Comparação do controlo de acesso em instituições de Saúde privadas e públicas, da região Norte.

Ana Sofia Silva Maria

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

SET|2017

MIM

Comparação do Controlo de acesso em instituições de saúde privadas e públicas, da região Norte

Ana Sofia da Silva Maria

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

ORIENTADORES:

Ana Ferreira, CINTESIS

SET|2017

ii

Agradecimentos

Em primeiro lugar, gostaria de agradecer à minha família, em especial aos meus pais e à minha irmã, pelo apoio incondicional e por acreditarem nas minhas capacidades.

À Doutora Ana Ferreira, minha orientadora, que sempre se mostrou disponível para me ajudar em todo o processo de elaboração deste trabalho, assim como por me ter ensinado, que independentemente das adversidades, devemos seguir em frente, pois estas tornar-se-ão em ensinamentos no futuro.

Aos representantes de todas as instituições, que participaram na recolha de dados, que sempre se mostraram disponíveis para me receber e ajudar em todas as fases da recolha de dados.

Ao engenheiro Hugo Rio Costa, que me ajudou a superar as dificuldades ligadas à análise estatística.

Aos meus amigos e colegas de trabalho, pelo apoio, carinho e sobretudo paciência.

Resumo

Introdução: A importância da informação hospitalar, é inquestionável, sendo que a partilha da mesma, é indispensável para uma prática clinica eficiente. Existe legislação para proteger os dados em saúde, mas nem sempre é fácil e aplicável na prática clinica diária. Assim sendo, um controlo de acesso rigoroso pode ser a chave para aumentar a confiança não só de quem usufrui dos cuidados de saúde, como também de quem os pratica.

Objetivo: O principal objetivo desta tese é sumariar e comparar quais os modelos, mecanismos e políticas de controlo de acesso utilizados nos departamentos de Radiologia de instituições de saúde públicas e privadas do norte de Portugal.

Métodos: O presente trabalho foi desenvolvido nos departamentos de Radiologia, em quatro instituições de saúde da região Norte de Portugal, sendo que destas, duas eram de natureza privada e duas de natureza pública. Foram elaborados dois instrumentos de recolha de dados: um "Questionário" e um "Levantamento". Estes instrumentos foram estruturados com conteúdos obtidos mediante uma pesquisa da literatura do tema em questão, e foram posteriormente aplicados à população alvo deste estudo: os profissionais de saúde dos Departamentos de Radiologia das quatro instituições de saúde já mencionadas. Na análise estatística considerou-se uma amostra de 105 inquiridos.

Resultados: A adaptação dos profissionais de radiologia aos modelos de controlo de acesso não é condicionada pela idade. Destaca-se que 85% dos profissionais inquiridos nas instituições públicas afirmam que o modelo de

controlo de acesso a dados clínicos dos doentes em formato eletrónico é o RBAC. Já nas instituições privadas apenas 57% dos profissionais inquiridos responderam da mesma forma. Privadas e Públicas estão de acordo, quando referem como mecanismo de autenticação preferencial o login/password. No entanto, tanto no privado (32,50%) como no público (1,85%) existem profissionais que afirmam partilhar as suas credenciais.

A existência de um documento regulamentador é vista como essencial por profissionais de ambas as instituições, no entanto 44,76% dos inquiridos afirma não saber da existência do mesmo e 30,48%, afirma mesmo que este não existe.

Discussão e Conclusões: A análise de resultados evidencia diferenças relativamente ao controlo de acesso aos dados dos doentes no departamento de Radiologia, dependendo da instituição. O modelo RBAC é o mais utilizado, mas nos privados necessita de melhor adequação. Em ambas as instituições o mecanismo de autenticação mais utilizado é o *login/password*, no entanto, a partilha de credenciais pode diminuir a sua eficiência. As instituições deveriam contemplar, assim como divulgar e atualizar um documento institucional, que regulamente a segurança ou o acesso aos dados clínicos e pessoais dos doentes, de forma a manter a confidencialidade dos mesmos, a limitar o acesso aos dados a pessoas não autorizadas, a uniformizar procedimentos e a salvaguardar os profissionais, as instituições e os pacientes.

Palavras-chave: Controlo de Acesso, Segurança Informática, Instituições de Saúde

Abstract

Introduction: The importance of healthcare information is unquestionable and indispensable for an efficient clinical practice. There is legislation to protect health data, but it is not always easy and applicable within the daily clinical practice. Thus, strict access control can be a key to increasing confidence not only among those who take care of health care, but also of those who practice it.

Objective: The main objective of this thesis is to summarize and compare the models, mechanisms and policies of access control used in the departments of Radiology of public and private healthcare institutions from the north region of Portugal.

Methods: The present study was carried out in the Radiology Departments of four health institutions in the Northern region of Portugal, two of which are of a private nature and two of a public nature. Two data collection instruments were developed: a "Questionnaire" and a "Survey". These instruments were structured with contents obtained from a literature review on the studied theme and were thus applied to the target population of the study: the health professionals of the Departments of Radiology of the already mentioned institutions. The statistical analysis integrated a sample of 105 respondents.

Results: The adaptation of radiology professionals to access control models is not conditioned by age. It is noteworthy that 85% of the professionals surveyed in public institutions affirm the most commonly used model of access control to clinical data in electronic format is RBAC. In the

private institutions, only 57% of the respondents responded in the same way. Private and Public institutions are in agreement when they refer that *login / password* is the preferential authentication mechanism. However, both private (32.50%) and public (1.85%) professionals also claim that they share their credentials.

The existence of a regulatory document is seen as essential by professionals from both institutions; however, 44.76% of the respondents are not aware of its existence and 30.48% say that it does not exist.

Discussion and Conclusions: An analysis of results evidences that access control of data from a radiology department can depends on the nature of the institution. The RBAC model is the most used model, but in private institutions it requires better adequacy. In both institutions, the most commonly used authentication mechanism is login / password, however, credentials' sharing may decrease its efficiency. Institutions should contemplate, as well as disclose an institutional document that regulates the security as well as access to clinical data in order to maintain their confidentiality, to limit access to data to unauthorized persons, to standardize procedures and to safeguard the professionals, the institution and the patients.

Key words: Access Control, Computer Security, Health Institutions

Preâmbulo

Em 2014 terminei a licenciatura em Radiologia, na Escola Superior de Saúde da Universidade de Aveiro. Nesse mesmo ano ingressei no Mestrado em Informática Médica e simultaneamente iniciei funções como técnica de Radiologia numa instituição de saúde privada.

No âmbito da licenciatura e já licenciada, tive a oportunidade de contactar com várias instituições de saúde, nomeadamente com serviços de Radiologia, percepcionando que existe uma lida diária com dados considerados sensíveis, havendo troca dos mesmos entre serviços, departamentos ou até mesmo instituições.

Os ataques a bases de dados de saúde são cada vez mais frequentes, fazendo diariamente títulos de notícias. Assim sendo, pareceu-me pertinente fazer um levantamento das formas que existem de controlar o acesso aos dados de saúde dos doentes e percepcionar se existem algumas diferenças nesta medida de confidencialidade, consoante a índole da instituição.

O levantamento desenvolve-se no departamento de Radiologia de instituições públicas e privadas, sendo os resultados deste trabalho apresentados aqui.

Índice

Acrónimos

ACCLs	Access control capabilities lists
ACL	Access Control Lists
CA	Controlo de Acesso
CCTV	Closed Circuit Television
CNDP	Comissão Nacional de Proteção de Dados
DAC	Discretionary Access Control
ISO	Organização Internacional para Padronização
LCA	Listas de Controlo de Acesso
MAC	Mandatory Access Control
PKI	Public Key Infrastructure
RBAC	Role-based Access Control
TI	Tecnologias da Informação

Índice de figuras

Índice de tabelas

1. Introdução e Motivação

A importância da informação hospitalar é inquestionável, sendo que a partilha da mesma é indispensável para uma prática clinica eficiente. Um registo clínico pormenorizado sem falhas e redundâncias, acessível a todos os níveis de cuidados de saúde, permite uma atuação mais rápida e objetiva, por parte dos profissionais e com menor desperdício de recursos.

