-se os resultados no Gráfico a) 4.3; depois de várias alterações, a aplicação foi verificada novamente a *checklist* e produzidos novos resultados, que podem ser vistos no Gráfico b) 4.3 (os números de 1 a 13 representam os aspetos a avaliar e são apresentados de seguida).

Os aspetos do software para avaliação e comparação do desenvolvimento feito na aplicação foram os seguintes:

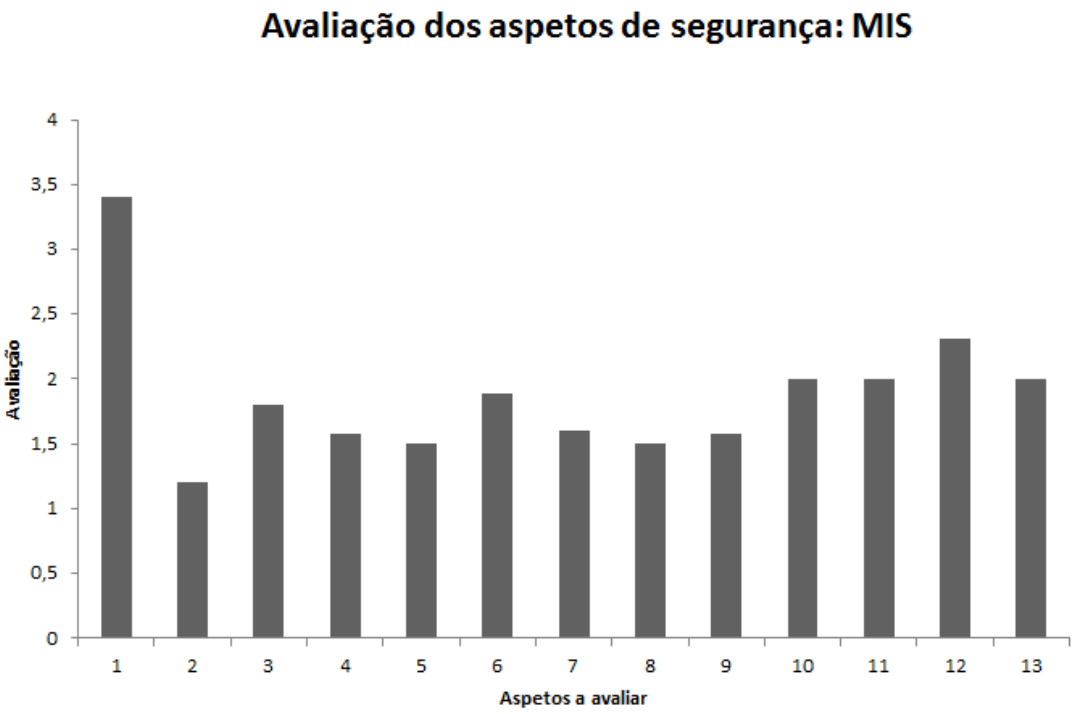
1. Autenticação e Autorização dos utilizadores
2. Confidencialidade dos dados
3. Integridade dos dados
4. Disponibilidade do sistema
5. Auditabilidade
6. Utilização ao nível de administração
7. Utilização normal
8. Conformidade com normas
9. Mecanismos de defesa
10. Comunicações
11. Teste e Verificação de Rotina
12. Verificação Aplicacional
13. Documentação

Para melhor compreensão dos temas apresentados será feita uma breve explicação do seu objetivo, bem como o que foi melhorado em cada aspeto.

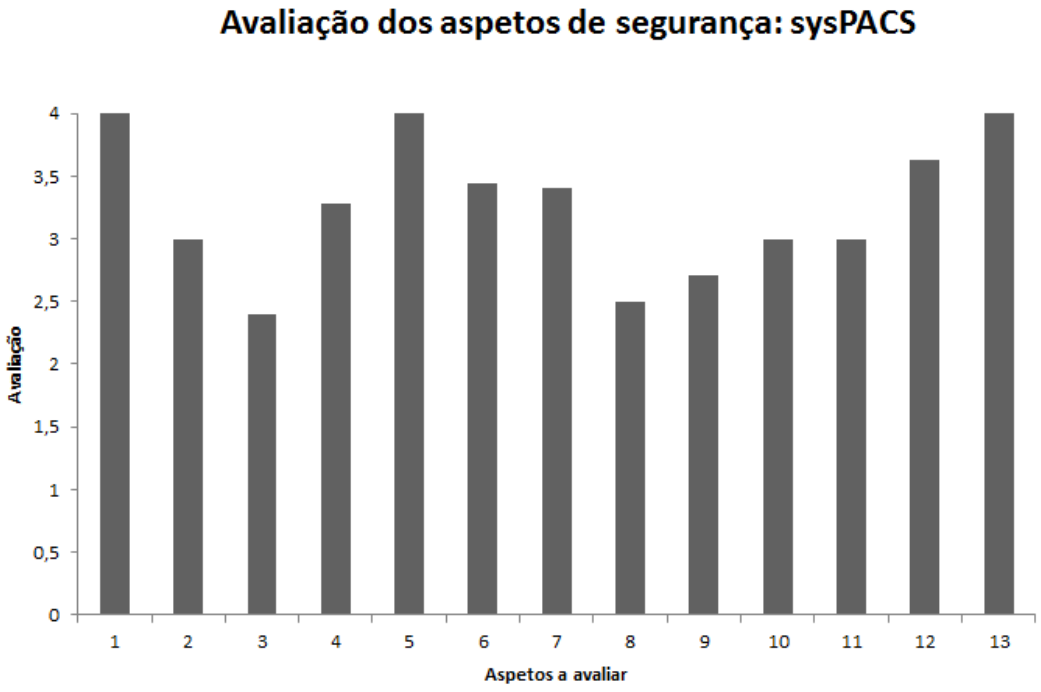
Autenticação e Autorização dos utilizadores

Ao nível da autenticação foi melhorada a gestão de senhas do utilizador, podendo este alterar a sua palavra-chave sempre que quiser. Existe também um sistema de quebra de sessão, que obriga o utilizador a introduzir a sua palavra-chave sempre que se esgota um tempo de inutilização.

Quanto à autorização dos utilizadores, cada utilizador só pode alterar a informação que produziu, sendo também controladas as permissões dos utilizadores.



(a)



(b)

Fig. 4.3: Evolução da aplicação: (a) MIS; (b) efficientia sysPACS.

Confidencialidade dos dados

Preferencialmente as imagens médicas são trocados entre o servidor e o utilizador se este estiver dentro da rede VPN, solução que permite manter a confidencialidade dos dados.

Não é possível aceder a dados através de links guardados no histórico, dados que está implementado um sistema de variáveis de sessão.

É possível verificar também quem alterou os dados, pois foi implementado um sistema de *logs* que cobre a VPN, comunicação DICOM, base de dados e aplicações.

Integridade dos dados

A integridade dos dados não foi muito desenvolvida ao longo deste trabalho. No entanto existe um pequeno aumento relacionado com o reforço da segurança em toda a aplicação, comfirmado com o bom comportamento da aplicação perante os testes que foram feitos ao longo do tempo.

Para garantia elevada da integridade dos dados será importante implementar um sistema baseado em encriptação.

Disponibilidade do sistema

A disponibilidade do sistema não é 100% garantida. Para melhorar este aspeto está previsto implementar dois servidores idênticos em pontos distintos, o que ainda não foi posto em prática.

Auditabilidade

A auditabilidade ao sistema foi melhorada substancialmente, pois foram implementados sistema de registo de versões, registo de falhas encontradas e criação de checklist, Anexo A.7, as quais foram tomadas para aumentar o controlo do sistema ao longo do tempo.

Utilização ao nível de administração

A administração do sistema é feita remotamente utilizando um mecanismo de autenticação chave pública, chave privada.

O fabricante do sistema onde está alojado o efficientia sysPACS tem acesso privilegiado à máquina. Contudo o administrador da aplicação efficientia sysPACS tem

um acesso igual aos outros utilizadores. O sistema está dividido em diferentes níveis de acesso.

O administrador pode recorrer ao ficheiro de logs para efetuar estatísticas do sistema.

Utilização normal

Os processos de utilização e implementação estão documentados nos manuais técnico e de utilizador.

O sistema tem mecanismos de autenticação com passwords, que são guardadas e encriptadas com a função de *hash* SHA.

As interfaces apresentadas ao utilizador foram desenvolvidas de forma a serem o mais simples possível.

Conformidade com normas

A conformidade com as normas de segurança e gestão de risco foi implementada o que levou a uma maior conformidade do sistema com as normas aplicáveis. Por conseguinte, aumentou também a conformidade com normas como o DICOM e HL7, pois são normas que têm como base boas práticas presentes nessas normas.

Mecanismos de defesa

Os mecanismos de defesa foram melhorados com a implementação de um algoritmo mais confiável. A ligação é remota e é feita através de uma aplicação que usa um sistema de chave pública chave privada. O sistema do login foi remodelado acrescentando proteção contra injeção sql.

Comunicações

As comunicações entre servidor e cliente são feitas segundo o protocolo HTTPS e a transmissão de imagens é também feita sobre uma rede VPN, o que permite manter a confidencialidade dos dados transmitidos.

Teste e Verificação de Rotina

As funções encontram-se documentadas, sendo que nas funções mais críticas é feita uma validação tanto dos parâmetros de entrada como de saída.

A camada de ligação à base de dados foi também alterada para usar um componente mais maduro e eficiente, o ADOdb[12], que permite essencialmente abstrair do tipo de base de dados usado, MySQL, SQL server ou Oracle. O ADObd melhorou a manutenção do sistema pois agora é mais fácil alterar o tipo de base de dados. Por outro lado, as funções de consulta à base de dados estão suportadas por um boa documentação produzida pela comunidade inerente à ADObd.

Verificação Aplicacional

Na aplicação são identificados os utilizadores correntes que dispõem de um sistema multi-idioma de fácil manutenção.

A aplicação apresenta uma estrutura muito idêntica entre os formulários usados, onde são apresentadas as principais operações que o utilizador pode realizar.

Aquando do preenchimento de formulários é disponibilizado um sistema de ajuda ao utilizador bem como uma pré-validação dos dados.

O efficientia sysPACS possui uma codificação de erros, disponível para consulta do administrador do sistema.

Existe um sistema, ao nível da administração, que calcula o espaço disponível em disco.

O efficientia sysPACS possibilita a impressão de relatórios que estão tipificados e em que a impressão corresponde ao pré-visualizado na aplicação.

Documentação

Ao longo do processo foi produzida documentação técnica para administração do sistema, bem como informação para a utilização do mesmo. Foram produzidos manuais tanto de utilização como de administração.

[12] http://adodb.sourceforge.net

Capítulo 5

Conclusões e Perspetivas futuras

A importância deste trabalho relaciona-se com o contributo da clarificação da classificação do efficientia sysPACS para a marcação CE de dispositivos médicos. Foram estudadas e analisadas as várias etapas inerentes a este processo, que se revela muito importante para a introdução de novos DM no mercado europeu.

As diretivas estudadas, essencialmente o Decreto-Lei 145/2009, impõem uma harmonização de normas e procedimentos na fase de concepção e de produção de dispositivos médicos que permite que o fabricante comercialize os dispositivos no mercado europeu sem a necessidade de aplicar legislação adicional.

O processo de marcação CE é moroso e requer inúmeros recursos por parte das empresas. A exigência do processo aumenta com o aumento da classe do dispositivo, estando esta centrada nos requisitos essenciais, os quais devem salvaguardar a plena segurança dos utilizadores. A concepção e o fabrico do efficientia sysPACS foi feita com a máxima exigência possível.

A classificação do efficientia sysPACS determinou que este produto pertence à classe I de dispositivos médicos e, consequentemente, deve cumprir os requisitos adequados a esta classificação.

Para garantir a conformidade com os requisitos essenciais, foram utilizadas várias técnicas de segurança, tendo em consideração os princípios de concepção de software seguro, a realização de uma gestão de risco e, por fim, uma validação e verificação de todo o software.

Na implementação de segurança em software abordaram-se as boas práticas para a troca de informação como imagens médicas. Os resultados obtidos pela aplicação do FMEA e da comparação entre o MIS e o efficientia sysPACS evidenciam que a implementação teve resultados positivos.

No que respeita à gestão de risco, as duas técnicas estudadas foram a ISO 14971:2007, muito vocacionada para a gestão de risco em dispositivos médicos, e o FMEA, que é uma técnica que se revelou muito interessante pelo seu método de classificação analítica do risco. Os resultados alcançados com a aplicação destas técnicas mostraram, numa primeira fase, os pontos mais vulneráveis do efficientia sysPACS, aos quais foram aplicadas medidas correctivas. Numa segunda avaliação foi evidenciado que essas ações foram bastante eficientes, pois verificou-se uma redução significativa dos valores do RPM obtidos no FMEA.

A verificação e validação do software foi efetuada com a aplicação da "Checklist - Avaliação dos aspetos de segurança", na qual se avaliaram os treze pontos essenciais de um software e, de um modo geral, verificou-se uma melhoria comparativamente à versão anterior.

Por último, é importante referir que o trabalho apresentado nesta dissertação resultou da conjugação de conhecimentos de diferentes áreas de trabalho, desde informações clínicas a processos legislativos até à área de informática. Em suma, este estágio integrou um conjunto multidisciplinar de temas atuais que abrange a essência do Mestrado em Engenharia de Computação e Instrumentação Médica. Todo este trabalho decorreu ao longo de 9 meses com um total de 1023 horas e foram realizadas 46 reuniões de orientação.

Deste trabalho resultou ainda a publicação de um poster, com o título *Certification of Medical Devices, Safety and Licensed Software*, no *Workshop on Biomedical Engineering*, que teve lugar na Faculdade de Ciências da Universidade de Lisboa, no dia 21 de Abril de 2012.

Bibliografia

[1] C. EUROPEIA, "Guia para a aplicação das directivas elaboradas com base nas disposições da nova abordagem e da abordagem global," tech. rep., COMISSÃO EUROPEIA, 1999.

[2] Y. David, "101 - telemedicine: Clinical and operational issues," in *Clinical Engineering Handbook* (J. F. Dyro, ed.), pp. 484 – 487, Burlington: Academic Press, 2004.

[3] B. Stanberry, "Legal ethical and risk issues in telemedicine," *Computer Methods and Programs in Biomedicine*, vol. 64, no. 3, pp. 225 – 233, 2001.

[4] C. D. C. EUROPEIAS, ed., *sobre os benefícios da telemedicina para os doentes, os sistemas de saúde e a sociedade*, (Bruxelas), 2008.

[5] C.-H. Wang, K.-F. Ssu, P.-C. Chung, H. C. Jiau, and W.-T. Shih, "Novel recovery mechanism for the restoration of image contents in teleconsultation sessions," *Computer Methods and Programs in Biomedicine*, vol. 105, no. 1, pp. 70 – 80, 2012.

[6] D. Caramella, J. Reponen, F. Fabbrini, and C. Bartolozzi, "Teleradiology in europe," *European Journal of Radiology*, vol. 33, no. 1, pp. 2 – 7, 2000.

[7] E. Seto, K. J. Leonard, J. A. Cafazzo, J. Barnsley, C. Masino, and H. J. Ross, "Developing healthcare rule-based expert systems: Case study of a heart failure telemonitoring system," *International Journal of Medical Informatics*, vol. 81, no. 8, pp. 556 – 565, 2012.

[8] J. Hasan, "Effective telemedicine project in bangladesh: Special focus on diabetes health care delivery in a tertiary care in bangladesh," *Telematics and Informatics*, vol. 29, no. 2, pp. 211 – 218, 2012.

[9] L. Martí-Bonmatí, A. Morales, and L. D. Bach, "Toward the appropriate use of teleradiology," *Radiología (English Edition)*, vol. 54, no. 2, pp. 115 – 123, 2012.

[10] H. D. le Pointe, "Teleradiology," *Biomedicine amp; Pharmacotherapy*, vol. 52, no. 2, pp. 64 – 68, 1998.

[11] F. B. Binkhuysen and E. Ranschaert, "Teleradiology: Evolution and concepts," *European Journal of Radiology*, vol. 78, no. 2, pp. 205 – 209, 2011. From PACS to the clouds.

[12] H. K. Huang, *PACS and Imaging Informatics: Basic Principles and Applications*. John Wiley Sons, second edition ed., 2010.

[13] NEMA, "Digital imaging and communication in medicine (dicom)," tech. rep., Medical Imaging Technology Alliance, 2011.

[14] E. Parliament, "On telemedicine for the benefit of patients, healthcare systems and society," tech. rep., COMMISSION OF THE EUROPEAN COMMUNITIES, 2008.

[15] H. Tachibana, M. Omatsu, K. Higuchi, and T. Umeda, "Design and development of a secure dicom-network attached server," *Computer Methods and Programs in Biomedicine*, vol. 81, no. 3, pp. 197 – 202, 2006.

[16] Acmite, "Market report: World medical devices market," tech. rep., Acmite Market Intelligence, 2007.

[17] P. Português, *Decreto-Lei n.º 145/2009, de 17 de Junho*. INFARMED Gabinete Jurídico e Contencioso, Junho 2009.

[18] "Medical devices: Guidance document - classification of medical devices," tech. rep., EUROPEAN COMMISSION, June 2010.

[19] G. Lalis, "Principles of medical devices classification," tech. rep., The Global Harmonization Task Force, June 2006.

[20] J. O. da União Europeia, ed., *DIRECTIVA 2007/47/CE DO PARLAMENTO EUROPEU E DO CONSELHO*, Setembro 2007.

[21] N. Pallikarakis, "125 - european union medical device directives and vigilance system," in *Clinical Engineering Handbook* (J. F. Dyro, ed.), pp. 582 – 585, Burlington: Academic Press, 2004.

[22] O. J. of the European Union, ed., *DECISIONS ADOPTED JOINTLY BY THE EUROPEAN PARLIAMENT AND THE COUNCIL*, July 2008.

[23] I. Lindsay, "European directives - an overview for oem's and system integrators," tech. rep., Rockwell Automaction, April 2012.

[24] A. Carvalho, "Essential principles of safety and performance of medical devices," tech. rep., Global Harmonization Task Force, May 2005.

[25] D. A. Simmons, "119 - health care quality and iso 9001:2000," in *Clinical Engineering Handbook* (J. F. Dyro, ed.), pp. 565 – 568, Burlington: Academic Press, 2004.

[26] M. Cheng, "117 - primer on standards and regulations," in *Clinical Engineering Handbook* (J. F. Dyro, ed.), pp. 557 – 559, Burlington: Academic Press, 2004.

[27] NP..EN..ISO..9001:2008, "Sistemas de gestão da qualidade requisitos (iso 9001:2008)," tech. rep., Instituto Português da Qualidade - IPQ, 2008.

[28] ISO..13485:2003, "Medical devices - quality management systems - requirements for regulatory purposes," tech. rep., ISO, 2003.

[29] P. J. S. Miguel Pupo Correia, *Segurança no Software*. FCA, 2010.

[30] L. DeNardis, "24 - a history of internet security," in *The History of Information Security* (K. D. Leeuw and J. Bergstra, eds.), pp. 681 – 704, Amsterdam: Elsevier Science B.V., 2007.

[31] M. Kimura, "Software vulnerability: Definition, modelling, and practical evaluation for e-mail transfer software," *International Journal of Pressure Vessels and Piping*, vol. 83, no. 4, pp. 256 – 261, 2006. The 16th European Safety and Reliability Conference.

[32] S. Harris, *CISSP All-in-One Exam Guide*. McGraw-Hill Osborne Media, 2 edition ed., 2003.

[33] I. 17799, "Information technology - security techniques - code of practice for information security management," 2005.

[34] T. Berners-Lee, "The world-wide web," *Computer Networks and ISDN Systems*, vol. 25, no. 4-5, pp. 454 – 459, 1992.

[35] T. Scholte, D. Balzarotti, and E. Kirda, "Have things changed now? an empirical study on input validation vulnerabilities in web applications," *Computers and Security*, vol. 31, no. 3, pp. 344 – 356, 2012.

[36] S. King, "Applying application security standards a case study," *Computers and Security*, vol. 23, no. 1, pp. 17 – 21, 2004.

[37] OWASP, "Owasp top 10 -2010, the ten most critical web application securyt risks," 2010.

[38] I. J. Kalet, R. S. Giansiracusa, J. Jacky, and D. Avitan, "A declarative implementation of the dicom-3 network protocol," *Journal of Biomedical Informatics*, vol. 36, no. 3, pp. 159 – 176, 2003.

[39] B. Schütze, M. Kroll, T. Geisbe, and T. Filler, "Patient data security in the dicom standard," *European Journal of Radiology*, vol. 51, no. 3, pp. 286 – 289, 2004.

[40] DICOM:15, "Part 15: Security and system management profiles," tech. rep., National Electrical Manufacturers Association, 2011.

[41] Z. Zhou, "Data security assurance in cad-pacs integration," *Computerized Medical Imaging and Graphics*, vol. 31, no. 4-5, pp. 353 – 360, 2007. Computer-aided Diagnosis (CAD) and Image-guided Decision Support.

[42] A. Kanso, H. Yahyaoui, and M. Almulla, "Keyed hash function based on a chaotic map," *Information Sciences*, vol. 186, no. 1, pp. 249 – 264, 2012.

[43] R. L. Rivest, "The md5 message-digest algorithm," Master's thesis, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992.

[44] HL7, "Health level seven implementation support guide," tech. rep., Health Level Seven International, 1998.

[45] P. d. C. Jorge Henriques, "Informática médica - health level seven," Master's thesis, DEI - Universidade de Coimbra, Outubro 2004.

[46] T. Carlson, "Information security management: Understanding iso 17799," tech. rep., Member of Consulting Staff, CISSP, September 2001.

[47] M. Filip, P. Linzer, F. mal, R. Herzig, and D. A. koloud, "Medical consultations and the sharing of medical images involving spinal injury over mobile phone networks," *The American Journal of Emergency Medicine*, vol. 30, no. 6, pp. 961 – 965, 2012.

[48] N. Malheiros, E. Madeira, F. Verdi, and M. Magalhães, "Managing layer 1 vpn services," *Optical Switching and Networking*, vol. 5, no. 4, pp. 196 – 218, 2008.

[49] CNPD, "Lei n.º 67/98 de 26 de outubro - lei da protecção de dados pessoais," tech. rep., Comissão Nacional de Protecção de Dados, Outubro 1998.

[50] A. Gerra, "Relatório de auditoria ao tratamento de informação de saúde nos hospitais," tech. rep., Comissão Nacional de Protecção de Dados, 2004.

[51] Lei.12/2005, "Lei nº 12/2005 de 26 de janeiro - informação genética pessoal e informação de saúde," tech. rep., 2005.

[52] J. van der Peijl, J. Klein, C. Grass, and A. Freudenthal, "Design for risk control: The role of usability engineering in the management of use-related risks," *Journal of Biomedical Informatics*, vol. 45, no. 4, pp. 795 – 812, 2012. Translating Standards into Practice: Experiences and Lessons Learned in Biomedicine and Health Care.

[53] I. Maglogiannis, E. Zafiropoulos, A. Platis, and C. Lambrinoudakis, "Risk analysis of a patient monitoring system using bayesian network modeling," *Journal of Biomedical Informatics*, vol. 39, no. 6, pp. 637 – 647, 2006.

[54] ISO..14971:2007, "Medical devices - application of risk management to medical devices," tech. rep., ISO, 2007.

[55] D. H. Stamatis, *Failure Mode and Analysis: FMEA from theory to execution.*, vol. Second Edition. Milwaukee, 2003.

[56] M. R. B. Bobin E. McDermott, Raymond J. Mikulak, *The basics of FMEA*. Taylor e Francis Group, 2009.

[57] M. D. D. de Araújo, "Melhoria da qualidade na concepção e desenvolvimento do produto," Master's thesis, UNIVERSIDADE FEDERAL DE SÃO CARLOS, Setembro 2011.

[58] E. C. D. S. VIEIRA, "Metodologia fmea análise de modo e efeitos de falha e orientações estratégicas," Master's thesis, UNIVERSIDADE FEDERAL DE SÃO CARLOS, 2008.

[59] "Fmea methodology design, implementation and integration with haccp system in a food company," *Food Control*, vol. 13, no. 8, pp. 495 – 501, 2002.

[60] L. Rosen, *Open Source Licensing Software Freedom and Intellectual Property Law*. Prentice Hall Professional Technical Reference, second ed., 2005.

[61] F. F. S. Foundation, "Gnu general public license, version 3." June 2007.

[62] F. L. F. de Almeida, "Empreendedorismo de software livre," Master's thesis, Faculdade de Engenharia da Universidade do Porto, Porto, Maio 2006.

[63] O. O. S. Initiative, "Eclipse public license -v 1.0.".

[64] L. M. R. Vieira, "Mis - medical image servise," Master's thesis, Instituto Superior de Engenharia do Porto, 2011.

[65] M. Alexandre and M. Norberto, "Desenvolvimento da aplicação medical image service," Master's thesis, Instituto Superior de Engenharia do Porto, 2011.

[66] W. V. K. Hamzeh, G. Pall, "Point-to-point tunneling protocol (pptp)." 1999.

[67] S. C. Araújo, "Segurança na circulação de informação clínica," Master's thesis, Faculdade de Engenharia da Universidade do Porto, Março 2007.

Apêndice A

Anexos

A.1 Requisitos Essenciais

Requisitos essenciais de um dispositivo médico - Diretiva 93/42/CEE na sua atual redação
(Decreto-lei nº 145/2009, na sua atual redação)

	Aplicável	
	Sim 1) Método(s) encontrado(s) para garantir cumprimento (indicar qual(is)) 2) Documento(s) do SGQ relacionado(s)	**Não** 1) Justificação
Grupo I - Requisitos gerais		
1.2.1 A redução, na medida do possível, dos riscos derivados de erros de utilização devido às características ergonómicas do dispositivo ou ao ambiente que está previsto para a utilização do produto (conceção tendo em conta a segurança do doente);	1) Concep-«o 2) ISO 9001:2008	
1.2.2 A consideração dos conhecimentos técnicos, da experiência, da educação e da formação e, se for caso disso, das condições clínicas e físicas dos utilizadores previstos (conceção para utilizadores não profissionais, profissionais, portadores de deficiência ou outros utilizadores);	1) Concep-«o 2) ISO 9001:2008	
2.1 Eliminar ou reduzir os riscos ao mínimo possível (conceção e construção intrinsecamente seguras);	**1) Gest«o de Risco** **2) Concep-«o**	
2.2 Quando apropriado, adotar as medidas de proteção adequadas, incluindo, se necessário, sistemas de alarme para os riscos que não podem ser eliminados;		1) O software n«o precisa de medidas de prote-«o.
2.3 Informar os utilizadores dos riscos residuais devidos a insuficiências nas medidas de proteção adotadas.		1) O software n«o presisa de medidas de prote-«o.
3 Os dispositivos devem atingir os níveis de adequação que lhes		

tiverem sido atribuídos pelo fabricante e ser concebidos, fabricados e acondicionados por forma a poderem desempenhar uma ou mais das funções previstas na alínea u) do artigo 3.º do decreto-lei de que o presente anexo é parte integrante, de acordo com as especificações do fabricante.	1) Concep- «o 2) ISO 9001:2008	
4 As características e os níveis de funcionamento referidos nos n.os 1 a 3 do presente anexo não devem ser alterados sempre que as alterações possam comprometer o estado clínico e a segurança dos doentes e, eventualmente, de terceiros, durante a vida útil dos dispositivos prevista pelo fabricante, quando submetidos ao desgaste decorrente das condições normais de utilização.	1) O software nao tem tempo de vida definido. 2) Conce- «o.	
5 Os dispositivos devem ser concebidos, fabricados e acondicionados de modo que as suas características e níveis de funcionamento, em termos da utilização prevista, não sofram alterações no decurso do armazenamento e do transporte, tendo em conta as instruções e informações fornecidas pelo fabricante.	1) Manual de utilizador.	
6.1 A demonstração da conformidade com os requisitos essenciais deve incluir uma avaliação clínica nos termos do anexo XVI.		**1) Deve proceder de acordo com o Anexo VII, n«o com o Anexo XVI.**
Grupo II - Requisitos relativos à conceção e ao fabrico		
Propriedades químicas, físicas e biológicas		
7.1.1 A seleção dos materiais utilizados, nomeadamente no que respeita à toxicidade e, se for caso disso, à inflamabilidade;		1) Software, no tem propriedades f²sicas, qu²micas ou biol· gicas.
7.1.2 A compatibilidade recíproca entre os materiais utilizados e os tecidos, as células biológicas e os líquidos corporais, atendendo à finalidade do dispositivo;		"
7.1.3 Sempre que aplicável, os resultados das investigações biofísicas ou de modelos cuja validade tenha sido previamente demonstrada.		"

7.2 Os dispositivos devem ser concebidos, fabricados e acondicionados por forma a minimizar os riscos relativos a contaminantes e resíduos no que respeita ao pessoal envolvido no transporte, armazenamento e utilização, bem como no que se refere aos doentes, tendo em conta a finalidade do produto, devendo ser prestada especial atenção aos tecidos expostos, bem como à duração e frequência da exposição.		"
7.3 Os dispositivos devem ser concebidos e fabricados por forma a poderem ser utilizados em segurança com os materiais, substâncias ou gases com que entrem em contacto no decurso da sua utilização normal ou de processos de rotina e, caso se destinem à administração de medicamentos, devem ser concebidos e fabricados de modo a serem compatíveis com os medicamentos em questão, de acordo com as disposições e restrições que regem esses produtos, de modo que o seu nível de adequação se mantenha conforme à finalidade prevista.		"
7.4 Quando um dispositivo inclua, como parte integrante, uma substância que, quando utilizada separadamente, possa ser considerada um medicamento nos termos do Decreto-Lei n.º 176/2006, de 30 de agosto, que procedeu à transposição da Diretiva n.º 2001/83/CE, do Parlamento Europeu e do Conselho, de 6 de novembro, e possa ter efeitos sobre o corpo humano através de uma ação acessória à do dispositivo, deve-se verificar a qualidade, segurança e utilidade da substância, de forma análoga aos métodos previstos no anexo I da Diretiva n.º 2001/83/CE, do Parlamento Europeu e do Conselho, de 6 de novembro (anexo I do Decreto-Lei n.º 176/206, de 30 de agosto).		"
7.7 Os dispositivos devem ser concebidos e fabricados por forma a		

reduzirem a um mínimo os riscos colocados pela libertação de substâncias do dispositivo, devendo ser concedida especial atenção a substâncias cancerígenas, mutagénicas ou tóxicas para a reprodução, em conformidade com o anexo I da Diretiva 67/548/CEE, do Conselho, de 27 de junho, relativa à aproximação das disposições legislativas, regulamentares e administrativas respeitantes à classificação, embalagem e rotulagem das substâncias perigosas. (Decreto-Lei n.º 280-A/87, de 17 de julho, que estabelece medidas relativas à notificação de substâncias químicas e à classificação, embalagem e rotulagem de substâncias perigosas; Decreto-Lei n.º 82/95, de 22 de abril, que transpõe para a ordem jurídica interna várias diretivas que alteram a Diretiva n.º 67/548/CEE, do Conselho, de 27 de junho, relativa à aproximação das disposições legislativas, regulamentares e administrativas respeitantes à classificação, embalagem e rotulagem de substâncias perigosas; Portaria n.º 732-A/96, de 11 de novembro, que aprova o Regulamento para a Notificação de Substâncias Químicas e para a Classificação, Embalagem e Rotulagem de Substâncias Perigosas.)		"
7.7.1 No caso de partes do dispositivo (ou o próprio dispositivo) destinadas a administrar medicamentos, líquidos corporais ou outras substâncias no corpo humano e, ou, a removê-las do corpo humano, ou dispositivos destinados ao transporte e ao armazenamento desses fluidos ou substâncias corporais, contenham ftalatos que sejam classificados como cancerígenos, mutagénicos ou tóxicos para a reprodução, da categoria 1 ou 2, em conformidade com o anexo I da Diretiva n.º 67/548/CEE, do Conselho, de 27 de junho, deve ser aposta na rotulagem do próprio dispositivo e ou na embalagem de cada		"

unidade ou, se for caso disso, na embalagem de venda, uma indicação de que se trata de um dispositivo que contém ftalatos.		
7.7.2 Se a utilização pretendida desses dispositivos incluir o tratamento de crianças ou o tratamento de mulheres grávidas ou em aleitamento, o fabricante deve fornecer uma justificação específica para a utilização dessas substâncias no que se refere ao cumprimento dos requisitos essenciais, nomeadamente dos constantes no presente número e nos n.os 7.7 e 7.7.1, na documentação técnica e nas instruções de utilização sobre os riscos residuais para estes grupos de doentes e, se for caso disso, as medidas de precaução adequadas.		"
7.8 Os dispositivos devem ser concebidos e fabricados por forma a reduzir ao mínimo os riscos derivados da introdução não intencional de substâncias no dispositivo, tendo em conta o próprio dispositivo e a natureza do meio em que se destina a ser utilizado.		"
Infeção e contaminação microbiana		
8.1 Os dispositivos e os respetivos processos de fabrico devem ser concebidos por forma a eliminar ou reduzir, tanto quanto possível, o risco de infeção para o doente, utilizador ou para terceiros, permitir a sua fácil manipulação e, se for caso disso, minimizar a contaminação do dispositivo pelo doente, e vice-versa, no decurso da utilização.		1) Software, n«o tem propriedades f²sicas, qu²micas ou biol· gicas.
8.2 Os tecidos de origem animal devem ser provenientes de animais que tenham sido submetidos a controlos veterinários e a medidas de fiscalização adequadas à utilização prevista para os tecidos, devendo os organismos notificados recolher e manter a informação sobre a origem geográfica dos animais.		"
8.3 Os dispositivos que são fornecidos estéreis devem ser concebidos, fabricados e acondicionados numa embalagem descartável e, ou, em		"

conformidade com procedimentos adequados, por forma a estarem estéreis aquando da sua colocação no mercado e a manterem este estado nas condições previstas de armazenamento e transporte até que seja violada ou aberta a proteção que assegura a esterilidade.		
8.4 Os dispositivos fornecidos estéreis devem ter sido fabricados e esterilizados segundo o método apropriado e validado.		"
8.5 Os dispositivos destinados a serem esterilizados devem ser fabricados em condições, nomeadamente de caráter ambiental, adequadas e controladas.		"
8.6 Os sistemas de embalagem para dispositivos não estéreis devem conservar o produto sem deterioração do grau de limpeza previsto e, caso se destinem a ser esterilizados antes da utilização, devem minimizar o risco de contaminação microbiana, bem como adequar-se ao método de esterilização indicado pelo fabricante.		"
8.7 A embalagem e rotulagem do dispositivo deve permitir distinguir produtos idênticos e análogos vendidos sob a forma esterilizada e não esterilizada.		"
Propriedades relativas ao fabrico e condições ambientais		
9.1 Caso um dispositivo se destine a ser utilizado em conjunto com outros dispositivos ou equipamentos, esse conjunto, incluindo o sistema de ligação, deve ser seguro e não prejudicar os níveis de funcionamento previstos, devendo qualquer restrição à utilização ser especificada na rotulagem ou nas instruções.		1) Software, no tem propriedades f²sicas, qu²micas ou biol· gicas.
9.2.1 Os riscos de lesão devidos às suas características físicas, incluindo a relação pressão-volume, e às suas características dimensionais e, eventualmente, ergonómicas;		"
9.2.2 Os riscos decorrentes de condições ambientais razoavelmente		"

previsíveis, nomeadamente campos magnéticos, influências elétricas externas, descargas eletrostáticas, pressão, temperatura ou variações de pressão e de aceleração;		
9.2.3 Os riscos de interferência recíproca com outros dispositivos normalmente utilizados nas investigações ou para um determinado tratamento;		"
9.2.4 Os riscos resultantes do envelhecimento dos materiais utilizados ou da perda de precisão de qualquer mecanismo de medição ou de controlo, quando não seja possível a manutenção ou calibração (como no caso dos dispositivos implantáveis).		"
9.3 Os dispositivos devem ser concebidos e fabricados por forma a minimizar os riscos de incêndio ou explosão em condições normais de utilização ou em situação de primeira avaria, devendo prestar-se especial atenção aos dispositivos cuja utilização implique a exposição a substâncias inflamáveis ou a substâncias suscetíveis de favorecer a combustão.		"
Dispositivos com função de medição		
10.1 Os dispositivos com funções de medição devem ser concebidos e fabricados por forma a assegurarem uma suficiente constância e exatidão das medições dentro de limites adequados, atendendo à finalidade dos dispositivos, e indicados pelo fabricante.		1) O software n«o tem fun-»es de medi-«o.
10.2 A escala de medição, de controlo e de leitura deve ser concebida de acordo com princípios ergonómicos e atendendo à finalidade dos dispositivos.		"
10.3 As medições feitas por dispositivos com funções de medição devem ser expressas em unidades legais, em conformidade com o disposto na legislação aplicável.		"