A informatização dos dados vem facilitar esta partilha, assim como a articulação com outras instituições e serviços, agregando informação dispersa, permitindo a circulação automática de informação e facilitando a fiscalização pelas autoridades de controlo (Almeida, 2009; Zriqat, 2016; Calberson et al., 2008; Rodrigues, 2015).

No entanto, o acesso à informação hospitalar mais precisamente aos dados considerados sensíveis, segundo a legislação a vigorar em Portugal, só é permitido: 1) ao paciente (Art.35º utilização da informática), podendo este retificá-los e atualizá-los, assim como exigir conhecer a finalidade a que se destinam; 2) a profissionais de saúde, durante todo o processo de diagnóstico/tratamento, sendo que estes estão obrigados ao sigilo profissional e devem estar garantidas as medidas de segurança da informação (art. 7.o n.o 4 da Lei 67/98, de 26/10 LPDP- Tratamento de dados de saúde); ou 3) sempre que haja disposição legal ou autorização da CNPD (Comissão Nacional de Proteção de Dados) por motivo de interesse público ou autorização do titular.

A legislação referida aplica-se a qualquer tipo de informação de qualquer natureza, independentemente do suporte, incluindo som e imagem,

relativa a uma pessoa identificada ou identificável (art. 3.º al. a) da Lei de Proteção de Dados Pessoais), abrangendo aquela que é considerada por muitos, uma das mais marcantes inovações na saúde, o registo clinico eletrónico.

Posto isto, a abordagem do tema "controlo de acesso" é incontornável sendo que este se define como a capacidade de limitar e controlar o acesso a recursos por utilizadores autorizados, de forma a garantir a integridade, a confidencialidade e a disponibilidade dos dados (Zriqat, 2016; Rodrigues, 2015).

O controlo de acesso é uma das áreas mais relevantes quando nos referimos à segurança informática, porque foca nas primeiras interações/decisões do sistema quanto a identificar, autenticar e proporcionar os recursos necessários aos utilizadores, para que estes consigam efetuar as ações necessárias com a informação que lhes é disponibilizada (Yeo et al., 2012; Pato, J. N., & Millett, 2010)

Apesar das vantagens que existem em ter a informação mais disponível e de haver legislação para a proteção da mesma na prática, o controlo de acesso apresenta diversas fragilidades ao nível da recolha dos dados, na transmissão dos mesmos assim como no seu armazenamento (Zriqat, 2016) .

Uma proteção abrangente e eficiente dos dados é um processo caro, que exige interação e integração de todos os intervenientes, assim como uma coordenação entre pessoas e tecnologias. Nos últimos dois anos foram relatados inúmeros ataques a dados em meio hospitalar, fragilizando a imagem das organizações (Zriqat, 2016). A perda de integridade dos dados pode torná-los inválidos conduzindo a tomadas de decisão erradas e desta forma atentar contra a integridade da pessoa humana, pondo em causa a competitividade com outras instituições do mesmo ramo (Abdulrahman et al., 2012; Martinho 2014).

Assim sendo, um controlo de acesso rigoroso pode ser a chave para aumentar a confiança não só de quem usufrui dos cuidados de saúde, como também de quem os pratica (Zriqat, 2016; Abdulrahman et al., 2012).

1.1 Objetivos

O principal objetivo desta tese é sumariar e comparar quais os modelos, mecanismos e políticas de controlo de acesso utilizados nas instituições de saúde públicas e privadas, mais precisamente nos departamentos de Radiologia da região Norte de Portugal.

Pretende-se assim:

a) **fazer uma recolha** de quais os modelos, mecanismos e politicas de controlo de acesso implementados nos dois tipos de instituições, em particular no departamento de Radiologia. Para além de analisarmos o que existe, é pretendido também saber se estão atualizados e como funcionam. Queremos perceber quem faz a gestão do controlo de acesso, se são profissionais ligados à informática, há quanto tempo, e se são especialistas na área da segurança informática.

A existência ou não de documentos, que regulem o controlo de acesso é outro dos pontos em que nos queremos focar, assim como o que neles consta.

Os profissionais de saúde são sem dúvida quem mais interage com as politicas de controlo de acesso, sendo uma das finalidades desta tese, saber qual a sua opinião sobre as mesmas, quais as dificuldades de interação com estas e quais consideram ser as vantagens da sua utilização/implementação na prática clinica;

b) **comparar** os modelos, mecanismos e politicas de controlo de acesso para perceber se existe alguma relação entre o tipo de instituição (pública ou privada) e perceber o porque dessas diferenças, se existirem;

c) **sugerir possíveis alterações** às medidas de controlo de acesso existentes visto estas poderem apresentar-se como barreiras ou facilitadores no *workflow* das instituições. Com base na opinião do profissionais do

departamento de Radiologia, queremos saber como classificam a adaptação às politicas de controlo de acesso, o que gostariam de ver alterado, quais pensam ser as maiores fragilidades e os pontos mais fortes dessas políticas e se é necessário muitas ações ou alterações às mesmas, aquando da admissão de novos funcionários.

1.2 Estrutura da Tese

A tese é composta por 6 capítulos principais: 1) Introdução e Motivação, 2) Estado da Arte, 3) Materiais e Métodos, 4) Resultados, 5) Discussão e Conclusões.

Capítulo 1- Abordagem inicial do tema apresentado, o que me motivou a realizar a tese, quais os principais objetivos e quais a relevância da mesma.

Capítulo 2 - Apresentação do estado da arte onde serão abordados os conceitos básicos de controlo de acesso, assim como explorados quais os mecanismos, modelos e políticas existentes.

Capítulo 3 - Descrição do estudo e recolha efetuada.

Capítulo 4 - Apresentação dos dados recolhidos.

Capítulo 5 - Análise dos dados recolhidos e discussão e apresentação de conclusões e limitações do estudo. Abordagem a possíveis trabalhos futuros.

2. Estado da arte

2.1 Controlo de Acesso

A informatização dos registos clínicos levou a um considerável aumento da eficiência e qualidade dos serviços prestados, assim como a uma redução de custos nas instituições de saúde, no entanto, levantou várias preocupações relativas à segurança e privacidade dos dados.

A segurança dos dados é um tema deveras importante quando nos referimos a sistemas de informação clínicos, uma vez que a integridade e confidencialidade dos mesmos deve ser impreterivelmente mantida. Deste modo, deve ser controlado o acesso garantindo que pessoas não autorizadas, não tenham acesso aos dados dos doentes (Khan & Sakamura, 2012; Martinho, 2014).

O controlo de acesso pode ter por base as funções dos utilizadores, a relevância dos dados e o contexto, sendo que este deve ser considerado a vários níveis, desde a recolha, a transmissão e o armazenamento (Zriqat, 2016). Deste modo, podemos definir controlo de acesso como a capacidade de limitar e controlar o acesso a usuários autorizados, recorrendo a processos de identificação, autenticação e autorização (Bai & Zheng, 2016).

A identificação, consiste no reconhecimento do usuário.

A autenticação, garante a autenticidade dos dados solicitados, assim como a validade.

A autorização é o processo que restringe os dados ao utilizador, tendo por base a política de segurança em vigor, ou seja, é a atribuição de permissões de acesso (Zriqat, 2016).

Um controlo de acesso eficaz deve garantir a privacidade dos dados, proporcionando um bom equilíbrio entre a disponibilidade e a confidencialidade dos mesmos (Zriqat, 2016).