Proteção contra radiações		
11.1 Os dispositivos são concebidos e fabricados por forma a reduzir ao nível mínimo compatível com o objetivo pretendido a exposição dos doentes, dos utilizadores e de terceiros à emissão de radiações, sem no entanto restringir a aplicação das doses prescritas como apropriadas para efeitos terapêuticos ou de diagnóstico.		1) O software n«o emite radia-»es.
11.2 No caso dos dispositivos concebidos para emitir níveis de radiações com um objetivo médico específico, cujo benefício se considere ser superior aos riscos inerentes à emissão, deve ser possível ao utilizador controlar as radiações, devendo tais dispositivos ser concebidos e fabricados por forma a garantir a reprodutibilidade dos parâmetros variáveis e as respetivas tolerâncias.		"
11.3 Os dispositivos que se destinam a emitir radiações visíveis ou invisíveis potencialmente perigosas devem ser equipados, sempre que possível, com indicadores visuais ou sonoros de tais emissões.		"
11.4 Os dispositivos devem ser concebidos e fabricados por forma a reduzir o mais possível a exposição de doentes, utilizadores e terceiros à emissão de radiações não intencionais, parasitas ou difusas.		"
11.5 As instruções de utilização dos dispositivos que emitem radiações devem conter informações pormenorizadas sobre a natureza das radiações emitidas, os meios de proteção do paciente e do utilizador, a maneira de evitar manipulações erróneas e eliminar os riscos inerentes à instalação.		"
11.6 Os dispositivos destinados a emitir radiações ionizantes devem ser concebidos e fabricados por forma a garantir que, sempre que possível, a quantidade, a geometria e a qualidade da radiação emitida possam ser reguladas e controladas em função da finalidade.		"

11.6.1 Os dispositivos que emitem radiações ionizantes destinados ao diagnóstico radiológico devem ser concebidos e fabricados por forma a proporcionar uma imagem adequada e, ou, de qualidade para os fins médicos pretendidos, embora com uma exposição às radiações tão baixa quanto possível, tanto do doente como do utilizador.		"
11.6.2 Os dispositivos que emitem radiações ionizantes destinados à radioterapia devem ser concebidos e fabricados por forma a permitir a supervisão e um controlo fiáveis da dose administrada, do tipo e energia do feixe e, se for caso disso, da qualidade da radiação.		"
Dispositivos médicos ligados a uma fonte de energia ou que dela disponham como equipamento		
12.1 Os dispositivos que integrem sistemas eletrónicos programáveis devem ser concebidos de modo a garantir a recetibilidade, a fiabilidade e o nível de funcionamento desses sistemas, de acordo com a respetiva finalidade, devendo, em caso de avaria, ser adotadas medidas adequadas para eliminar, ou reduzir tanto quanto possível, os riscos que dela possam advir, sendo que no respeitante a dispositivos que incorporem um software ou que sejam eles próprios um software com finalidade médica, este deve ser validado de acordo com o estado da técnica, tendo em consideração os princípios do ciclo de vida, do desenvolvimento, da gestão dos riscos, da validação e da verificação.		1) Software
12.2 Os dispositivos que integram uma fonte de energia interna de que dependa a segurança do doente devem dispor de meios que permitam determinar o estado dessa fonte.		
12.3 Os dispositivos ligados a uma fonte de energia externa de que dependa a segurança do doente devem dispor de um sistema de alarme que indique qualquer eventual falta de energia.		1) N«o entrevem diretamente com o doente.

12.4 Os dispositivos destinados à fiscalização de um ou mais parâmetros clínicos de um doente devem dispor de sistemas de alarme adequados que permitam alertar o utilizador para situações suscetíveis de provocar a morte ou uma deterioração grave do estado da saúde do doente.		1) O efficiencia sysPACS não provoca morte em situação alguma.
12.5 Os dispositivos devem ser concebidos e fabricados por forma a minimizar os riscos decorrentes da criação de campos eletromagnéticos suscetíveis de afetar o funcionamento de outros dispositivos ou equipamentos instalados no meio ambiente.		1) O efficiencia sysPACS não cria campos magnéticos.
• **Proteção contra riscos elétricos**		
12.6 Os dispositivos devem ser concebidos e fabricados por forma a evitar, tanto quanto possível, os riscos de choques elétricos não intencionais em condições normais de utilização e em situações de primeira avaria, desde que os dispositivos estejam corretamente instalados.		1) Software
• **Proteção contra riscos mecânicos e térmicos**		
12.7.1 Os dispositivos devem ser concebidos e fabricados por forma a proteger o doente e o utilizador contra riscos mecânicos relacionados, por exemplo, com a resistência, a estabilidade e as peças móveis.		1) O software n«o tem caracter²sticas mec©nicas ou t®rmicas.
12.7.2 Os dispositivos devem ser concebidos e fabricados por forma a minimizar, na medida do possível, os riscos decorrentes das vibrações por eles produzidas, atendendo ao progresso técnico e à disponibilidade de redução das vibrações, especialmente na fonte, exceto no caso de as vibrações fazerem parte do funcionamento previsto.		"
12.7.3 Os dispositivos devem ser concebidos e fabricados por forma a minimizar, na medida do possível, os riscos decorrentes do ruído		"

produzido, atendendo ao progresso técnico e à disponibilidade de meios de redução do ruído produzido, designadamente na fonte, exceto no caso de as emissões sonoras fazerem parte do funcionamento previsto.		
12.7.4 Os terminais e dispositivos de ligação às fontes de energia elétrica, hidráulica, pneumática ou gasosa que devam ser manipulados pelo utilizador devem ser concebidos e construídos por forma a minimizar os riscos eventuais.		"
12.7.5 Em condições normais de utilização, as partes acessíveis dos dispositivos, excluindo as partes ou zonas destinadas a fornecer calor ou atingir determinadas temperaturas e o meio circundante, não devem atingir temperaturas suscetíveis de constituir perigo nas condições normais de utilização.		"
• **Proteção contra os riscos inerentes ao fornecimento de energia ou administração de substâncias aos doentes**		
12.8.1 A conceção e a construção dos dispositivos destinados a fornecer energia ou administrar substâncias aos doentes devem permitir que o débito seja regulado e mantido com precisão suficiente para garantir a segurança do doente e do utilizador.		1) O software n«o fornece energia ou administra subst©ncias.
12.8.2 Os dispositivos devem ser dotados de meios que permitam impedir e, ou, assinalar qualquer deficiência no débito que seja suscetível de constituir um perigo, devendo os dispositivos incorporar sistemas adequados que permitam, tanto quanto possível, evitar que os débitos de energia e, ou, substâncias fornecidos pela respetiva fonte de alimentação atinjam, acidentalmente, níveis perigosos.		"
12.8.3 A função dos comandos e indicadores deve encontrar-se claramente indicada nos dispositivos e, sempre que um dispositivo		"

contenha instruções de funcionamento ou indique parâmetros de funcionamento ou de regulação através de um sistema visual, essas informações devem ser claras para o utilizador e, se for caso disso, para o doente.		
Informações fornecidas pelo fabricante		
13.1 Cada dispositivo deve ser acompanhado das informações necessárias para a sua correta utilização e com segurança e para a identificação do fabricante, tendo em conta a formação e os conhecimentos dos potenciais utilizadores, devendo essas informações ser constituídas pelas indicações constantes da rotulagem e do folheto de instruções.	1) Manual do Utilizador 2) Concepção	
13.2 As informações necessárias para a utilização do dispositivo com toda a segurança devem figurar, se exequível e adequado, no próprio dispositivo e, ou, na embalagem individual, ou, eventualmente, na embalagem comercial, mas, se os dispositivos não puderem ser embalados individualmente, as informações devem constar de um folheto de instruções que acompanhe um ou mais dispositivos.	1) Manual do Utilizador 2) Concepção	
13.3 Todos os dispositivos devem ser acompanhados de um folheto de instruções, incluído nas respetivas embalagens, sem prejuízo da possibilidade de, a título excecional, o referido folheto de instruções não ser incluído para dispositivos das classes I e IIa, desde que a respetiva segurança de utilização possa ser garantida sem ele.	1) Manual do Utilizador 2) Concepção	
13.4 Sempre que adequado, as informações devem ser apresentadas sob a forma de símbolos, os quais, bem como as respetivas cores de identificação, devem estar em conformidade com as normas harmonizadas, ou devem ser descritos na documentação que acompanha o dispositivo, nos domínios em que não existam quaisquer		1)Software, não é adequado a utilização de símbolos.

normas.		
• **Rotulagem**		
13.5.1 O nome, ou a firma e o endereço do fabricante, sendo que, relativamente aos dispositivos importados para serem distribuídos na União Europeia, o rótulo, a embalagem exterior ou as instruções de utilização devem ainda incluir o nome e o endereço do mandatário do fabricante, sempre que o fabricante não dispuser de sede social na União Europeia;	1) Manual de Utilizador Manual de Técnico 2) Concepção	
13.5.2 As informações estritamente necessárias para que o utilizador possa identificar o dispositivo e o conteúdo da embalagem, em especial para os utilizadores;	1) Manual de Utilizador Manual de Técnico 2) Concepção	
13.5.3 Se aplicável, a menção «Estéril»;		1) Não aplicável, software
13.5.4 Se aplicável, o código do lote, precedido da menção «Lote», ou o número de série;		1) Não aplicável, software
13.5.5 Se aplicável, a data limite de utilização do dispositivo em condições de segurança, expressa pelo ano e mês;		1) Não aplicável, software
13.5.6 Sempre que aplicável, uma indicação de que o dispositivo é para utilização única, sendo que a indicação do fabricante sobre a utilização única deve ser uniforme em toda a União Europeia;		1) Não aplicável, software
13.5.7 Para os dispositivos feitos por medida, a menção «Dispositivo feito por medida»;		1) Não aplicável, software
13.5.8 Para os dispositivos destinados à investigação clínica, a menção «Exclusivamente para investigação clínica»;		1) Não aplicável
13.5.9 Condições especiais de armazenamento e, ou, manuseamento;		1) Não aplicável
13.5.10 Instruções particulares de utilização;		1) Não aplicável
13.5.11 Advertências ou precauções a tomar;		1) Não aplicável
13.5.12 O ano de fabrico para os dispositivos ativos não abrangidos no		1) Não aplicável

n.º 13.5.5 supra, indicação que pode ser incluída no número do lote ou de série;		
13.5.13 Se aplicável, o método de esterilização;		1) Não aplicável, software
13.5.14 No caso de um dispositivo na aceção do disposto na alínea b) do n.º 2 do artigo 2.º do decreto-lei de que o presente anexo é parte integrante, a menção de que o dispositivo incorpora como parte integrante uma substância derivada do sangue humano.		1) Não aplicável, software
13.6 Caso a finalidade prevista de um dispositivo não seja evidente para o utilizador, o fabricante deve especificá-la claramente na rotulagem e nas instruções de utilização.		1) Não aplicável, software
13.7 Os dispositivos e os componentes destacáveis devem, se tal se justificar e for exequível, ser identificados em termos de lotes, por forma a possibilitar a realização de ações destinadas a detetar riscos ocasionados pelos dispositivos e pelos componentes destacáveis.		1) Não aplicável, software
• **Instruções de utilização**		
13.8.1 As indicações referidas no n.º 13.5, exceto as constantes dos n.os 13.5.4 e 13.5.5;	1) Manual do utilizador 2) Concepção	
13.8.2 Os níveis de adequação referidos no n.º 3, bem como quaisquer efeitos secundários indesejáveis;		1) Não aplicável, não provoca efeitos secundários.
13.8.3 Caso um dispositivo deva ser instalado em ou ligado a outros dispositivos ou equipamentos médicos, para funcionar de acordo com a finalidade prevista, devem ser fornecidos pormenores suficientes das suas características de modo a permitir identificar os dispositivos ou os equipamentos que devem ser utilizados para que se obtenha uma combinação segura;	1) Manual Técnico 2) Concepção	
13.8.4.1 As instruções de calibração e o manual de manutenção, sempre que aplicável aos produtos em causa;		1) Não aplicável, não necessita de calibração.

13.8.5 Se aplicável, informações úteis para evitar determinados riscos decorrentes da implantação do dispositivo;		1) Não aplicavel.
13.8.6 Informações relativas aos riscos de interferência recíproca decorrentes da presença do dispositivo aquando de investigação ou tratamentos específicos;		1) Não aplicavel.
13.8.7 As instruções necessárias em caso de danificação da embalagem que assegura a esterilidade e, se necessário, a indicação dos métodos adequados para se proceder a uma nova esterilização;		1) Não aplicavel.
13.8.8 Caso o dispositivo seja reutilizável, informações sobre os processos de reutilização adequados, incluindo a limpeza, desinfeção, acondicionamento e, se for caso disso, método de reesterilização, se o dispositivo tiver de ser novamente esterilizado, bem como quaisquer restrições quanto ao número possível de reutilizações;		1) Não aplicavel.
13.8.9 Caso os dispositivos sejam fornecidos com a condição de serem previamente esterilizados, as instruções relativas à limpeza e esterilização devem ser de molde a garantir que, se forem corretamente respeitadas, o dispositivo satisfaça os requisitos gerais referidos na secção i do presente anexo;		1) Não aplicavel.
13.8.10 Se o dispositivo indicar se destina a utilização única, informações sobre as características conhecidas e os fatores técnicos de que o fabricante tem conhecimento que podem constituir um risco no caso de o dispositivo ser novamente utilizado e, se em conformidade com o n.º 13.3, não sejam necessárias instruções de utilização, as informações devem ser facultadas ao utilizador, a seu pedido;		1) Não aplicavel.
13.8.11 Caso um dispositivo deva ser submetido a um tratamento ou operação adicional antes de ser utilizado (por exemplo, esterilização,		1) Não aplicavel.

montagem final, etc.), as indicações sobre esse tratamento ou operação;		
13.8.12 Caso um dispositivo emita radiações para fins médicos, as informações relativas à natureza, tipo, intensidade e distribuição das referidas radiações.		1) Não aplicável
13.9.1 As precauções a tomar em caso de alteração do funcionamento do dispositivo;	1) Manual de Utilizador, Manual Técnico. 2) Concepção	
13.9.2 As precauções a tomar no que respeita à exposição, em condições ambientais razoavelmente previsíveis, a campos magnéticos, a influências elétricas externas, a descargas eletrostáticas, à pressão ou às variações de pressão, à aceleração, a fontes térmicas de ignição, etc.;		1) Não aplicável
13.9.3 Informações adequadas sobre os medicamentos que o dispositivo em questão se destina a administrar, incluindo quaisquer limitações à escolha dessas substâncias;		1) Não aplicável
13.9.4 As precauções a tomar caso o dispositivo apresente um risco especial ou anormal no que respeita à sua eliminação;		1) Não aplicável
13.9.5 Os medicamentos ou as substâncias derivadas do sangue humano incorporados no dispositivo como sua parte integrante, em conformidade com os n.os 7.4 e 7.5;		1) Não aplicável
13.9.6 O grau de precisão exigido para os dispositivos de medição;		1) Não aplicável
13.9.7 A data da publicação ou da última revisão das instruções de utilização.	1) Manual de Utilizador 2) Concepção	

Nota: Os pontos referem-se ao Decreto-Lei nº 145/2009, Anexo I

Os métodos usados para cumprimento podem advir de:

a) conformidade com normas reconhecidas e/ou outras
b) conformidade com métodos de teste industriais comummente aceites
c) conformidade com método desenvolvido pela empresa
d) avaliação dos dados pré-clínicos e clínicos
e) comparação com dipositivo semelhante já disponível no mercado

A.2 Declaração de Conformidade

Declaração CE de Conformidade

(Dispositivos Médicos Classe I)

Nome do Fabricante ou do seu Mandatário estabelecido em Portugal:

_____

_____

Endereço ou Sede Social:

_____

_____

Declara:

Que o dispositivo que fabrica _____ (*designação genérica do produto ou família de produtos**), cumpre com os requisitos essenciais estabelecidos no Anexo I da Directiva 93/42/CEE, de 14 de Junho, na sua actual redacção e do Decreto-Lei nº145/2009, de 17 de Junho, que lhes são aplicáveis, pelo que não compromete o estado clínico nem a segurança dos doentes, nem, ainda, a segurança e a saúde dos utilizadores ou, eventualmente, de terceiros, quando utilizado nas condições e para os fins previstos, considerando-se que os eventuais riscos associados à utilização a que se destina constituem riscos aceitáveis quando comparados com o benefício proporcionado aos doentes e são compatíveis com um elevado grau de protecção da saúde e da segurança.

*Quando se designa a família de produtos, anexar à Declaração lista dos produtos abrangidos na família.

Compromete-se a:

- Criar e manter actualizado um processo de análise sistemática da experiência adquirida com os dispositivos na fase de pós- produção incluindo as disposições referidas no anexo XVI, do Decreto-lei nº 145/2009, de 17 de Junho.

- Desenvolver meios adequados para aplicação de quaisquer acções correctivas necessárias, tendo em conta a natureza e os riscos relacionados com o produto e a notificar a Autoridade Competente sobre os seus incidentes, tais como:

    - Qualquer disfunção, avaria ou deterioração das características ou do comportamento funcional, bem como qualquer imprecisão, omissão ou insuficiência na rotulagem ou nas instruções de utilização de um dispositivo, que sejam susceptíveis de causar ou ter causado a morte ou uma deterioração grave do estado de saúde de um doente, utilizador ou terceiro;

    - Qualquer dano indirecto, na sequência de uma decisão médica incorrecta, relacionada com um dispositivo médico, quando utilizado de acordo com as instruções de utilização fornecidas pelo fabricante;

    - Qualquer motivo de ordem técnica ou médica relacionado com as características ou com o comportamento funcional de um dispositivo que, pelas razões referidas nas alíneas anteriores, tenha conduzido a uma acção correctiva de segurança no mercado português dos dispositivos do mesmo tipo por parte do fabricante

    - Outras informações que a experiência demonstre deverem ser notificadas.