A disponibilidade é a propriedade de um sistema acessível, utilizável e disponível por utilizadores autorizados, a qualquer momento e em qualquer lugar.

A confiabilidade garante a recuperação de dados clínicos em qualquer momento, mesmo que haja alguma falha, de forma a não prejudicar o estado do paciente. A tolerância a falhas é um requisito necessário para a confiabilidade.

A flexibilidade permite que profissionais não autorizados, acedam a dados específicos em situações de emergência (Zriqat, 2016; Ferreira, 2009).

Os meios de fornecer controlo de acesso devem ser cuidadosamente estudados dentro do ambiente de aplicação, para que o controlo de acesso possa ser corretamente desenvolvido e aplicado sem dificultar o uso do sistema (Ferreira, 2010).

2.2 Modelos, Mecanismos e Políticas de CA

Os meios de fornecer controlo de acesso tornam-se mais desafiantes à medida que as politicas se tornam mais complexas (Ferreira, 2010).

A definição de políticas de controlo de acesso estruturadas, assim como de modelos são a base do complexo processo de concepção de sistemas de controlo de acesso. Enquanto uma política de controlo de acesso descreve as regras que devem ser aplicadas para fornecer os requisitos de segurança da informação da instituição, o modelo deve ser escolhido de forma a modelar as

regras definidas na política. Existem diversos modelos de controlo de acesso: Controlo de acesso discricionário (DAC), Controlo de Acesso Obrigatório (MAC), Controlo de Acesso baseado em Funções (RBAC), entre outros (Ferreira, 2010).

Os mecanismos de autenticação permitem a identificação e autenticação de um utilizador ao sistema (por exemplo *login* e impressão digital); os mecanismos de controlo de acesso, protegem contra o uso não autorizado dos recursos solicitados (por exemplo listas de controlo de acesso e etiquetas de segurança) (Ferreira, 2010).

2.2.1 Discretionary Acess Control (DAC)

O Controlo de Acesso Discricionário (DAC) possibilita que a cedência de privilégios de controlo de acesso fique ao critério do proprietário. Este pode conceder ou revogar permissões de acesso a outros utilizadores sem a mediação de um administrador de sistema. Geralmente, o sistema identifica a identidade do utilizador permitindo ou limitando o uso de recursos, de acordo com o grau de permissão (Khan& Sakamura, 2012; Bai & Zheng, 2016; Ferreira et al., 2007).

Os mecanismos mais comuns de implementação do DAC são a matriz de controlo de acesso, lista de controlo de acesso (ACL) e listas de capacidades de controlo de acesso (ACCLs) (Khan& Sakamura, 2012; Bai & Zheng, 2016; Ferraiolo, & Kuhn, 1998).

O DAC é um dos modelos de controlo de acesso mais utilizados pelas aplicações web, mostrando-se bastante flexível. No entanto, não é o mais seguro, pois permite que utilizadores que não tenham acesso aos dados originais possam aceder a cópias dos mesmos (Ferreira et al., 2007); pouco eficiente para grandes sistemas (Ferraiolo, & Kuhn, 1998).

I. Matriz de Controlo de acesso

A matriz de controlo de acesso utiliza uma matriz bidimensional para regular as permissões de acesso de qualquer assunto e objeto (Figura 1). Cada elemento da matriz faz a associação de um utilizador a um objeto e mostra quais as operações que o utilizador tem permissões para concretizar sobre o objeto (Bai & Zheng, 2016; Ferraiolo, & Kuhn, 1998)

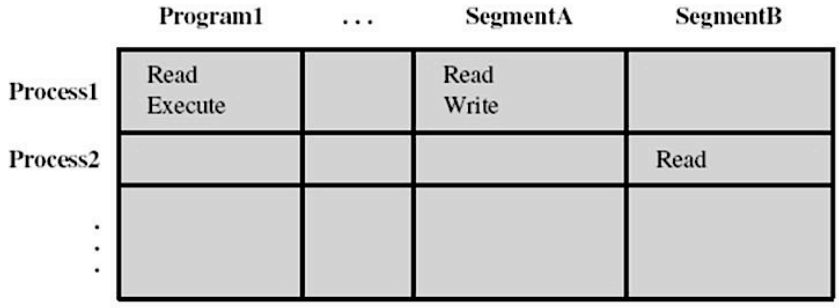

Figura 1: Matriz de Controlo de Acesso (Bai & Zheng, 2016)

A matriz de controlo de acesso não se apresenta como a melhor opção para sistemas muitos grandes visto que há grande desperdício de espaços de armazenamento, levando a baixa eficiência do sistema. Para além disso, a entrada de um novo utilizador ou de novo objeto, dependerá de uma boa gestão de memória (Khan& Sakamura, 2012; Bai & Zheng, 2016; Ferreira et al., 2007).

II. Listas de Controlo de Acesso

A ACL sumaria as operações que cada utilizador pode praticar sobre um objeto (Figura 2). Aquando do acesso, a lista é verificada pelo sistema, deliberando se o acesso é concedido ou negado.

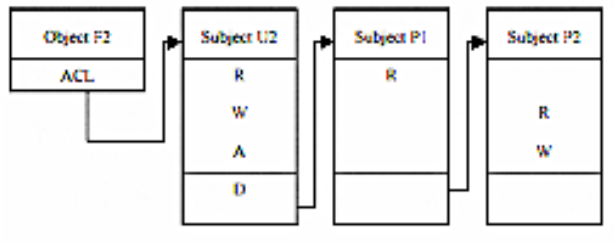

Figura 2: Listas de Controlo de Acesso (Bai & Zheng, 2016)

Desta forma é mais simples perceber se existem acessos privilegiados a objetos e quais os utilizadores que usufruem destas autorizações. Além disso, é simples anular/bloquear o acesso por um utilizador ou grupo de utilizadores a um objeto, basta apagar na ACL. Uma outra vantagem prende-se com o facto de podermos agrupar utilizadores com acessos comuns a um dado objeto, em vez de termos utilizadores individuais, que tornam as listas demasiado longas (Bai & Zheng, 2016).

Práticas, simples e convenientes assim podem ser caracterizadas as ACL, pontos que fazem com sejam usadas como estratégias de controlo de acesso de muitos sistemas operativos (Bai & Zheng, 2016; Ferreira et al., 2007; Ferraiolo, & Kuhn, 1998).

No entanto, estas devem ser verificadas rigorosamente, pois uma vez que se são agrupados utilizadores, a entrada de novos elementos num determinado grupo, pode alterar os objetos acessíveis a qualquer membro (Ferraiolo, & Kuhn, 1998).

III. Listas de Controlo de Acesso de capacidades (ACCLs)

ACCLs armazenam linhas de capacidades. A capacidade é um elemento da matriz de controlo de acesso, que representa um par, objeto/permissão (Figura 3) (Ferraiolo, & Kuhn, 1998).

O que define o mecanismo de capacidades é o facto de estas serem transferíveis entre utilizadores, isto é, não é relevante quem apresenta a capacidade. Desta forma, elimina-se a necessidade de autenticação (Bai & Zheng, 2016).

Basicamente, as ACCLs permitem-nos saber que operações o utilizador pode praticar sobre um objeto (figura 3); enquanto que as ACL, possibilitam perceber quais os utilizadores autorizados a executar ações sobre um objeto(Bai & Zheng, 2016; Lampson, 2009).

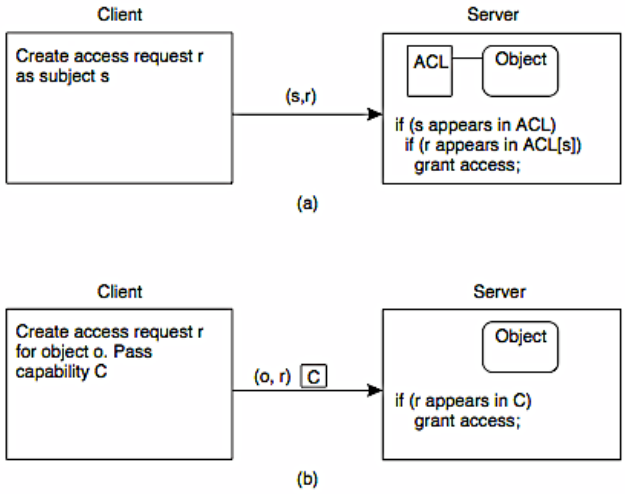

Figura 3: Comparação entre ACL e ACCLs (Lampson,2009)

Assim sendo, a maior vantagem é a facilidade com que se pode verificar todos os acessos autorizados para um dado assunto. No entanto, por outro

lado, é difícil confirmar quais os utilizadores que podem aceder a um determinado objeto (Ferraiolo, & Kuhn, 1998).

A revogação de direitos de acesso é um processo difícil e complexo, apresentando-se também como uma desvantagem. Esta requer a eliminação de todas as capacidades associadas ao objeto, podendo a solução passar por usar "indirecção" (Ferraiolo, & Kuhn, 1998).

O sucesso do mecanismo baseado em capacidades está dependente de as tornar-mos "inesquecíveis", tendo à disposição uma vasta gama de possibilidades:

Criptografia - É usada para codificar uma entrada e produzir um texto cifrado que é difícil de decifrar sem uma chave. Deste modo, além da identidade e das permissões, incluímos uma assinatura digital, que garante a integridade, tornando a capacidade indecifrável aos programas que não podem ter acesso (Ferraiolo, & Kuhn, 1998).

Segurança baseada em linguagem - Impor restrições de acesso e modificação de recursos, usando uma linguagem de programação para impor restrições (Ferraiolo, & Kuhn, 1998).

Espaço de endereços protegidos - armazenamento de capacidades em partes da memória inacessíveis aos programas (Ferraiolo, & Kuhn, 1998).

Tags de hardware - Cada palavra tem um tag de 1 bit associada. O tag "on" significa que os programas não podem alterar ou copiar essa palavra (porque ela armazena uma capacidade) (Ferraiolo, & Kuhn, 1998).

2.2.2 Mandatory Acess Control (MAC)

O MAC é "Um meio de restringir o acesso a objetos com base na sensibilidade (como representada por um rótulo) das informações contidas nos objetos e na autorização formal para aceder a informações com essa sensibilidade" (Khan& Sakamura, 2012).

Neste modelo, existe uma autoridade central, o administrador de sistema, responsável pelas decisões, não estando as mesmas a cargo do proprietário individual dos objetos. No caso do tipo de sistema operativo usado pelo Mac, o utilizador não pode modificar os direitos/privilégios de acesso (Khan& Sakamura, 2012; Bai & Zheng, 2016; Ferreira et al., 2007).

No Mac os níveis de segurança contemplam as vertentes hierárquicas (unclassified-U, confidencial-C, secret-S e top-secret-TS) e não hierárquicas (NATO e NUCLEAR). Neste modelo, qualquer comportamento que não respeita o fluxo de informação acíclico unidirecional, é proibido (Ferraiolo, & Kuhn, 1998).

Geralmente, o nível de segurança atribuído a um dado objeto, é reflexo da sensibilidade de conteúdos do mesmo.

Quando comparado com o DAC, o MAC inclui um controlo de acesso mais rigoroso, podendo ultrapassar problemas como erros nos programas ou falsos utilizadores. No entanto, é um modelo pouco flexível e difícil de implementar e gerir (Bai & Zheng, 2016; Ferraiolo, & Kuhn, 1998)

2.2.3 Role-based access control (RBAC)

O RBAC baseia as decisões de acesso nas funções e responsabilidades que os utilizadores desempenham/têm na instituição. Basicamente, este modelo associa a autoridade de acesso ao papel do utilizador (Bai & Zheng, 2016; Bugliesi et al. 2012).

Deste modo, o processo de definição de papéis deve fundamentar-se numa análise completa, que contemple a forma de funcionamento, assim como na entrada de um amplo espectro de funcionários na instituição (Khan & Sakamura, 2012; Bugliesi et al. 2012).

O administrador agrega papéis diferentes, em diferentes conjuntos de operações, atribuindo-lhe funções. O utilizador desempenha funções, apenas em alguns departamentos e as operações que pratica têm de estar de acordo com a sua função. Quando as funções de um utilizador são alteradas, as operações que este pode praticar sofrem também elas alterações. O administrador de sistema deve legar ou cancelar funções a utilizadores (Bai & Zheng, 2016; Ferrara & Warinschi, 2013).

O RBAC tem por fundamento três princípios de segurança: o princípio do menor privilégio, princípio de separação de responsabilidades e o princípio de abstração de dados (Ferraiolo & Kuhn, 1998).

Principio do menor privilégio- No momento de atribuir privilégios a utilizadores, a prática administrativa eleita é a do menor privilégio, de maneira que o utilizador não tenha acesso a mais do que o estritamente necessário para desempenhar as funções inerentes ao seu trabalho. Desta forma, conseguem evitar-se vários problemas, uma vez que o utilizador não consegue realizar ações desnecessárias e potencialmente perigosas (Ferraiolo, & Kuhn, 1998).

Privilégios são direitos deferidos a utilizadores, que possibilitam ao detentor desses direitos agir no sistema dentro dos limites, desses mesmos direitos (Bai & Zheng, 2016; Ferraiolo, & Kuhn, 1998).

A atribuição de privilégios, neste caso privilégio mínimo, exige que sejam identificadas as funções de trabalho, assim como a especificação dos privilégios necessários para desempenhar cada uma delas, restringindo o utilizador a um domínio com apenas esses privilégios (Ferraiolo & Kuhn, 1998).

Princípio de separação de autoridades – Consiste em papéis mutuamente exclusivos a ser ativados simultaneamente para complementar uma determinada tarefa, isto é, o particionamento de tarefas e privilégios associados entre diferentes funções associadas a um único utilizador, de forma a impedir que os utilizadores se conciliem entre si (Ferraiolo, & Kuhn, 1998).

Princípio da abstração de dados- Consiste em abstrair as autoridades de gestão e a não inclusão de operações diretas aos objetos como adicionar, apagar, ler, escrever e executar (Bai & Zheng, 2016).

O modelo de segurança RBAC considera-se abstrato e geral. Abstracto na medida em que não se incluem propriedades que não sejam consideradas relevantes na segurança; geral porque existem várias interpretações válidas do modelo(Cotrini & Clavel, 2015). Os recursos deste modelo alternam entre simples e complexos, sendo o principal objetivo facilitar a gestão e revisão das autorizações (Cotrini & Clavel, 2015).

A generalidade inerente ao RBAC possibilita uma ampla gama de possíveis implementações, que têm a capacidade de se aplicar a diferentes ambientes com base no seu objetivo de controlo e perfil de risco (Ferraiolo, & Kuhn, 1998; Cotrini & Clavel, 2015).

De forma a preservar as características e motivações base do RBAC, foi desenvolvida uma taxonomia que permita distinguir as características incorporadas, consistindo esta em quatro modelos: RBAC central, RBAC hierárquico, RBAC estático limitado e RBAC dinâmico restrito (Ferraiolo, & Kuhn, 1998).

O RBAC é utilizável como base para a concepção de uma grande variedade de sistemas TI, mostrando-se um modo de controlar o acesso eficaz, quando se trata de implementar uma estratégia de segurança orientada à instituição (Khan& Sakamura, 2012). Este modelo, quando comparado com outros já referenciados, mostra flexibilidade, conveniência e segurança, sendo largamente aplicado no gerenciamento de sistemas de bases de dados (Bai & Zheng, 2016). Deste modo, o RBAC pode ser considerado o padrão de controlo de acesso da indústria (Khan& Sakamura, 2012; Cotrini & Clavel, 2015).