- Elaborar a documentação técnica e mantê-la actualizada, incluindo esta declaração, à disposição da Autoridade Competente para efeitos de inspecção durante cinco anos a contar da última data de fabrico do dispositivo médico.

Data: ____/_____/_____

Assinatura do Responsável

_____

A.3 Requerimento Avaliação da Conformidade

Minuta de requerimento para avaliação da conformidade

(Decreto Lei n.º 145/2009 na sua atual redação)

Exmo. Sr.
Presidente do Conselho Diretivo INFARMED I.P.
Organismo Notificado
Parque da Saúde de Lisboa
Avenida do Brasil, nº 53, Pav. 17-A
1749-004 Lisboa
Portugal

Fabricante / Representante legal: _____
Morada: _____
Localidade:_____
Código Postal: _____ - _____ _____
Telefone:_____ Fax: _____
E-mail: _____@ _____
Responsável técnico: _____

Dispositivos médicos a avaliar
Categoria:_____
Família:_____
Identificação: _____
Marca(s) Comercial(is): _____

Venho por este meio solicitar ao INFARMED, I.P., como Organismo Notificado, a avaliação de conformidade do(s) dispositivo(s) médico(s) supracitado(s), de classe ____ , de acordo com a(s) regra(s) de classificação _____ (menção da(s) regra(s) aplicada(s)), estabelecida(s) no anexo IX do Decreto-lei n.º 145/2009, na sua atual redação.

A avaliação da conformidade deverá ser efetuada de acordo com o Anexo ____ (procedimento de avaliação da conformidade escolhido) do referido diploma.

Requerente: _____
Data: ____/_____/_____

_____
(Assinatura do Requerente)

NOTA: Este requerimento deverá ser acompanhado do respetivo CD contendo a documentação técnica exigida para avaliação da conformidade do dispositivo e a declaração de compromisso.

A.4 Declaração de Compromisso

Declaração CE de conformidade e Declaração de compromisso

Dispositivo(s) médico(s): _____

Categoria(s):_____

Família:_____

Identificação do(s) dispositivo(s)*: _____

Marca comercial: _____

Para vários produtos, anexar à Declaração a lista dos produtos abrangidos.

Fabricante / Representante legal: _____

Responsável técnico: _____

Declaro que:

- Não foi apresentado a nenhum outro Organismo Notificado um requerimento equivalente, relativo ao mesmo sistema de qualidade, a que se refere(m) o(s) dispositivo(s) em análise.

- O(s) referido(s) dispositivo(s) médico(s) (contêm / não contêm) como parte integrante da sua constituição, uma das substâncias referidas nos nºs 7.4 e 7.5 do Anexo I do Decreto-Lei 145/2009.

- No fabrico do(s) dispositivo(s) (não) se utilizam tecidos de origem animal, tal como referidos na Diretiva nº 2003/32/CE, da Comissão, de 23 de abril e no capítulo VII do Decreto-Lei supra citado.

- O(s) dispositivo(s) cumpre(m) com os requisitos essenciais aplicáveis estabelecidos no anexo I do Decreto-lei supracitado, pelo que não põe(m) em risco a saúde e a segurança dos utilizadores desde que utilizado(s) de acordo com a finalidade para que foi(ram) concebido(s).

Comprometo-me a:

- Notificar o Organismo Notificado Infarmed, caso haja alguma modificação do produto após aprovação.

- A autorizar o Organismo Notificado a efetuar todas as inspeções necessárias e a fornecer-lhe todas as informações que me sejam solicitadas para que o Organismo Notificado possa assegurar-se da aplicação correta do sistema da qualidade aprovado ou a aprovar.

- A cumprir as obrigações decorrentes do sistema de qualidade aprovado, mantendo-o adequado e eficaz, não delegando nenhuma das funções relativas ao sistema de qualidade, tais como o tratamento de reclamações ou vigilância do dispositivo.

- A informar o Organismo Notificado de qualquer projeto de alterações introduzidas no sistema da qualidade aprovado ou da gama de produtos abrangidos.

- A criar e manter atualizado um processo de análise sistemática dos dados adquiridos com os dispositivos na fase de pós-produção e a desenvolver meios adequados de execução das ações corretivas necessárias tendo em conta a natureza e os riscos relacionados com o produto e os incidentes abaixo referidos:
  - qualquer deterioração das características e/ou do funcionamento de um dispositivo, bem como qualquer inadequação da rotulagem ou das instruções respeitantes a um dispositivo que sejam suscetíveis de causar ou ter causado a morte ou degradação grave do estado de saúde de um doente ou utilizador;

  - qualquer motivo de ordem técnica ou médica ligado às características ou ao funcionamento de um dispositivo pelas razões acima definidas que tenha ocasionado a retirada sistemática do mercado dos dispositivos do mesmo tipo;

- A informar a entidade com competência de fiscalização sobre as ocorrências acima referidas, assim que delas tiver conhecimento, bem como o Organismo Notificado.

Data: ____/_____/_____

_____

(Assinatura do Responsável técnico)

A.5 Manual de Utilizador

Manual Utilizador efficientia sysPACS

1. Índice

1. Índice
2. Introdução
3. Símbolos de Botões de Acção / Estado
4. Acessos e Autorizações
    4.1 Ecrã de entrada
    4.2 Autorizações de acesso
    4.3 Selector Preferências Pessoais
5. Módulo Administrador
    5.1. Selector Query/Retrive
    5.2. Selector Escala Médica
    5.3 Selector Info Sistema
    5.4. Selector Ferramentas Sistema
    5.5. Selector Definições Sistema
    5.6. Selector Definições DICOM
6. Módulo Médico
    6.1. Selector Lista de Trabalho
    6.2. Selector Relatório Tipo

2. Introdução

A solução **efficientia sysPACS** é um serviço *online* abrangente que permite gestão integrada do armazenamento e distribuição de imagens médicas para apoio ao diagnóstico.

O serviço tem como principais objectivos:

- Diminuir o tempo de diagnóstico do médico relator fornecendo-lhe ferramentas de diagnóstico, transcrição ou de gravação;
- Permitir ao utente, através de uma senha gerada no atendimento, aceder às imagens pela web fazendo o download do CD com um visualizador e o respectivo relatório.
-

Tem implementado um sistema de alertas e prioridades. Este sistema, através de uma escala médica, irá alertar o médico relator, via email ou por sms, dos estudos que tem de relatar ajudando-o a gerir melhor o seu tempo para diminuir o período de espera do diagnóstico em cada estudo.

O serviço permite a ligação à maioria dos sistemas já existentes no mercado uma vez que é compatível com as seguintes normas:

- DICOM 3.0;
- HL7 v2 ou v3.

3. Símbolos de Botões de Acção / Estado

Gerais


Selecção da linguagem da aplicação;


Sair da aplicação;


Visualizar conteúdo escondido;


Esconder conteúdo;


Efectuar visualização;


Escolher data;


Abrir visualizador Weasis;


Visualizar miniatura da imagem médica;


Gravar registo;


Editar registo;


Gravar registo editado;


Apagar Registo


Adicionar nova linha;


Anexar ficheiros ao estudo;


Estudo sem notas, ao clicar abre ecrã notas;


Estudo com notas, ao clicar abre ecrã notas;


Adicionar nota;


Editar nota;


Apagar nota;


Escrever relatório;


Pré-visualizar relatório;


Imprimir relatório em pdf;


Validar relatório;

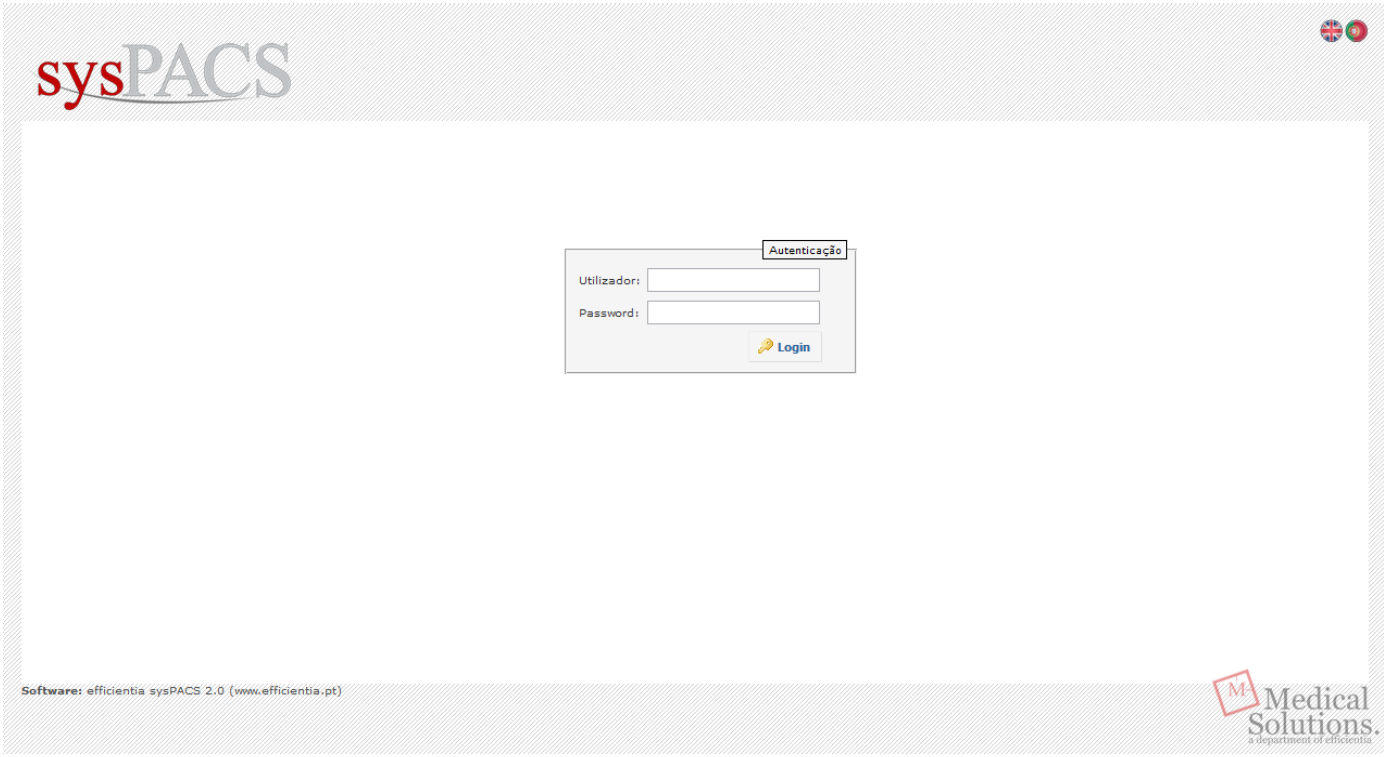

Cancelar validação do relatório;

Visualizar mais informações sobre o estudo;

4. Acessos e Autorizações

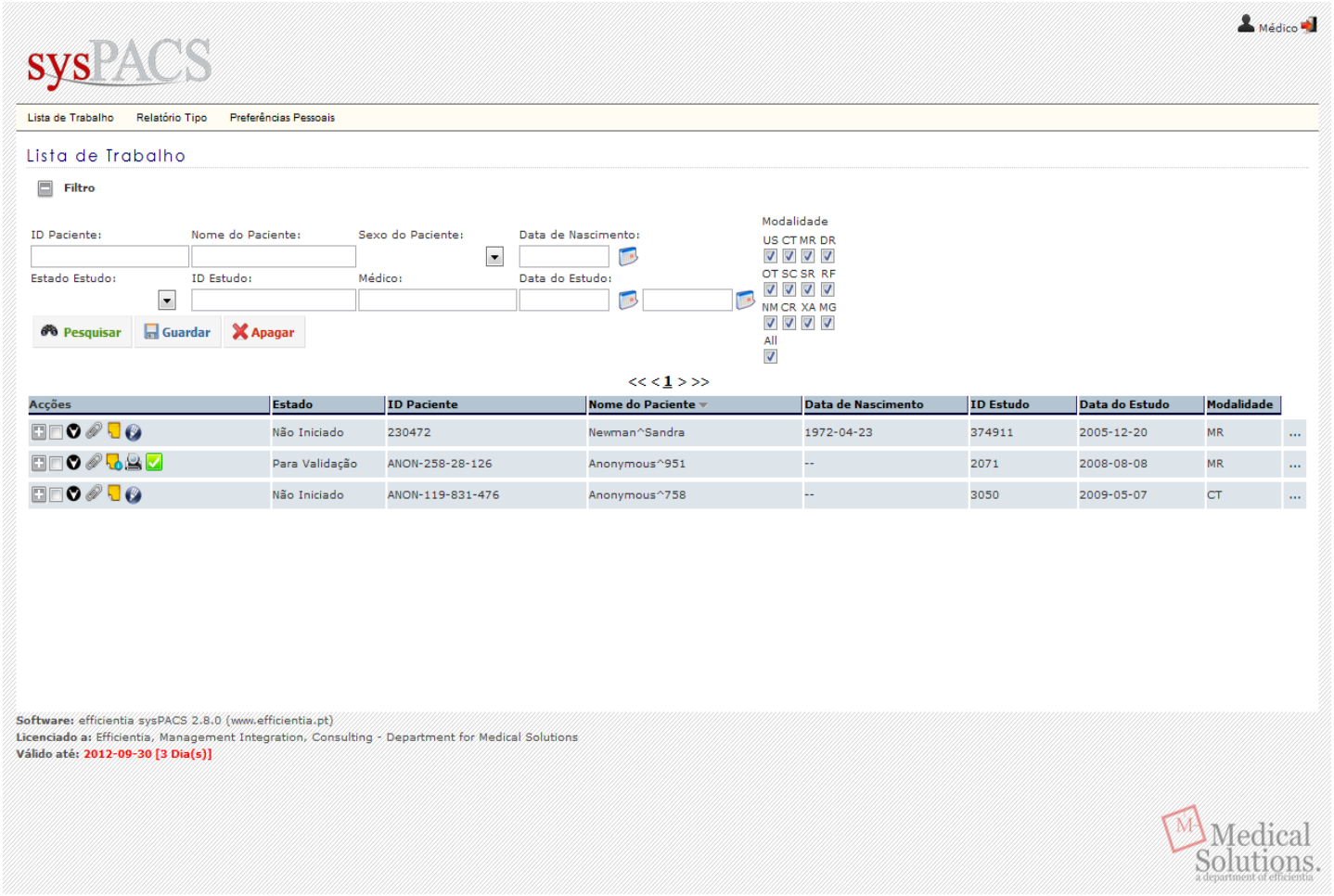
O acesso à aplicação pelo utilizador é efectuado através de um Browser (IE 7 ou superior ou Firefox versão 8 ou superior) disponível com leitor de pdf (Adobe Reader).
O link deverá ser atribuído pelo responsável do sistema informático e será do tipo *http:///192.168.1.200/ sysPACS.*
Efectuar o login com a inserção da password atribuída.

Entrada/login



4.1 Ecrã de entrada

O ecrã de entrada apresenta os selectores disponíveis e as respectivas opções, como no exemplo do Médico.

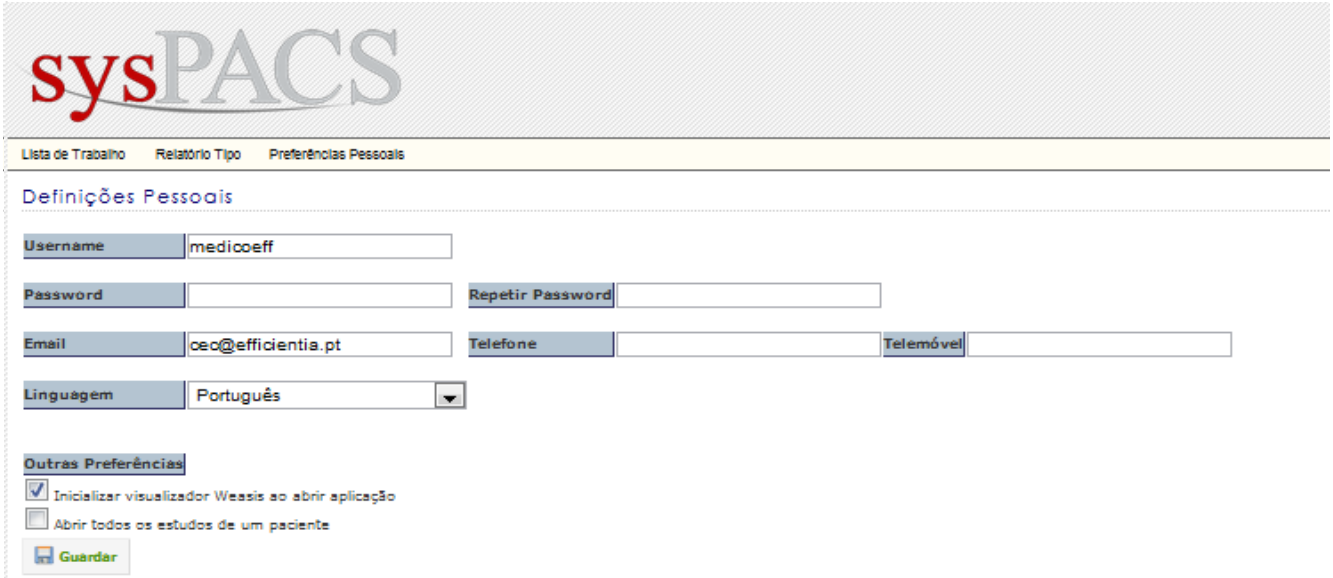


4.2 Autorizações de acesso

Existem 4 tipos de utilizadores que estarão disponíveis mediante os módulos adquiridos.

	Tipo	Acesso
4	Administrador	Administrador Global Cria utilizadores e atribui autorizações
3	Médico	Aceder aos estudos Relatar exames
2	Transcrição	Transcrever o relato
1	Recepção	Gere passwords dos utentes

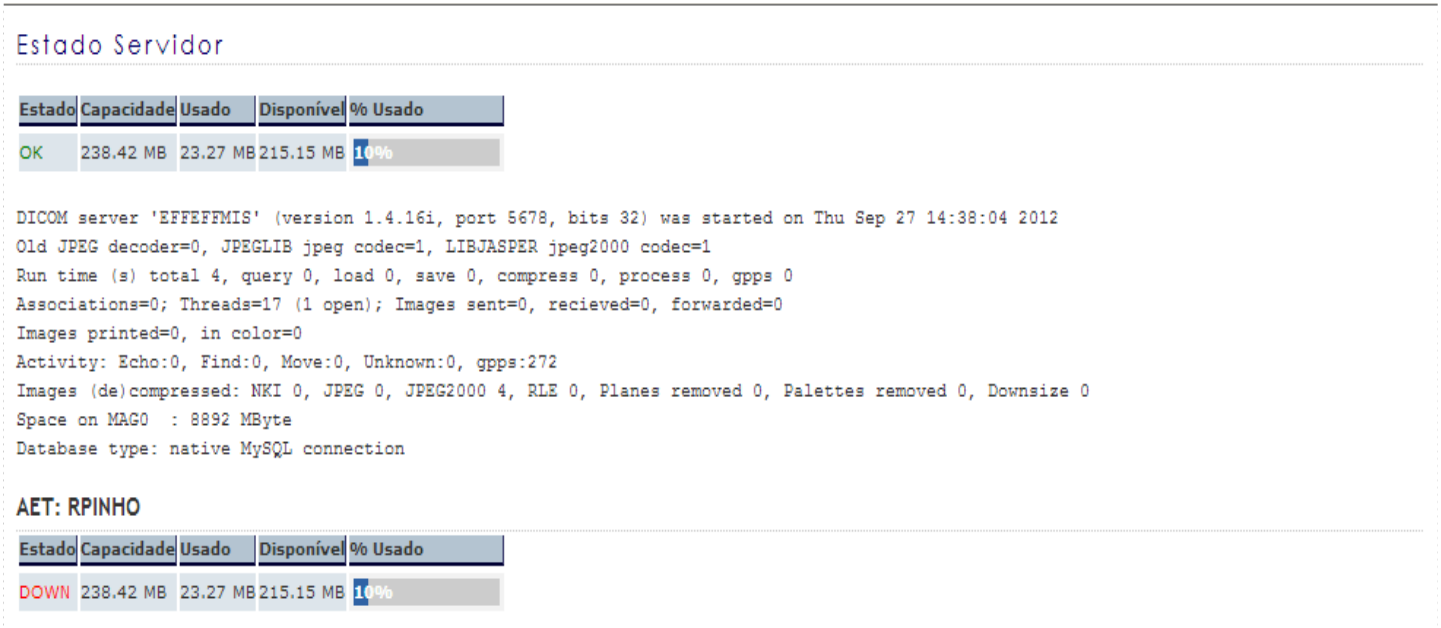
4.3 Selector Preferências Pessoais



Neste selector é possível alterar o “Username” e a “Password“ juntamente com outras informações pessoais. Nas opções “Outras Preferências” pode seleccionar a opção iniciar o visualizador ao abrir a aplicação, juntamente com a opção abrir todos os estudos do paciente.

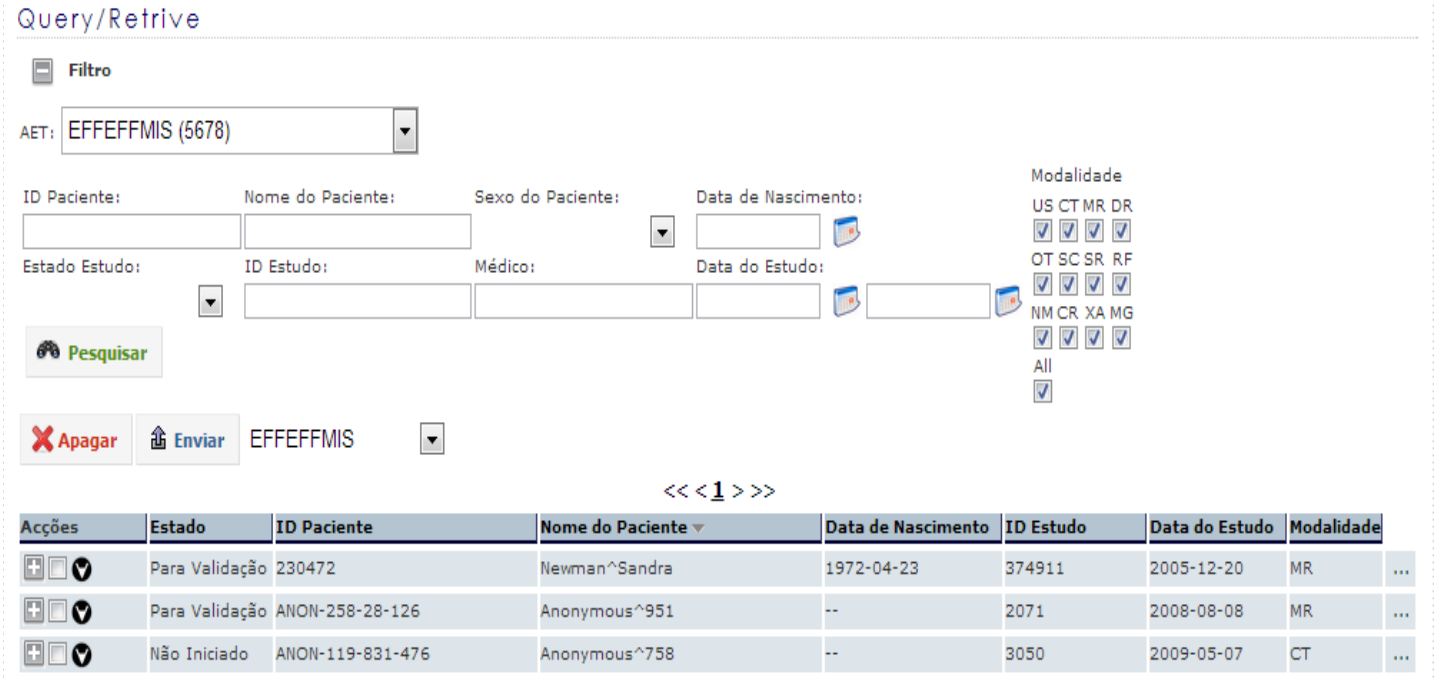
5. Módulo Administrador

Após a autenticação do utilizador do tipo administrador, será encaminhado para o ecrã “*Estado do Servidor*”, onde poderá ter uma rápida informação sobre o estado do PACS e armazenamento.



O ecrã anteriormente exibido, será explicado em pormenor posteriormente.

5.1. Selector Query/Retrive



O selector Query/Retrive permite enviar estudos para os nós DICOM configurados na aplicação, além de possibilitar apagar definitivamente os estudos do PACS.
Na parte superior do ecrã, encontra-se um filtro que permitirá pesquisar os estudos.

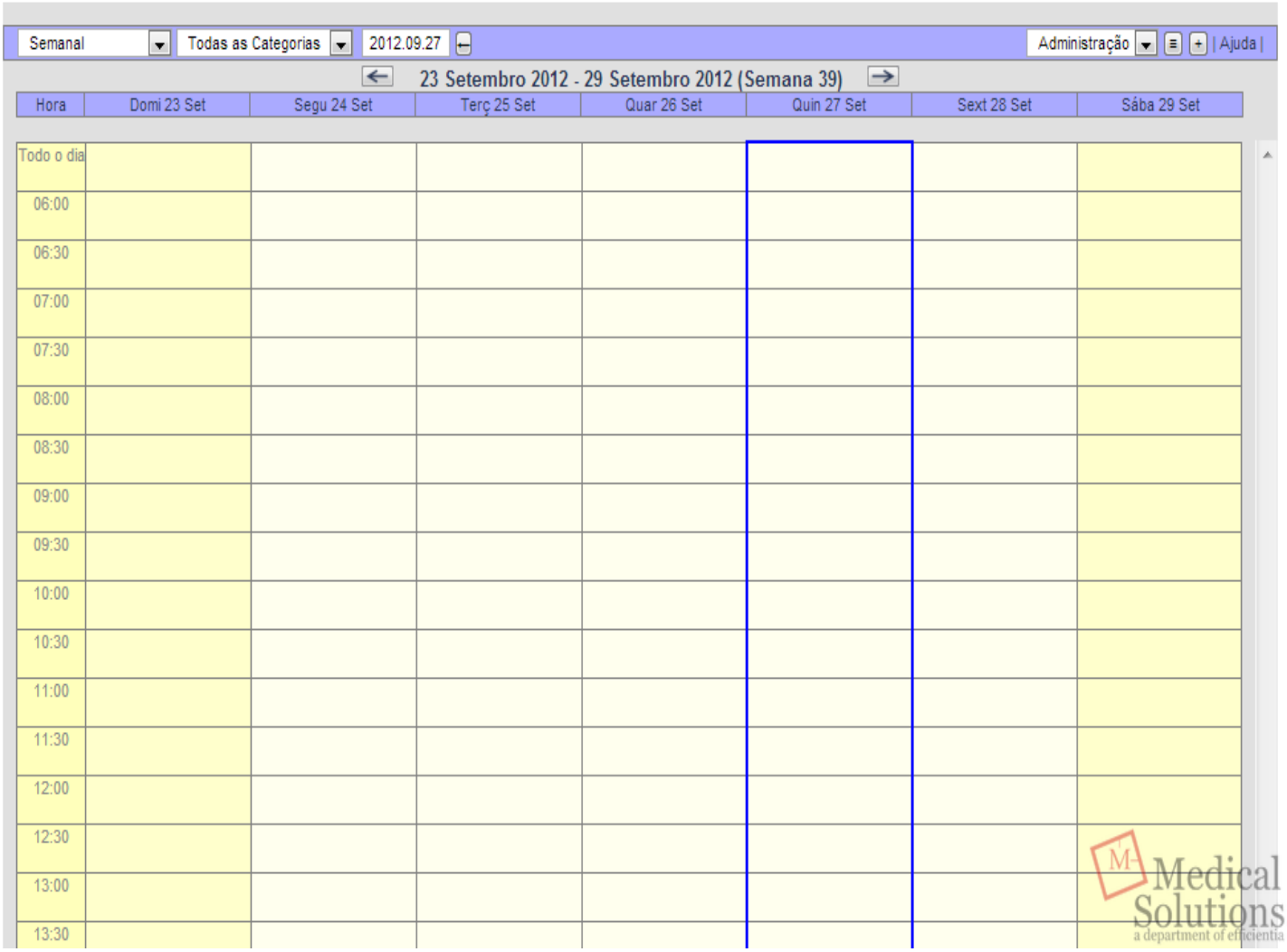
Campos disponíveis:
AET - Caso o cliente tenha adquirido o módulo "*Multiple AET*", irá aparecer um *select box* de forma a pesquisar os estudos associados a esse AET;
ID Paciente - Pesquisa pelo ID do paciente;
Nome do Paciente - Pesquisa pelos nomes dos pacientes similares ao introduzido;
Sexo do Paciente - Pesquisa pelo sexo do paciente;
Data de Nascimento - Pesquisa pela data de nascimento do paciente. A data poderá ser escolhida ou introduzida no formato (aaaa-mm-dd);
Estado Estudo - Pesquisa pelo estado do estudo;
ID Estudo - Pesquisa pelo ID do estudo;
Médico - Pesquisa pelos nomes dos médicos referência similares ao introduzido;
Data do Estudo - Pesquisa de intervalo pela data de realização do estudo. A data poderá ser escolhida ou introduzida no formato (aaaa-mm-dd);
Modalidade - Pesquisa dos estudos pelas modalidades:

Para executar uma acção de apagar, deverá seleccionar o estudo na *checkbox* e clicar no botão Apagar.

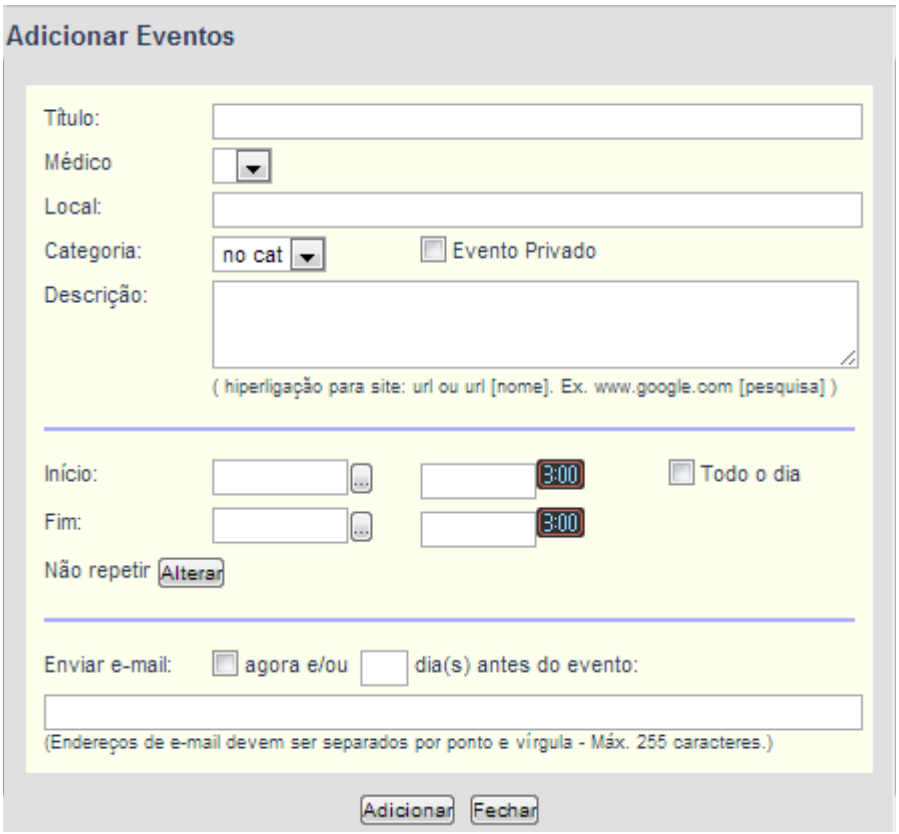
Para executar uma acção de envio do estudo seleccionado, deverá seleccionar o estudo, escolher no nó DICOM na *select box* e clicar em Enviar.

Além das acções descritas anteriormente, será também possível abrir um estudo através do visualizador Weasis, além de ser possível visualizar as miniaturas das imagens do estudo, usando a imagem .

5.2. Selector Escala Médica



O ecrã escala médica é importante para os clientes que têm activo o módulo de alertas e prioridades. Neste ecrã é possível visualizar, criar e editar a escala médica do médico relator de serviço, para que este seja notificado automaticamente assim que receber um estudo para relatar.
Para adicionar um bloco de tempo, deverá clicar no botão +.



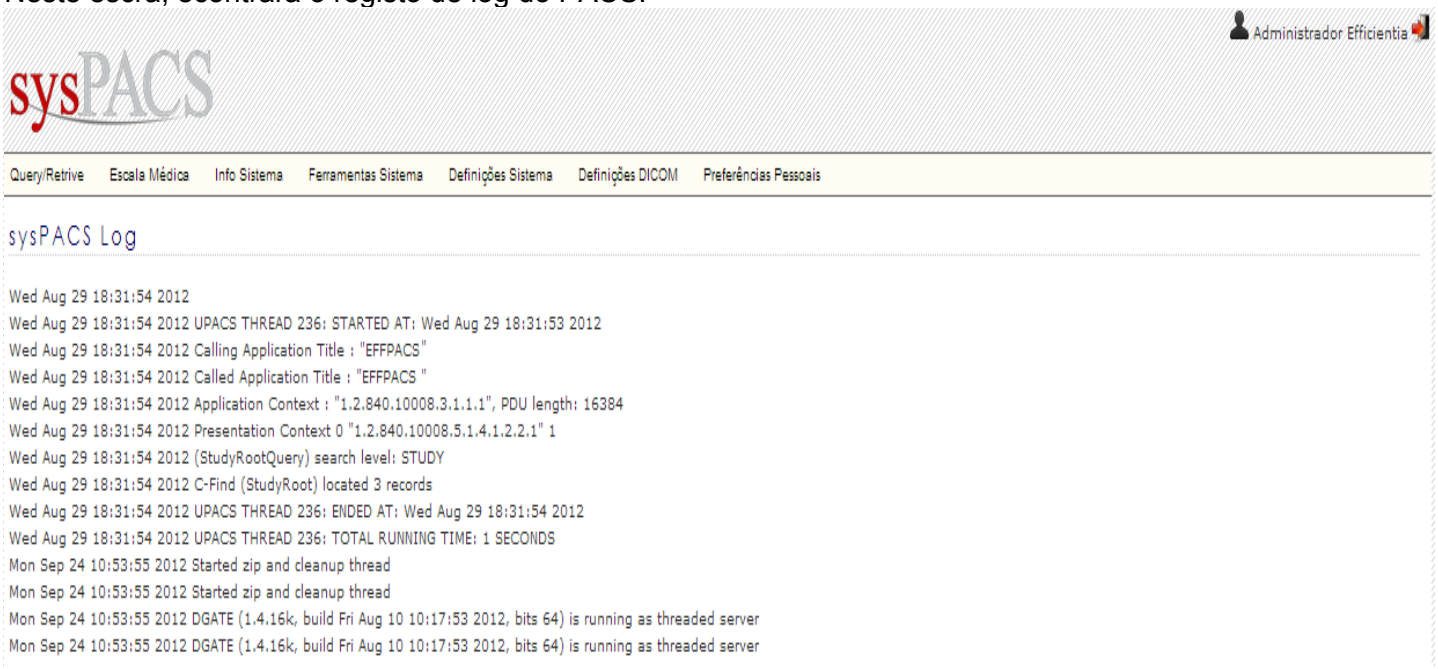
Deverá preencher os campos de acordo com a informação pretendida e clicar em Adicionar.