2.3 Controlo de Acesso na Saúde

As tecnologias da informação são cada vez mais reconhecidas como uma ferramenta importante para melhorar a segurança e a qualidade dos cuidados de saúde, promovendo a medicina baseada em evidência (Martinho& Varajão 2014).

Considerando a vasta gama de TI na saúde utilizadas atualmente, o registo médico eletrónico (EMR), destaca-se por possuir elevada capacidade de abrangência e, portanto, maior potencial para melhor a qualidade dos cuidados prestados (Rodrigues, 2015).

A melhoria da qualidade dos cuidados verifica-se em termos de registo de procedimentos e visualização, prescrição e teste, gestão de lembretes de cuidados e mensagens, entre outras (Miller & Sim,2004).

O paradigma dos cuidados partilhados tem por base os EMR, sejam eles centralizados ou descentralizados, apontando-os como essenciais em sistemas de informação hospitalar e redes de saúde (Blobel, 2004).

A implementação dos EMR facilita não só o acesso aos dados clínicos por parte de instituições e profissionais, mas também por parte dos proprietários dos dados clínicos, os pacientes. À medida que as TI tornam os registos médicos mais acessíveis aos pacientes, estes podem revê-los e alterá-los (segundo a orientação de profissionais). Segundo (Ross& Lin,2003), este acesso aos dados clínicos por parte do paciente tem modestos benefícios, por exemplo, no aprimoramento da comunicação médico-paciente; mas apresenta riscos como, aumentar a preocupação ou confusão do paciente em relação ao seu estado de saúde, podendo por em causa todo o processo terapêutico.

O controlo de acesso é uma parte essencial do EMR garantindo a sua confidencialidade, verificando se um utilizador, possui os direitos necessários para aceder aos recursos que solicitou.

Os EMR possuem uma arquitetura baseada em modelos e padrões internacionais, permitindo a comunicação e a cooperação entre organizações, mediante a existência de autorização de acesso. Portanto devem ser estabelecidos modelos, métodos e ferramentas, que definam uma política estruturada de controlo de acesso (Blobel, 2004).

A política de segurança assegura o complacente das implicações legais, éticas, sociais, organizacionais, psicológicas, funcionais e técnicas para a confiabilidade dos sistemas de informação de saúde, e formulam o conceito de requisitos e condições para a criação de confiança, armazenamento, processamento e uso de informações sensíveis (Blobel, 2004).

As políticas básicas, mais comuns passam por:

• políticas de autorização que definem ações permitidas, portanto, contendo assunto (exceto em funções), alvo, ação;
• políticas de obrigação que são desencadeadas por eventos e definem ações para serem implementadas pelos utilizadores, portanto, contendo o assunto (exceto nas funções), ação, evento;
• abster-se de políticas que definem ações que os sujeitos devem abster-se de realizar, portanto, conter o assunto (exceto em papéis), ação;
• políticas de delegação que definem quais autorizações podem ser delegadas, e a quem (Blobel, 2004).

Enquanto uma política de controlo de acesso descreve as regras que devem ser aplicadas para fornecer os requisitos de segurança da informação da instituição; o modelo deve ser escolhido, de forma a modelar as regras definidas na política (Bai & Zheng, 2016).

Os mecanismos de autenticação através de processos de identificação, autenticação e autorização, levam a cabo as políticas e modelos a vigorar (Bai & Zheng, 2016). Uma possível estrutura de autenticação foi especificada, por exemplo, na ISO 9798 e ISO 10181. Existem ainda vários procedimentos de

autenticação, podendo referir como exemplo os baseados numa infraestrutura de chave pública (PKI) (Blobel,2004).

Segundo Ferreira et al., a maioria dos sistemas de controlo de acesso, que são publicados na literatura são apenas estudos ou protótipos, nos quais os profissionais de saúde ou os pacientes não participaram da definição das políticas, modelos ou mecanismos de controlo de acesso (Ferreira et al., 2010). O envolvimento dos profissionais de saúde na definição e aprimoramento das políticas de controlo de acesso, pode tornar a segurança da informação mais fundamentada nos seus fluxos de trabalho e práticas diárias (Ferreira et al., 2010), evitando assim alterar os mesmos fluxos para tentar adaptar as suas tarefas e processos aos sistemas. Se o controlo de acesso puder ser melhorado de acordo com as necessidades dos profissionais de saúde e adequadamente adaptado aos seus padrões de fluxo de trabalho, a hipótese de que são barreiras ao uso efetivo de EMR seria provavelmente refutada. Desta forma, os EMR poderiam ser mais bem-sucedidos, proporcionando um melhor tratamento do paciente assim como da sua informação e privacidade (Ferreira et al., 2007)

Na verdade, apesar da recente pesquisa na elaboração de normas e regulamentos em matéria de segurança e privacidade nos sistemas de EMR, ainda não estão completamente resolvidos os seus desafios de privacidade (Zriqat, 2016).

Lovis et al. (2007) apresenta algumas soluções com o objetivo desafiante de proteger a privacidade do paciente dentro dos limites regulamentares, mantendo o sistema operacional em termos de uso e gestão. As principais características do sistema são: (a) uma política de controlo de acesso a toda a instituição para o registo informatizado do paciente; (b) uma gestão institucional dos contratos dos colaboradores; (c) perfis de acesso com base em direitos de acesso independentes e de qualidade; (d) uma atribuição descentralizada de perfis de acesso específicos da profissão; (e) um registo

completo e centralizado de todos os acessos ao sistema de informação clínica; e (f) uma verificação descentralizada dos acessos.

No entanto, a educação dos profissionais é componente importante para uma gestão bem sucedida da segurança da informação.

A forma de determinar as soluções adequadas e as modificações na educação dos profissionais em relação ao controlo de acesso, passa por conhecer o ponto de situação em que a instituição se encontra e ter à disposição uma ferramenta adequada de monitorização e auditoria. Contudo, segundo Landolt et al., não existe nenhum estudo que compare hospitais, ou instituições de saúde semelhantes, em relação à segurança da informação (ou, mais especificamente, ao controlo de acesso), uma vez que este tipo de estudos integra dados sensíveis que podem influenciar a credibilidade da instituição de saúde. Outra razão pode prender com o fato de não existir uma ferramenta de referência que facilite a avaliação do estado da segurança da informação de uma dada instituição.

Landolt et al., faz também referência à Radiologia como uma das áreas em que cada vez mais é difícil proteger e manter a integridade das imagens contra manipulações não autorizadas.

Assim sendo, e uma vez que não existem estudos na literatura que verificam as condições de controlo de acesso na área de Radiologia, quer em instituições de saúde públicas, quer privadas, o presente trabalho focou em realizar tal estudo, que compara o controlo de acesso aos dados clínicos no Departamento de Radiologia, entre instituições de saúde públicas e privadas na região norte de Portugal, tendo por base requisitos e conhecimento adquirido na revisão da literatura efetuada no decurso deste trabalho (Anexo I).

3. Material e Métodos

3.1. Visão geral

O presente trabalho foi desenvolvido no âmbito do Mestrado em Informática Médica da Faculdade de Medicina da Universidade do Porto, e aplicado nos departamentos de Radiologia, em quatro instituições de saúde da região Norte do país, sendo que destas, duas eram de natureza privada e duas de natureza pública.

A fim de comparar a existência de diferenças nos mecanismos, modelos e políticas de controlo de acesso no departamento de Radiologia destas instituições, foram elaborados dois questionários, um para levantamento geral de informação, aplicado aos responsáveis do Departamento de Radiologia e outro aplicado aos restantes profissionais, com base na revisão da bibliografia já retratada.

A aplicação dos questionários foi aprovada pelas Comissões de Ética das quatro instituições, assim como pelos responsáveis dos Departamentos de Radiologia e Sistemas de Informação das mesmas.