5.3 Selector Info Sistema

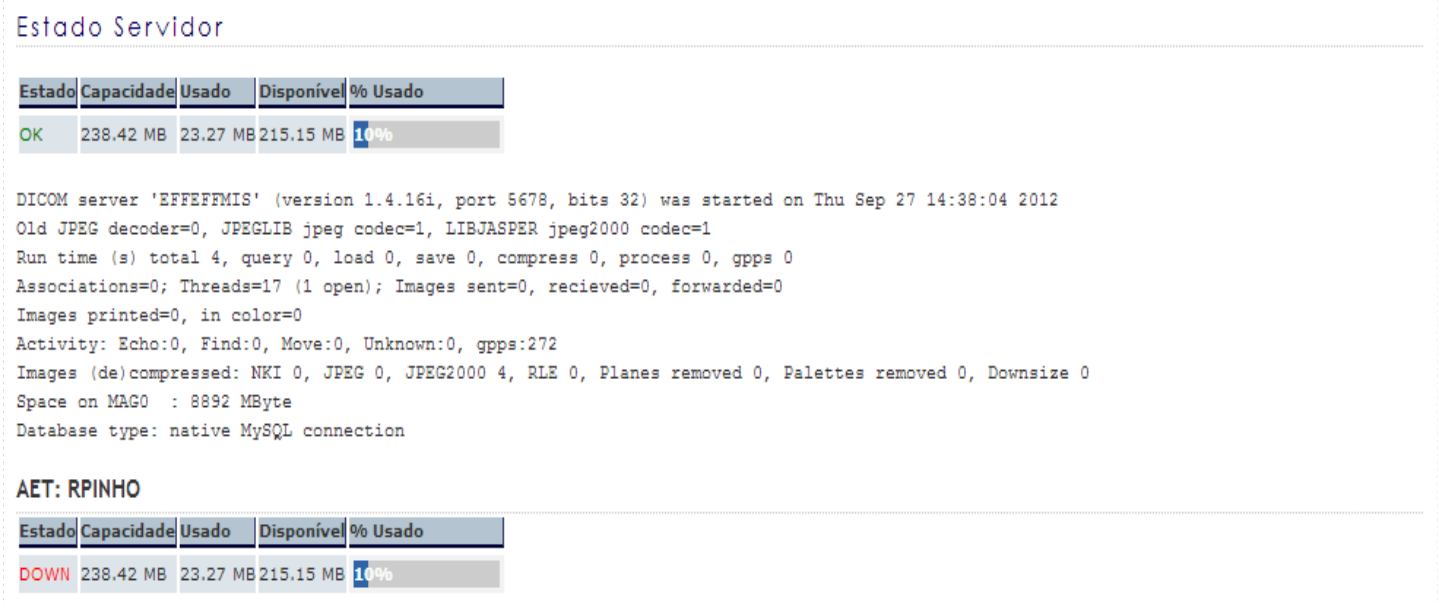
Este selector permite obter informações sobre o funcionamento do sistema. Dentro do selector existem dois subselectores, *sysPACS Log* e *Estado do Servidor*.

5.3.1. Subselector sysPACS Log

Neste escrã, econtrará o registo de log do PACS.



5.3.2. Subselector Estado Servidor

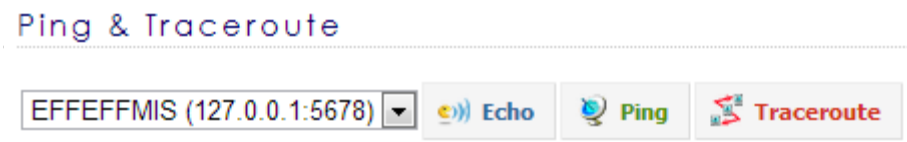


Informação obtida:
Estado
OK - PACS em funcionamento;
DOWN - PACS desligado;
Capacidade
Capacidade contratada para armazenamento;
Usado
Capacidade de armazenamento já utilizado;
Disponível
Capacidade de armazenamento ainda disponível;
% Usado
Percentagem de armazenamento utilizado;

5.4. Selector Ferramentas Sistema

Neste selector, poderá encontrar ferramentas importantes para verficar o funcionamento do sistema, contendo um subselector denominado "*Ping & Traceroute*".

5.4.1. Subselector Ping & Traceroute



No ecrã "*Ping & Traceroute*", existem três ferramentas para análise do sistema, permitindo testar também a comunicação com nós DICOM configurados no PACS.
Ferramentas disponíveis:
Echo
Efectua um comando C-ECHO ao nó DICOM escolhido;
Ping
Efectua um ping ao IP do nó DICOM escolhido;
Traceroutre
Efectua um trace route ao IP do nó DICOM escolhido;

5.5. Selector Definições Sistema

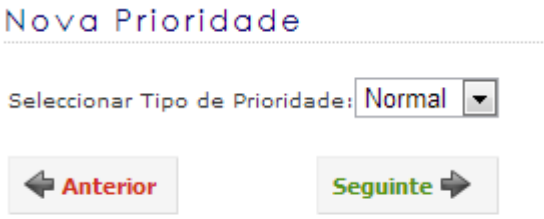
Neste selector, poderá fazer definições relacionadas com o as contas de utilizador e com a gestão das definições que serão usadas no módulo de alertas (caso o cliente tenha adquirido este módulo).

5.5.1. Subselector Lista de Prioridades

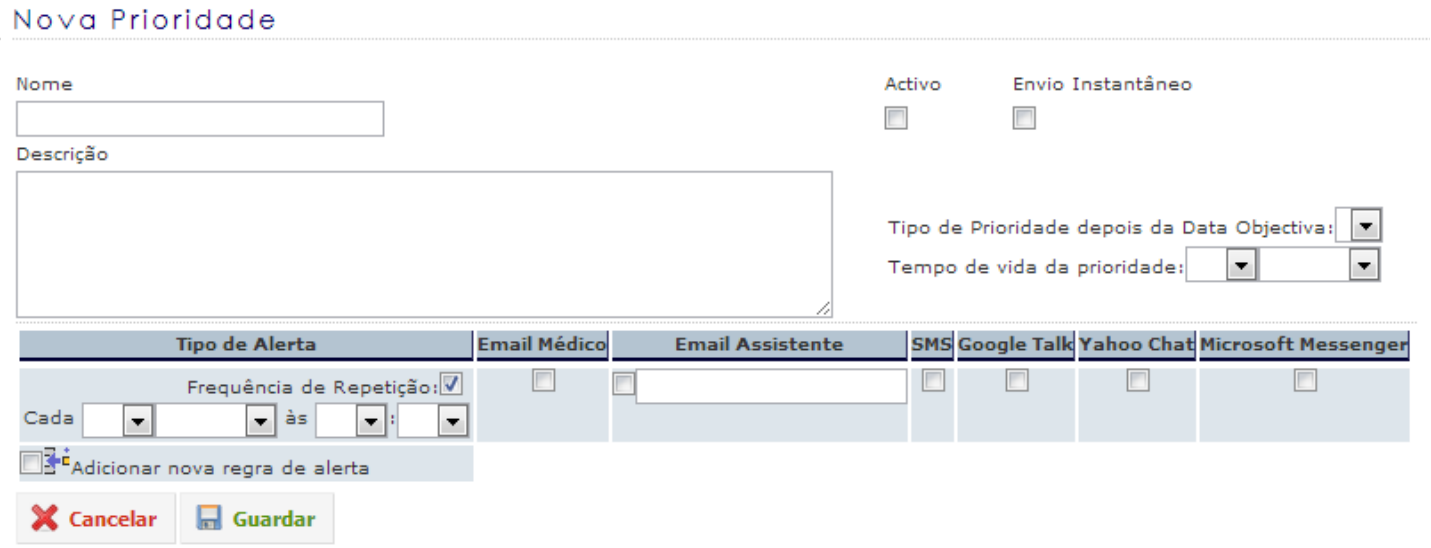
Como referido anteriormente, as prioridades serão utilizadas, pela solução, para o módulo de alertas. Sempre que for registado um estudo, deverá ser atribuído uma prioridade (pelo utilizador tipo recepção), sendo de seguida o médico relator notificado.
Existem dois tipo de prioridades:

- Normal
- Urgente

Sendo que cada prioridade irá desencadear um conjunto de alertas definidos pelo administrador do sistema.



Antes de criar, deverá escolher o tipo de prioridade, obtendo ecrãs diferentes mediante a escolha.



Campos a preencher:

Nome

Nome da prioridade que será exibida no sistema;

Descrição

Campo para efectuar uma descrição sobre a prioridade;

Activo

Indica se a prioridade está activa;

Envio Instantâneo

Indica se o médico relator é imediatamente notificado quando lhe é atribuído um estudo com esta prioridade;

Tipo de Prioridade depois da Data Objectiva

Caso o estudo não seja relatado durante o período definido em "*Tempo de vida da prioridade"*, este irá assumir uma prioridade do tipo Urgente definida neste campo;

Tempo de vida da prioridade

Tempo útil em que deverá ser relatado o estudo antes de assumir uma prioridade urgente;

Tipo de Alerta (Frequência de Repetição)

O alerta será enviado para o médico relator repetidamente segundo o período definido neste campo;

Email Médico

Será enviado um email para o médico relator;

Email Assistente

Caso esteja atribuído um assistente ao médico relator, será enviado um email para esse assistente;

SMS

Enviado uma sms para o médico relator (se contratatado);

Mensagem instântanea (Google Talk, Yahoo Chat e Microsoft Menssenger)

Será enviado uma mensagem instantânea para a conta de utilizador do médico relator;

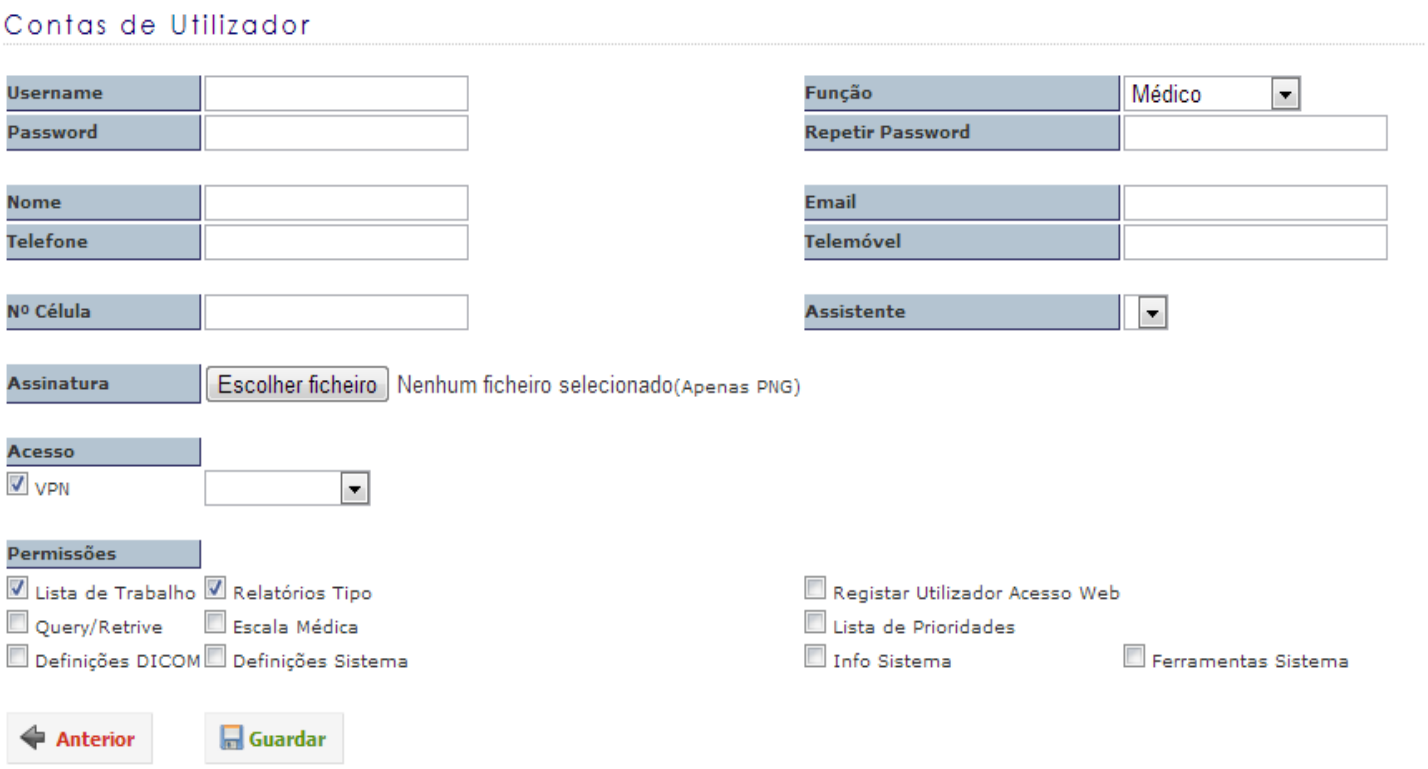
5.5.2. Subselector Contas de Utilizador

Neste subselector poderá fazer a gestão dos utilizadores do sistema. Existem 4 perfis de utilizador, sendo possível configurar individualmente as suas permissões. Os utilizadores são:

- Adminsitrador
- Recepção
- Transcripção
- Médico Relator

No ecrã, poderá criar, editar ou apagar um utilizador.

Antes de inicar a criação de utilizador, deverá escolher inicialmente a sua função, clicando de seguida em . De seguida será dado um exemplo de criação de um utilizador do tipo médico (médico relator).



Campos a preencher:

Username
: Nome de utilizador atribuído ao utilizador para autenticação na aplicação;

Password
: Palavra-chave utilizada para autenticação;

Nome
: Nome de utilizador que será apresentado na aplicação;

Email
: Email do utilizador

Telefone*
: Contacto Telefónico do utilizador;

Telemóvel*
: Contacto telemóvel do utilizador;

Nº Célula*
: Nº de célula profissional do utilizador tipo Médico Relator;

Assistente*
: Utilizador do tipo Recepção ou Transcrição definido como assistente do utilizador em questão;

Assinatura
: Imagem em formato PNG, que será utilizada para validação dos relatório;

Acesso*
: Se o utilizador necessitar de um acesso VPN, deverá ser criado inicial o nó DICOM no selector *Definições DICOM -> AE Title Remoto*, sendo de seguida atribuído esse nó DICOM ao utilizador em questão;

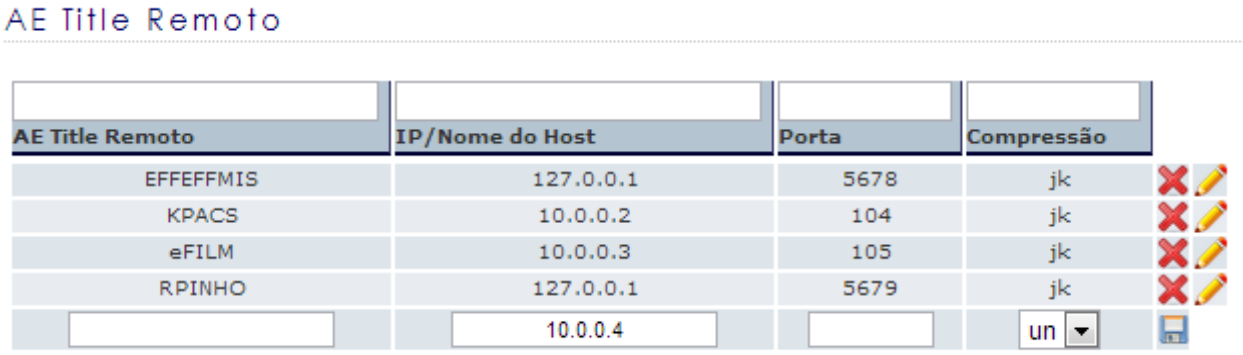
Permissões
: Mediante o tipo de utilizador, as permissões serão previamente seleccionadas. No entanto poderá adicionar ou retirar permissões ao utilizador.

* Campos de preenchimento opcionais.

5.6. Selector Definições DICOM

5.6.1. Subselector AE Title Remoto

Neste ecrã poderá criar os nós DICOM que o PACS irá conhecer.



Por defeito, o sistema preenche automaticamente o campo *IP/Nome do Host* com um IP válido de VPN. Caso deseje que o nó DICOM a criar seja atribuído a um utilizador do tipo *Médico Relator* deverá utilizar o IP apresentado.

Campos a preencher:

AE Title Remoto
: AE Title do nó DICOM;

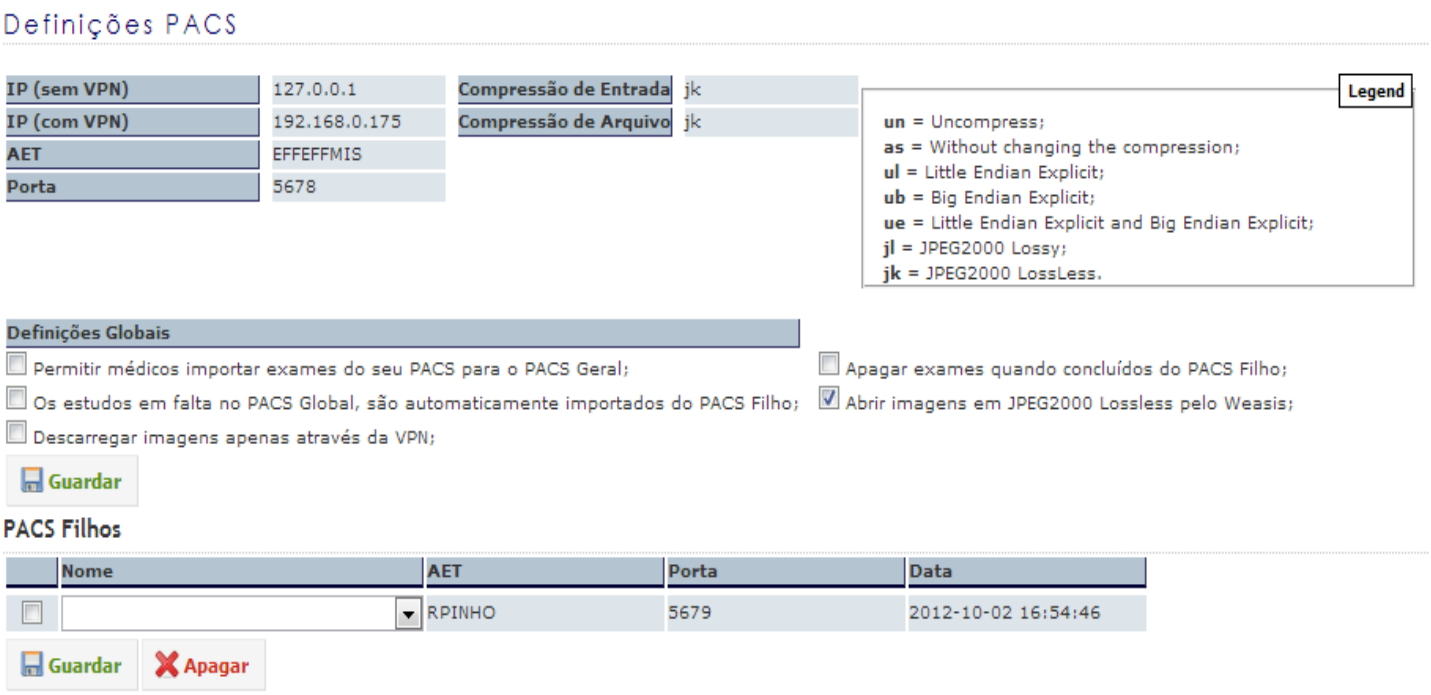
IP/Nome do Host
: IP do nó DICOM. Caso deseje um IP de VPN, deverá deixar o campo com o valor introduzido pelo sistema;

Porta
: Porta do nó DICOM;

Compressão
: Tipo de compressão das imagens que serão enviadas para o nó DICOM definido.

5.6.2. Subselector Definições PACS

Neste ecrã poderá configurar o modo de funcionamento da aplicação/PACS.



Na parte superior do ecrã, encontra informações DICOM acerca do PACS e a forma como está configurada o modo de arquivo das imagens.

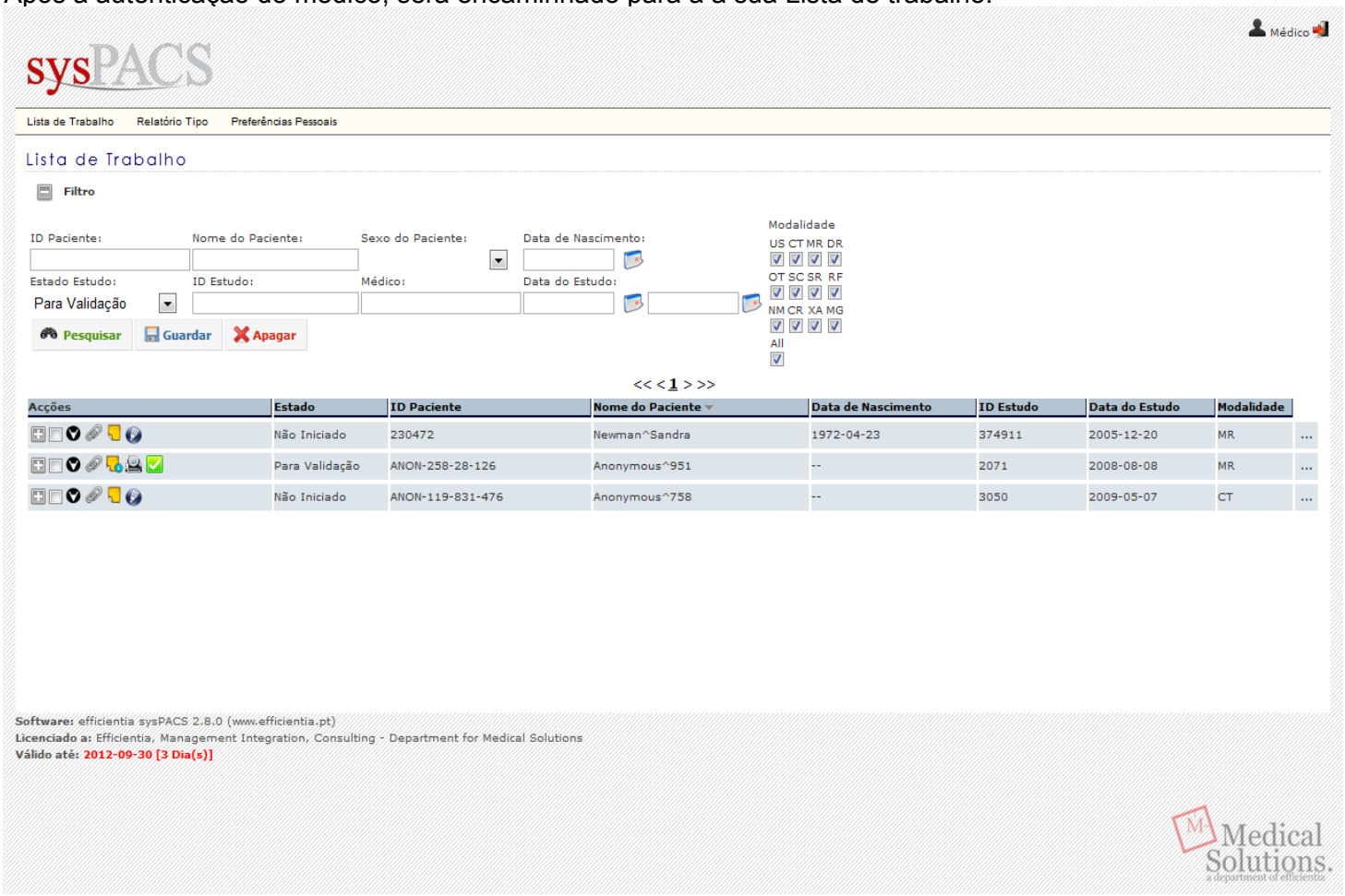
Na secção *Definições Globais* poderá fazer as configurações globais do PACS e que estarão em vigor para todos os utilizadores. (As opções disponíveis dependerão da licença adquirida.)

Caso o cliente tenha adquirido o módulo *Multiple AET,* irá também aparecer neste ecrã a secção *PACS Filhos* que são os PACS dependentes dos PACS principal. Cada PACS Filho, poderá ser atribuído a um utilizador do tipo médico.

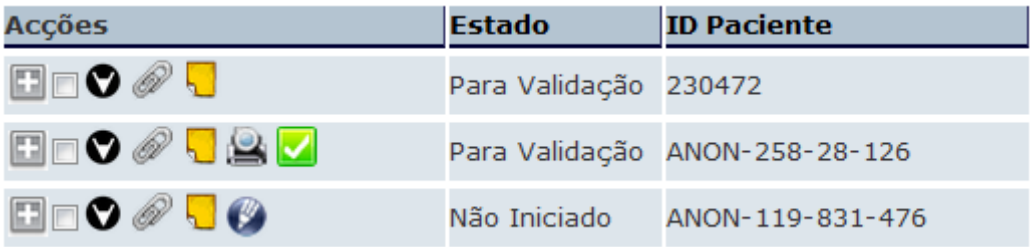
6. Módulo Médico

6.1. Selector Lista de Trabalho

O módulo do médico relator disponibiliza as funções de relatar e visionamento das imagens.
Após a autenticação do médico, será encaminhado para a a sua Lista de trabalho.



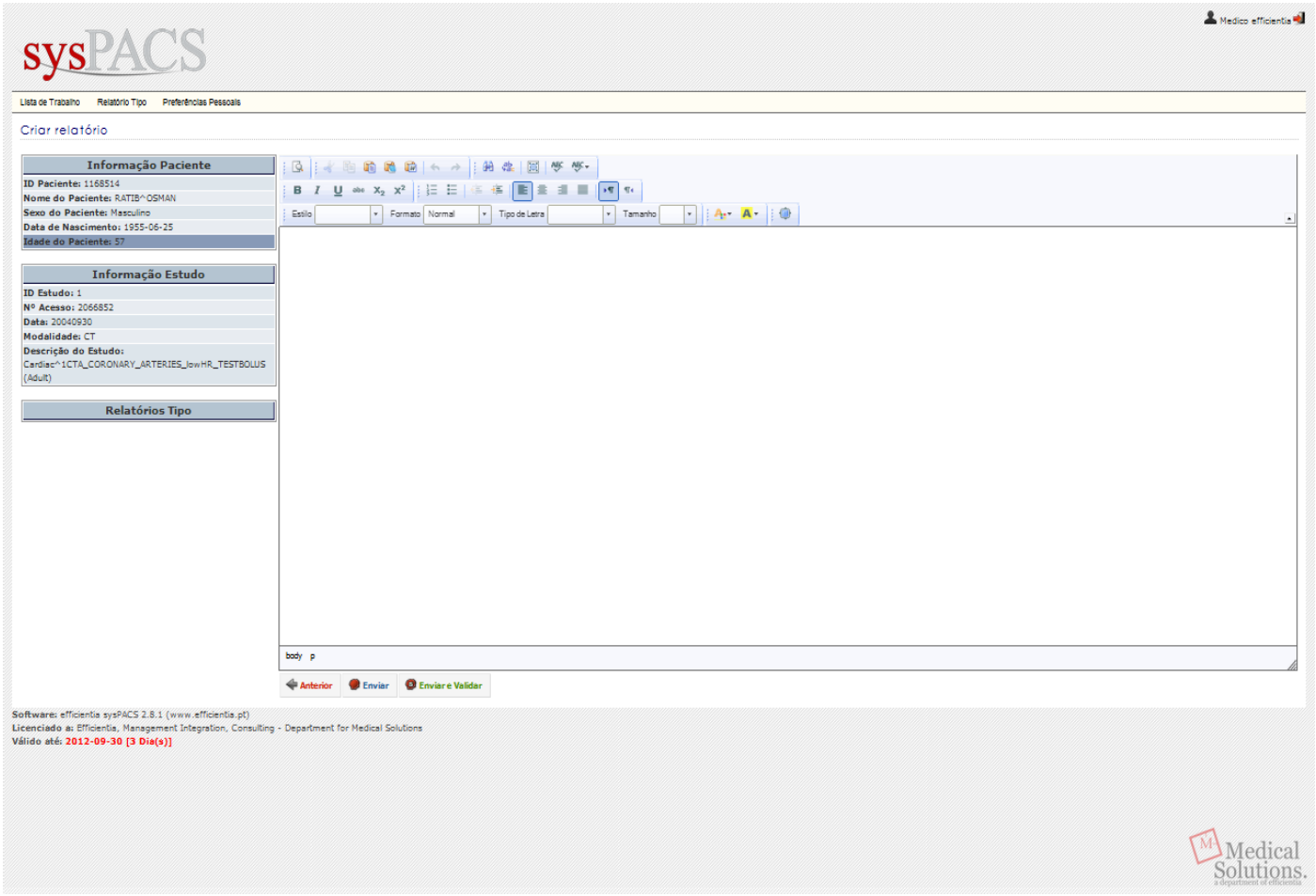
Na lista de trabalho encontra-se um filtro que permite pesquisar estudos associados ao médico autenticado.

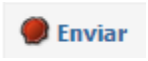


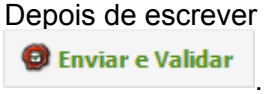
Na tabela são disponibilizados os estudos juntamente com as acções que podem ser efectuadas sobre cada estudo.

 Visualizar conteúdo escondido;
 Esconder conteúdo;
 Efectuar visualização;
 Abrir visualizador Weasis;
 Visualizar miniatura da imagem;
 Gravar registo;
 Editar registo;
 Gravar registo editado;
 Anexar ficheiros ao estudo;
 Estudo sem notas, ao clicar abre ecrã notas;
 Estudo com notas, ao clicar abre ecrã notas;
 Adicionar nota;
 Editar nota;
 Apagar nota;
 Escrever relatório;
 Pré-visualizar relatório;
 Imprimir relatório em pdf;
 Validar relatório;
 Cancelar validação do relatório;
 Visualizar mais informações sobre o estudo;

Seleccionando a opção “Escrever Relatório ” será reencaminhado para editor de texto onde será possível escrever o relatório , como se pode ver na imagem seguinte. Tem disponível do lado esquerdo do ecrã informações do Paciente juntamente com informação do estudo.

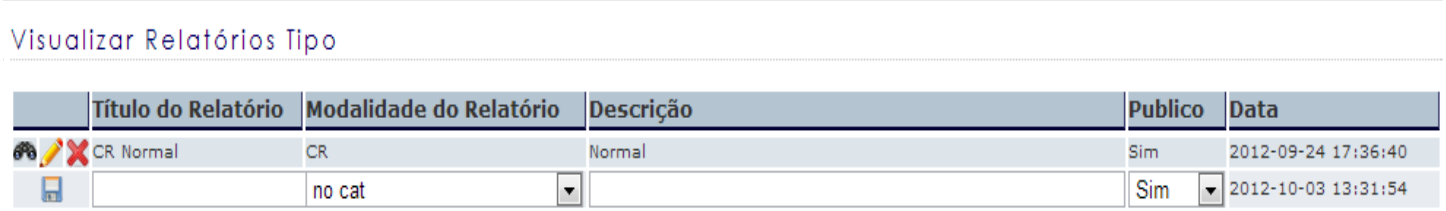


Depois de escrever o relatório é possível guardar clicando em 

ou guarda e validar clicando em 

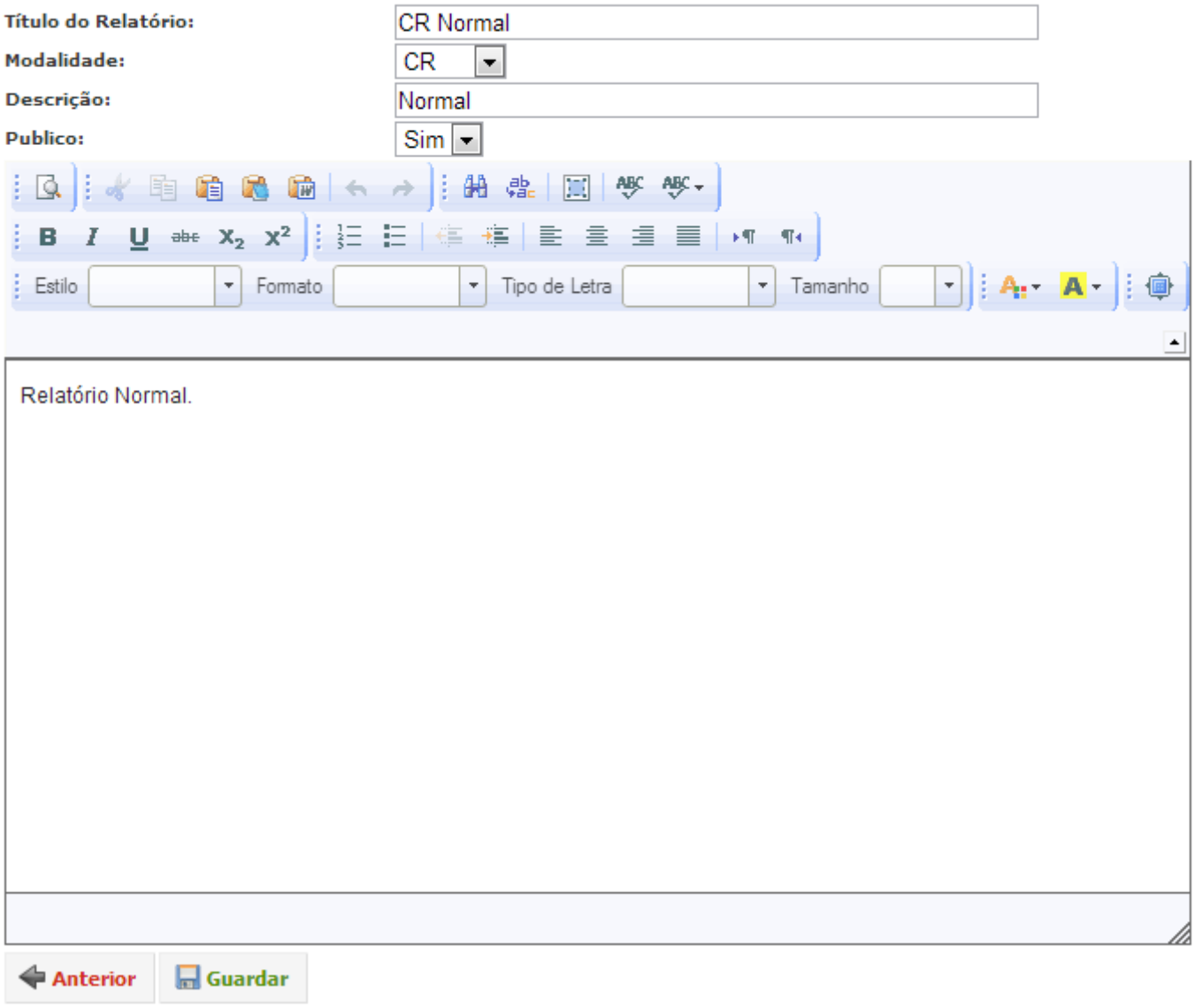
.

6.2. Selector Relatório Tipo



Neste selector é possível escrever um relatório tipo que pode usar aquando da escrita do relatório do estudo. Depois de escrever o titulo do relatório deve escolher a modalidade e se quer torna-lo publico e será reencaminhado para um editor de texto que permite escrever o relatório tipo.

Editar


Título do Relatório:
CR Normal
Modalidade:
CR
Descrição:
Normal
Publico:
Sim
Estilo
Formato
Tipo de Letra
Tamanho
Relatório Normal.
Anterior
Guardar

A.6 Processo de Concepção

Objectivo e Âmbito do processo Estudo e desenvolvimento de produtos ou serviços que possam satisfazer os clientes.