Nas instituições em causa, foi ainda entregue um termo de responsabilidade, garantindo a confidencialidade dos dados durante todo o projeto, assim como em qualquer divulgação ou publicação de resultados, respeitando a Declaração de Helsínquia.

Deste modo, designaremos as instituições públicas como 1 e 2; as privadas como 3 e 4, garantindo assim a anonimidade das mesmas.

3.2 Elaboração dos instrumentos de recolha

Considerando a revisão bibliográfica efectuada (figura4 e Anexo I), não foram encontrados estudos idênticos, assim como ferramentas de recolha de dados, que se adaptassem às necessidades do presente trabalho. Desta forma, foram elaborados: a) um questionário (Anexo II), que se destinava a todos os profissionais do departamento de Radiologia (médicos, enfermeiros, técnicos, administrativos, auxiliares, entre outros); e b) um levantamento (Anexo III) para três responsáveis (diretor clínico, técnico coordenador e responsável informático).

O questionário (Anexo II) e o levantamento eram precedidos de um esclarecimento sobre o estudo, assim como da garantia de anonimidade e confidencialidade quer dos participantes, quer das instituições envolvidas. Estes instrumentos apresentavam questões de resposta múltipla (maioritariamente) e resposta curta, sendo que nas primeiras foi utilizado o mesmo *layout* e ordem de respostas para reduzir a complexidade visual.

O levantamento (Anexo III) continha questões para uma abordagem mais geral do que existe na instituição e em particular no Departamento de Radiologia, como por exemplo o número de camas, número de profissionais, índole da instituição, inclusão de departamento de informática, os mecanismos e os modelos de controlo de acesso, assim como a formação dos profissionais responsáveis pelos mesmos.

O questionário englobava as mesmas questões do levantamento, relativas aos modelos, mecanismos e políticas de controlo de acesso, de forma a poder comparar respostas. No entanto, o foco do questionário, passava não

tanto por saber o que existe, mas como é que os profissionais lidam com o que está implementado e o que pensam ser mais importante, quanto ao controlo de acesso (Ver Anexo II).

De forma a garantir a funcionalidade técnica dos instrumentos de recolha, cada um deles foi aplicado a quinze participantes teste, sem qualquer ligação às instituições de recolha, de variadas áreas profissionais (informática, saúde, ensino, administração).

Tendo em consideração as críticas apresentadas, foram retificados alguns pontos e estimado como tempo médio de preenchimento dez minutos.

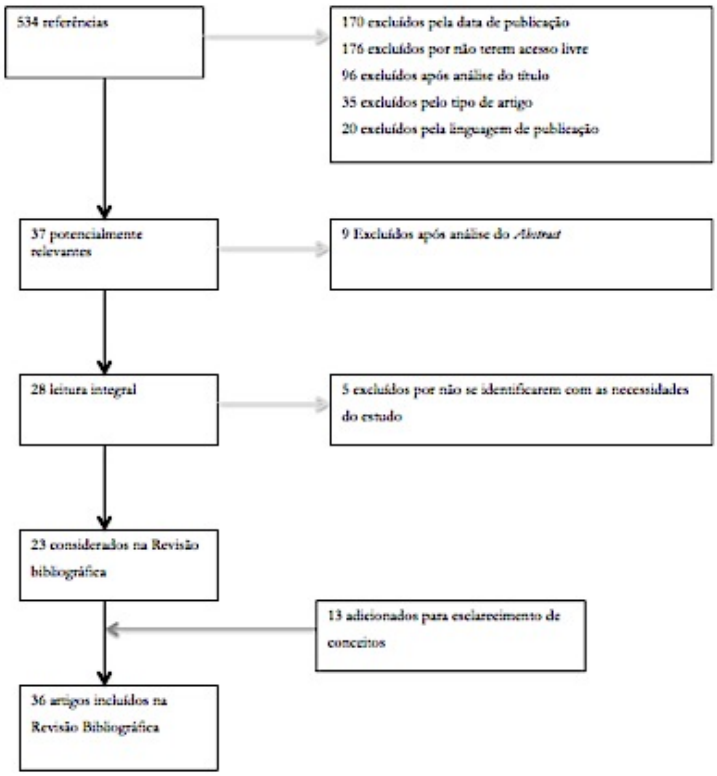

Figura 4: Fluxograma Revisão Bibliográfica (Anexo I)

3.3 População alvo

A população alvo deste estudo foram os profissionais dos Departamentos de Radiologia de quatro instituições de saúde da região Norte de Portugal (duas privadas e duas públicas), que de forma livre e esclarecida, mostraram disponibilidade para o preenchimento dos questionários/ levantamentos, disponibilizados no departamento.

Os instrumentos de recolha foram disponibilizados juntamente com um elo de ligação, um membro do departamento selecionado pela instituição, de forma a garantir a participação apenas de profissionais pertencentes ao mesmo.

3.4 Desenho de estudo e implementação

A aplicação dos objetos de recolha foi subdividida em duas etapas: aplicação dos levantamentos (Figura 5) e aplicação dos questionários (Figura 6).

No emprego dos levantamentos reservaram-se dois dias, uma vez que eram apenas três em cada instituição e que estes se destinavam a profissionais com horário fixo.

Quanto aos questionários, foram reservados cinco dias, considerando que a população alvo destes trabalha por turnos e desta forma seria possível abranger um maior número de profissionais.

No dia 1 foi conhecido o elo de ligação das instituições públicas e entregues os três levantamentos, destinados a responsáveis. O mesmo sucedeu no dia 2, mas nas instituições privadas.

Concluída a primeira etapa, no dia 3 iniciou-se a aplicação dos questionários, nas instituições públicas, sendo que dos 50 questionários

disponibilizados em cada uma das instituições, apenas foram recolhidos 10 na instituição 1 e 15 na instituição 2.

No dia 4, prosseguiu-se com a recolha de questionários nas instituições públicas, conseguindo reunir 7 na instituição 1 e 15 na instituição 2.

No dia 5, regressou-se à instituição 1, uma vez que nas duas primeiras visitas os profissionais presentes no serviço eram praticamente os mesmos, recolhendo 13 questionários.

No dia 6, foram entregues 50 questionários em cada uma das instituições privadas, tendo recolhido 20 na instituição 3 e 12 na instituição 4.

No dia 7, recolheram-se 13 questionários na instituição 4 e visitou-se a instituição 3, mas sem qualquer recolha.