Responsável pelo processo Efficientia – Gerência WeMake – Investigação e Desenvolvimento

Descrição do Processo

Entradas

Processo Recursos Humanos
- Recursos Humanos disponíveis e formados

1. Processo Planeamento Estratégico e Melhoria Contínua
   - Identificação de necessidades de clientes relativamente a novos produtos
   - Política (QD009)
   - Quadro de Indicadores BSC (QI036)
   - Objectivos Globais (QD013)
   - Objectivos e Plano de Acções de Melhoria (QI034)
2. Processo Cliente
   - Proposta adjudicada

LEGENDA

- Actividades
- Processo Fornecedor / Cliente
- ● Responsável
- ⊙ Participa

Entradas	Actividades	Saídas	Gerência	COO	Administrativo e RH	Qualidade	Serviço de Apoio	Medical Solutions	Formação	Gestão de Sistemas	Customer Relationship Departament	Engineering	Investigação e Desenvolvimento	Descrição	Documentos
1.Planeamento Estratégico e Melhoria Contínua 2. Cliente	Especificação para o projecto		⊙			⊙		●	●	●	●	●	●	Uma nova concepção pode ser desencadeada por necessidade interna ou por solicitação de clientes. O desenvolvimento de um novo serviço ou produto inicia-se com o lançamento no AI001 e registo no QI019 ou EI010 respectivamente.	QP007-Concepção de serviços IP001-Concepção de produtos QI004-Verificações e Revisões QI019-Concepção de serviços EI001 – Recolha de requisitos EI002 – Configuração de software EI010-Verificações e Planeamento da Concepção EI014 – Reuniões de análise e revisão de concepção EI015 – Reuniões de Projecto – Alterações/ Correcções
	Concepção Inicial		⊙					●	●	●	●	●	●	Elaboração do planeamento da concepção que refere as etapas da concepção e as respectivas revisões, verificações e validação final, designando as responsabilidades.	QP007-Concepção de serviços IP001-Concepção de produtos QI004-Verificações e Revisões QI019-Concepção de serviços EI001 – Recolha de requisitos EI002 – Configuração de software EI010-Verificações e Planeamento da Concepção EI014 – Reuniões de análise e revisão de concepção EI015 – Reuniões de Projecto – Alterações/ Correcções
	1º Fornecimento		⊙					●	●	●	●	●	●	Elaboração do primeiro fornecimento com base na concepção desenvolvida.	QP007-Concepção de serviços IP001-Concepção de produtos QI004-Verificações e Revisões QI019-Concepção de serviços EI001 – Recolha de requisitos EI002 – Configuração de software EI010-Verificações e Planeamento da Concepção EI014 – Reuniões de análise e revisão de concepção EI015 – Reuniões de Projecto – Alterações/ Correcções
	Lançamento	1. Execução	⊙					●	●	●	●	●	●	Colocação em funcionamento e elaboração de um relatório que valida o lançamento. Verificação da fase, de forma a garantir que os resultados satisfazem as especificações para o projecto. Conclusão de todo o Processo de Concepção.	QP007-Concepção de serviços IP001-Concepção de produtos QI004-Verificações e Revisões QI019-Concepção de serviços EI001 – Recolha de requisitos EI002 – Configuração de software EI010-Verificações e Planeamento da Concepção EI014 – Reuniões de análise e revisão de concepção EI015 – Reuniões de Projecto – Alterações/ Correcções

Saídas

Processo Gestão da Qualidade
- Quadro de Indicadores BSC (QI036)

Processos Suporte
- Identificação de necessidades de Recursos humanos, materiais e de apoio a nível da gestão da qualidade

1. Processo Execução
   - Verificações e Revisões (QI004)
   - Concepção de serviços (QI019)
   - Recolha de requisitos (EI001)
   - Configuração de software (EI002)
   - Verificações e Planeamento da Concepção (EI010)
   - Reuniões de análise e revisão de concepção (EI014)

A.7 Checklist - Avaliação dos aspetos de segurança

Avaliação dos aspectos de segurança					**Legenda:** 1-Fraco; 2-Insuficiente; 3-Razoável; 4- Bom;
Aspectos a Avaliar	**Avaliação**				
	1	**2**	**3**	**4**	
Autenticação e Autorização dos utilizadores					
São utilizados mecanismos de autenticação por tipo de utilizador (administrador, utilizador, gestor, etc)? Quais são?					
É identificado correctamente o utilizador correctamente? (A aplicação deve mostrar o utilizador conectado ao sistema, seja por via indirecta (login via sistema operativo) ou por via directa (login na própria aplicação))					
Existem políticas de senhas? São alteradas regularmente? (Por exemplo, desconfio que alguém sabe a minha password. Posso altera-la já?)					
Poderá um utilizador alterar informação registada por outro utilizador? (Por exemplo falsear informação: Util1 escreve 100Euros, Util2 altera para 10Euros)					
São dadas e controladas as permissões por tipo de utilizador?					
Confidencialidade dos dados					
Existem mecanismos de garantia de confidencialidade no acesso aos dados em operação normal?					
E em situação de ataque? Os mecanismos de protecção são suficientemente robustos?					
E no caso de acesso aos dados para estudos estatísticos ou científicos?					
É possível aceder à aplicação através de um link/atalho existente no histórico? (Por exemplo, no navegador da internet)					
Existem mecanismos de rastreio às operações de configuração do utilizador/sistema? (Por exemplo, alteram a minha configuração. Eu nada fiz. Quem foi?)					
Integridade dos dados					
Existem mecanismos que permitam controlar a integridade dos dados em operação normal?					

E em situação de ataque? Os mecanismos de protecção são suficientemente robustos?					
Existe procedimentos de verificação, correcção e controlo de qualidade dos dados?					
Após uma falha de energia, qual o estado dos registos e Bases de Dados? (Poderão ser os registos reparados, pelo cliente?)					
Existem mecanismos de backup implementados na aplicação? (A aplicação gere os backups internamente?)					
Disponibilidade do sistema					
Existem mecanismos para garantir a disponibilidade do sistema em operação normal?					
Existe mecanismos para contrariar potenciais ataques ao sistema do tipo "Negação de Serviços"?					
Tolerância a falhas do sistema em caso de avaria? E em caso de ataque?					
Existência de pontos críticos informáticos?					
É possível aceder a aplicação pela “porta de trás”? (Poderá um utilizador aceder directamente à informação (registos) das tabelas/bases de dados, sem ser pela aplicação principal?)					
Existência de pontos críticos físicos?					
Está especificado qual o nível de segurança pretendido?					
Auditabilidade					
Existe registos que permitam efectuar auditoria?					
Que informação é registada?					
Existe verificação regular desses registos?					
Que meios suportam esses registos?					
Utilização ao nível de administração					
A administração do sistema é remota ou tem de ser feita na consola?					
Quais os mecanismos de autenticação utilizados? Existem cuidados especiais?					

De que forma é feita a protecção da sessão de administração remota?					
Os procedimentos de administração estão documentados?					
As interfaces são fáceis de perceber e utilizar?					
Em situação de elevada carga do sistema o administrador têm prioridade de acesso?					
É possível configurar o sistema de diferentes formas, para diferentes utilizadores?					
Que poderes tem o administrador? Existe diferentes tipos de administradores?					
Acesso ao sistema para estatísticas?					
Utilização normal					
O acesso ao sistema é remoto ou local?					
A utilização do sistema está devidamente documentada?					
Mecanismos de autenticação utilizados?					
As interfaces são fáceis de perceber e utilizar?					
Em situação de elevada carga do sistema?					
Conformidade com normas					
O sistema está em conformidade com certificações oficiais?					
Qual é o grau de conformidade?					
Mecanismos de defesa					
É usado algum sistema criptográfico de protecção?					
A que nível são usados os mecanismos criptográficos? (Ao nível aplicação, ao nível do sistema ou ao nível da rede?)					
Grau de robustez do sistema criptográfico? (Qual o algoritmo e o comprimento das chaves criptográficas?)					
Existe mecanismos para prevenção de intrusão?					
Existe mecanismos para detecção de intrusão?					
Existe mecanismos de recuperação em situação de intrusão?					
Comunicações					

Tipos e meios de comunicação usados?					
Os meios usados são propícios a escuta e quebra de confidencialidade dos dados transmitidos?					
Existe mecanismo para garantir a integridade da informação em trânsito?					
Existe mecanismo de certificação do utilizador de forma a prevenir o "disfarce"? Qual?					
Existe mecanismo para prevenir a interrupção das comunicações?					
Teste e Verificação de Rotina					
As rotinas (procedimentos e funções) estão documentadas? (Estão comentadas as entradas (parâmetros), saídas (valores de retorno), ligações a outras rotinas, etc...)					
Se a rotina for uma função, retorna um valor quaisquer que sejam as circunstâncias. (Estão testados valores de retorno, tipo: Empty, Null, Zero, -1, ...)					
A rotina protege-se contra os dados de entrada errados? (Cada rotina verifica a validade dos respectivos parâmetros)					
A convenção utilizada permite distinguir entre variáveis locais, de módulo e globais.					
Os nomes são formatados para melhorar a sua legibilidade.					
A eficiência da rotina tem em conta não só a velocidade de execução mas também as ligações a bases de dados?					
A rotina possui mecanismos de debug que podem ser facilmente activados ou desactivados.					
As variáveis são inicializadas perto do local onde são utilizadas pela primeira vez?					
Verificação Aplicacional					
É identificado correctamente o utilizador corrente? (A aplicação deve mostrar o utilizador conectado ao sistema, seja por via indirecta (login via Sistema Operativo) ou por via directa (login na própria aplicação))					
A aplicação é funcional nos seus requisitos em idioma diferente? (Exemplo: A aplicação foi desenvolvida em MS Access 2000 em português e funciona em Inglês ?)					
A comutação de várias resoluções na aplicação está					

salvaguardada? (Exemplo: aquando uma resolução inferior (800x600) a aplicação apresenta-se redimensionada correctamente?)					
Os forms apresentam-se coerentes (cor, posicionamento de controlos, ...) ? (Exemplo: Ao navegar na aplicação todos os seus ecrãs apresentam-se idênticos? Os botões e o seu posicionamento são semelhantes em todos os interfaces?)					
O acesso aos controlos está "tabulado" correctamente? (Exemplo: Posso usar a aplicação sem o rato? Somente com o teclado?)					
Está explicito o tipo de conteúdo que o utilizador deve preencher nos campos? (Exemplo: Ao registar uma data, o utilizador sabe qual o seu formato? yyyy-mm-dd ou dd-mm-yyyy)					
Quando o tipo de dados não corresponde ao programado, existem mensagens de ajuda? (Exemplo: Ao registar a idade, o utilizador introduz letras. O que sucede? O software corrige, alerta ou aborta a aplicação)					
Está definido um interface com o utilizador para mensagens de erro?					
Está especificada a quantidade máxima de espaço em disco?					
Está definida uma estratégia de gestão de códigos de erros ? (Por Exemplo: Como gerir os erros? O cliente telefona e diz Erro: 1432.)					
Testaram-se todas as fronteiras simples: máximo, mínimo e "fora de limite". (por exemplo um número atómico na inserção da data de nascimentos)					
São visíveis todos os tempos de resposta, do ponto de vista do utilizador, para todas as operações necessárias? (Exemplo: Quando uma operação é demorosa, existe um gráfico de processamento 0% -- 100%?)					
A pré-visualização corresponde à impressão (standard WYSWYG)? (Exemplo: O que eu pré visualizo é o que eu obtenho?)					
Existem mecanismos de Paginação e Codificação implementados nos relatórios? (Exemplo: Cada relatório pode ter um código específico e todas as suas páginas estão identificadas?)					
As margens definidas nos relatórios abarcam toda a informação necessária?					

A impressão em diferentes tipos de impressora (laser, jacto tinta,...) foi testada?					
Toda a arquitectura é independente da máquina em que será implementada?					
Esta arquitectura prevê futuras integrações?					
A declaração dos dados e a respectiva consistência estilística é garantida pela utilização de uma máscara.					
Documentação					
Existe informação técnica para administração do sistema?					
Existe informação para a utilização do sistema?					

A.8 FMEA

FMEA de Projecto - Falha no controlo de acesso

PRODUTO:	efficientia sysPACS

											Resultados			
FUNÇÃO DA OPERAÇÃO	MODO DE FALHA POTENCIAL	EFEITOS DE FALHA POTENCIAL	GRAVIDADE	CAUSAS DE FALHA POTENCIAIS	OCORRÊNCIA	CONTROLOS ACTUAIS	DETEÇÃO	RPN	ACÇÕES RECOMENDADAS	RESPONSÁVEL	ACÇÕES TOMADAS	OCORRÊNCIA	DETEÇÃO	RPN
Falha no controlo de acesso -Identificação do utilizador. - Protecção de dados pessoais.	Quebra do Login	- Perda de informação confidencial. - Perda de dados de saúde. - Introdução errada de dados no sistema	10	Injecção SQL	7	Nenhum	8	560	Codificação de caracteres; Codificação contra tag`s;	RSP CEC	Codificação de caracteres; Codificação contra tag`s;	7	1	70
				Autenticação e gestão de seções	5	Logout;	6	300	A sessão deve expirar; Log`s do login; Re-autenticação; Número máximo de tentativas de autenticação; HTTPS;	RSP CEC	A sessão deve expirar; Log`s do login; Re-autenticação; HTTPS;	6	2	100
				Falha na restrição de acesso a URL`s	7	Nenhuma	5	350	Níveis de acesso; Encriptação URL;	RSP CEC	Níveis de acesso; Encriptação URL;	7	2	100
				Roubo de credenciais de acesso	6	Nenhuma	8	480	Sistema de validação por sms;	RSP CEC	Nenhuma	6	8	480

FMEA de Projecto - Introdução de dados errados no sistema

PRODUTO:	efficientia sysPACS

											Resultados			
FUNÇÃO DA OPERAÇÃO	MODO DE FALHA POTENCIAL	EFEITOS DE FALHA POTENCIAL	GRAVIDADE	CAUSAS DE FALHA POTENCIAIS	OCORRÊNCIA	CONTROLOS ACTUAIS	DETEÇÃO	RPN	ACÇÕES RECOMENDADAS	RESPONSÁVEL	ACÇÕES TOMADAS	OCORRÊNCIA	DETEÇÃO	RPN
Validação Input	Introdução de dados errados no sistema.	Erros que podem levar a quebra do sistema. Introdução de dados médicos errados. Troca de dados médicos dos utentes.	7	Referência direta a objetos	7	Nenhuma	9	441	Encriptação dos URL´s Validação de dados	RSP CEC	Uso de funções que permitem a encriptação de dados	7	2	98
				Redirecionamento não validados	7	Nenhuma	8	392	Validação e encriptação dos dados	RSP CEC	Encriptada e validação de grande parte dos dados.	8	2	98
				Validação de input e output de funções	6	Algumas validações	7	294	Validação dos valores de entrada e saída das funções	RSP CEC	Validação das entradas e saídas na maioria das funções	7	3	126

FMEA de Projecto - Perda de informação

PRODUTO:	efficientia sysPACS

											Resultados			
FUNÇÃO DA OPERAÇÃO	MODO DE FALHA POTENCIAL	EFEITOS DE FALHA POTENCIAL	GRAVIDADE	CAUSAS DE FALHA POTENCIAIS	OCORRÊNCIA	CONTROLOS ACTUAIS	DETEÇÃO	RPN	ACÇÕES RECOMENDADAS	RESPONSÁVEL	ACÇÕES TOMADAS	OCORRÊNCIA	DETEÇÃO	RPN
Troca de dados com o servidor - Troca de informação. - Imagens Médicas. - Dados Médicos.	Perda de informação	Perda de informação. Falta de confiança por parte dos clientes. Problemas legais.	10	Comunicação insegura	5	Nenhum	7	350	Utilização de um protocolo de comunicação seguro.	RSP CEC	Implementação de HTTPS. Implementação de VPN.	5	1	100
				Armazenamento criptográfico inseguro	8	Uso de funções criptográficas fracas.	7	560	Uso de funções criptográficas mais seguras.	RSP CEC	Implementação de SHA.	8	1	80

A.9 Fluxograma dos Procedimentos de Avaliação de Conformidade

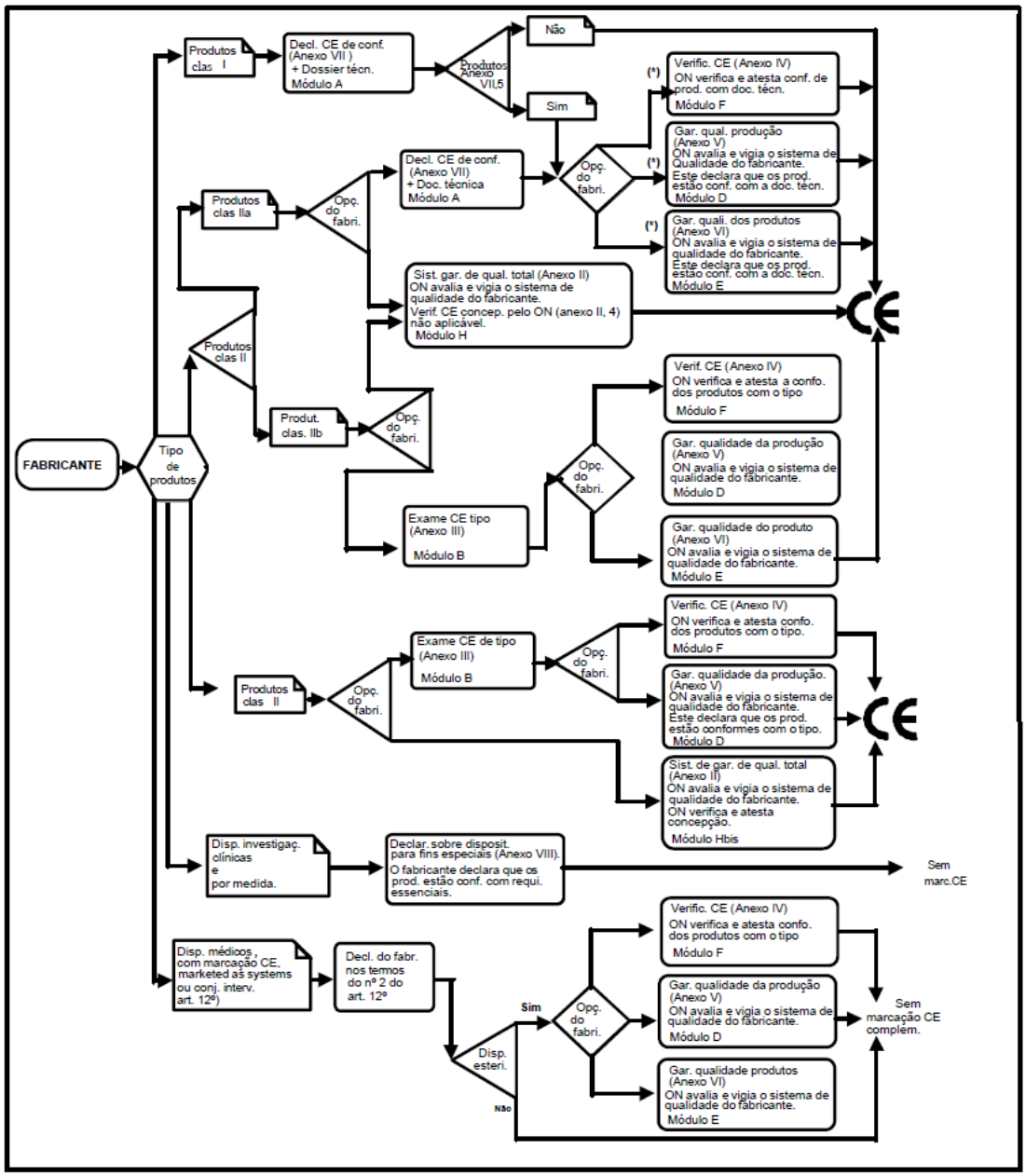


Fig. A.1: Fluxograma dos Procedimentos de Avaliação de Conformidade [1].