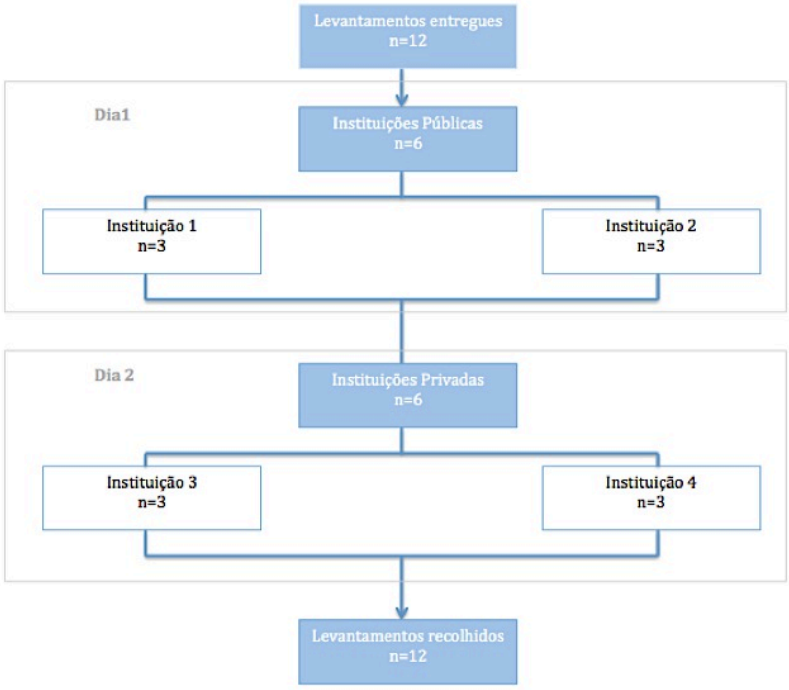

Figura 5: Fluxograma aplicação de Levantamentos

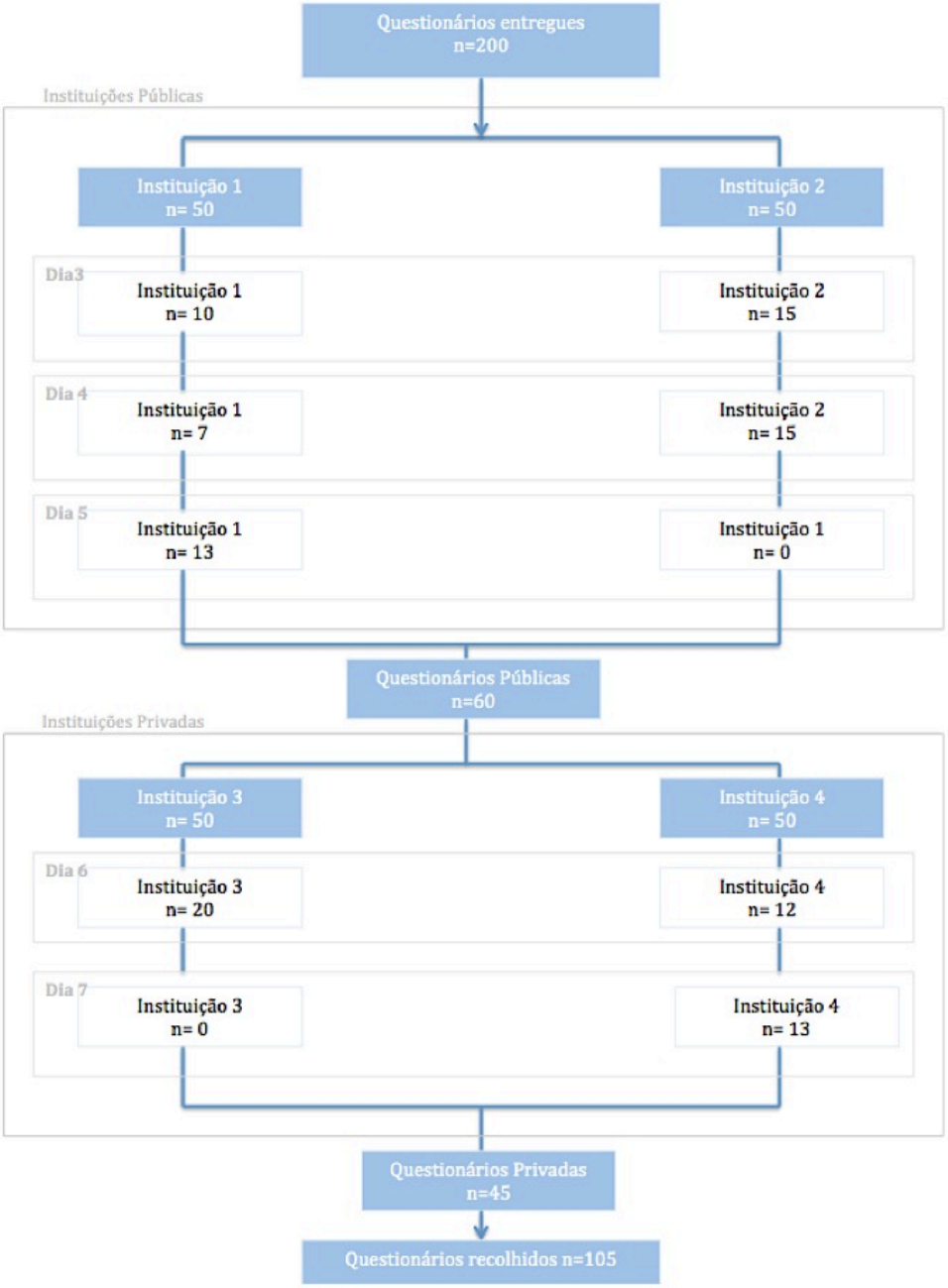

Figura 6: Fluxograma aplicação dos Questionários

3.5 Análise Estatística

Na análise estatística considerou-se uma amostra de 105 inquiridos, não tendo sido considerados os 12 levantamentos, uma vez que o método de recolha destes, não foi o apropriado considerando a sua finalidade, factor esclarecido mais à frente na seção 5.2 "Limitações".

A análise foi realizada com recurso do software GNU PSPP, versão 0.10.4.

De forma a caracterizar a amostra, recorreu-se à estatística descritiva.

Na análise estatística dos dados recolhidos utilizamos o teste do Qui-Quadrado baseado em tabelas de contingência, uma vez que este permite verificar a independência entre duas variáveis que, sendo expressas em qualquer escala, se apresentam agrupadas em classes mutuamente exclusivas e exaustivas, como aliás é descrito por (Guimarães, 1999).

4. Resultados

4.1 Descrição da Amostra

A amostra é composta por 105 indivíduos, 59 do sexo feminino (58,10%) e 46 do sexo masculino (41,90%). Destes indivíduos, 60 (57,14%) pertencem a instituições públicas e 45 (42,86%) a instituições privadas.

A maioria dos profissionais inquiridos tem idades compreendidas entre os 36 e os 55 anos (66,67%) (figura 8) e pertence à categoria dos Técnicos de Diagnóstico e Terapêutica (54,29%) (figura 7). Relativamente aos anos de experiência na instituição em estudo apenas 3 têm menos de 1 ano (2,86%); 24 apresentam entre 1 a 5 anos de experiência (22,86%); 36 têm entre 6 a 10 anos de experiência (34,29%); 41 trabalham na instituição há mais de 10 anos (39,05%); e 1 optou por não responder (0,95%).

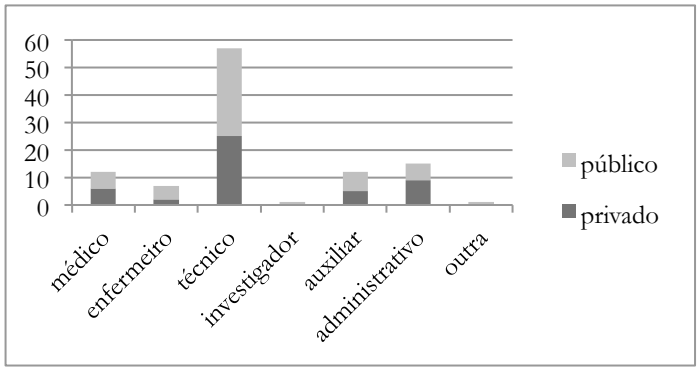

Figura 7: Número de inquiridos por Categoria Profissional

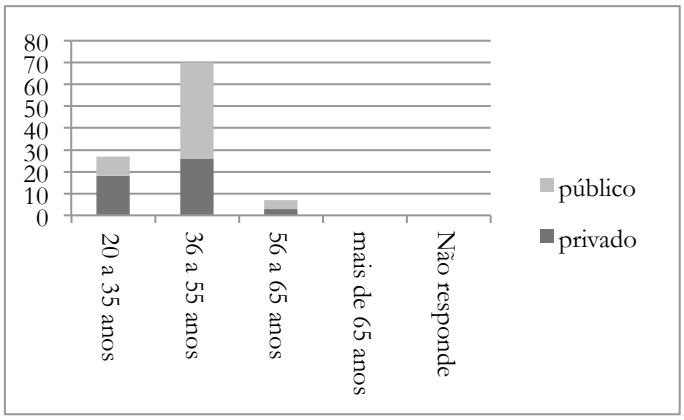

Figura 8: Número de inquiridos por faixa etária

4.2 Comparação de Instituições Públicas e Privadas

Foram elaboradas tabelas de contingência com base nas respostas ao "Questionário" (Anexo II), de forma a percepcionar se os dois tipos de instituições de saúde independentes, Privadas e Públicas, diferem relativamente a uma determinada característica, e assim poder efetuar comparação entre elas. É de referir, que as tabelas apresentadas foram selecionadas porque representam as questões em que houve menor número de não resposta.

Desta forma expõe-se a percentagem de indivíduos de cada tipo de instituição, que selecionou cada opção de resposta.

4.2.1 Tipo de Instituição e acesso aos dados em papel

O objetivo deste teste é verificar se a restrição de acesso aos dados em papel dos doentes depende do tipo de instituições inquiridas, ou seja, se depende se a instituição é pública ou privada (Tabela 1).

Tabela 1: Relação entre o tipo de instituição e o acesso aos dados em papel. Resultados em percentagem e valor absoluto

	Pergunta 1.1 do questionário				
Tipo de Instituição	**A**	**B**	**C**	**D**	**Total**
PRIV	28,00	10,00	,00	1,00	39,00
(%)	71,79	25,64	,00	2,56	100,00
PUB	12,00	18,00	4,00	1,00	35,00
(%)	34,29	51,43	11,43	2,86	100,00
Total	40,00	28,00	4,00	2,00	74,00
(%)	54,05	37,84	5,41	2,70	100,00

A- Não tenho acesso aos dados de todos os doentes do departamento de Radiologia; **B** – Sim, tenho acesso aos dados que necessito para realizar o meu trabalho; **C**- Sim, apenas consigo aceder a parte do que necessito para o meu trabalho; **D** - Não aplicável.

Conclui-se que o tipo de instituição condiciona ($P<0.010$) o acesso aos dados em formato de papel. Destaca-se que 71.79% dos funcionários das instituições privadas, conseguem ter acesso a todos os dados em formato de papel do Departamento de Radiologia. Este valor contrasta com os 34.29% dos funcionários das instituições públicas.

4.2.2. Tipo de Instituição e mecanismo de autenticação

O objetivo deste teste é verificar se os mecanismos de autenticação utilizados para aceder aos dados dos doentes em formato eletrónico depende do tipo das instituições inquiridas, ou seja, se depende se a instituição é pública ou privada (Tabela 2).

Tabela 2: Relação entre o tipo de instituição e o mecanismo de autenticação. Resultados em percentagem e valor absoluto

	Pergunta 2.3 do questionário			
Tipo de Instituição	**A**	**AB**	**D**	**Total**
PRIV	29,00	,00	5,00	34,00
(%)	85,29	,00	14,71	100,00
PUB	42,00	6,00	3,00	51,00
(%)	82,35	11,76	5,88	100,00
Total	71,00	6,00	8,00	85,00
(%)	83,53	7,06	9,41	100,00

A – Login/Password; **B** – Smart-Card; **D** – Não existem mecanismos de autenticação.

Conclui-se que não existe uma dependência significativa (P>0.050) entre os mecanismos de autenticação utilizados para aceder aos dados dos doentes em formato eletrónico e o tipo de instituição, ou seja, os mecanismos de autenticação utilizados são estatisticamente semelhantes entre o tipo de instituições, sendo o *Login/password* o mecanismo preferencial.

4.2.3 Tipo de Instituição e modelo de CA

O objetivo deste teste é verificar se os modelos de controlo de acesso a dados clínicos dos doentes em formato eletrónico dependem do tipo das instituições inquiridas, ou seja, se variam quando a instituição é pública ou privada (Tabela 3).

Tabela 3: Relação entre o tipo de instituição e o modelo de CA. Resultados em percentagem e valor absoluto

	Pergunta 3 do questionário						
Tipo de Instituição	**A**	**AB**	**B**	**C**	**D**	**N**	**Total**
PRIV	26,00	1,00	1,00	3,00	5,00	9,00	45,00
(%)	57,78	2,22	2,22	6,67	11,11	20,00	100,00
PUB	51,00	1,00	2,00	,00	1,00	5,00	60,00
(%)	85,00	1,67	3,33	,00	1,67	8,33	100,00
Total	77,00	2,00	3,00	3,00	6,00	14,00	105,00
	73,33 %	1,90 %	2,86 %	2,86 %	5,71%	13,33%	100,00 %

A – Grupo de utilizadores de acordo com as suas funções na instituição; **B** – Necessidades especificas de cada utilizador; **C** – Regras obrigatórias para todos os utilizadores do sistema; **D** – Não existe controlo de acesso; **N** – Não responderam.

Conclui-se que existe uma dependência significativa ($P<0.050$) entre os modelos de controlo de acesso a dados clínicos dos doentes em formato eletrónico e o tipo das instituições inquiridas, ou seja, depende se a instituição é pública ou privada. Destaca-se que 85% dos profissionais inquiridos nas instituições públicas afirmam que os modelos de controlo de acesso a dados clínicos dos doentes em formato eletrónico são baseados em grupos de

utilizadores de acordo com as suas funções nas instituições, ou seja, um modelo RBAC, pois associa a autoridade de acesso ao papel do utilizador. Já nas instituições privadas apenas 57% dos profissionais inquiridos responderam da mesma forma, sendo que 20 % optaram por não responder. Outro aspecto relevante é que no público apenas 1,67 % refere não existir qualquer modelo de CA a dados clínicos em formato eletrónico, enquanto no privado 11,11% refere esta inexistência.

4.2.4 Tipo de instituição e partilha de credenciais de acesso

O objetivo deste teste é verificar se existe uma associação entre o tipo de instituição e a partilha com colegas das credenciais de acesso aos dados dos doentes (Tabela 4).

Tabela 4: Relação entre o tipo de instituição e a partilha das credenciais. Resultados em percentagem e valor absoluto

	Pergunta 2.6 do questionário				
Tipo de Instituição	**A**	**B**	**C**	**N**	**Total**
PRIV	13,00	15,00	6,00	6,00	40,00
(%)	32,50	37,50	15,00	15,00	100,00
PUB	1,00	48,00	3,00	2,00	54,00
(%)	1,85	88,89	5,56	3,70	100,00
Total	14,00	63,00	9,00	8,00	94,00
	14,89%	67,02%	9,57 %	8,51 %	100,00%

A – Sim; **B** – Não; **C** – Não respondo; **N** – Respostas em branco.

Conclui-se que existe uma associação (P<0.005) entre o tipo de instituição e a partilha com colegas das credenciais de acesso aos dados dos doentes. De notar que 88.89% dos profissionais do público afirmam não partilhar as suas credências com colegas, em contraste com os 37.50% dos profissionais no privado que também afirmam não partilhar as credenciais. No privado 13 profissionais afirmaram partilhar as suas credenciais, enquanto no público tal foi afirmado apenas por 1. Mais se acrescenta que , no privado 6 profissionais não responderam e no público apenas 2.

4.2.5 Tipo de instituição e existência de documento regulamentador

O objetivo deste teste é verificar se existe uma associação entre o tipo de instituição e o conhecimento por parte dos profissionais inquiridos da existência de algum documento institucional que regulamente a segurança ou o acesso aos dados clínicos e pessoais dos doentes (Tabela 5).

Tabela 5: Relação entre o tipo de instituição e a existência de um documento regulamentador. Resultados em percentagem e valor absoluto

	Pergunta 9 do questionário				
Tipo de Instituição	**A**	**B**	**C**	**N**	**Total**
PRIV	5,00	19,00	14,00	7,00	45,00
(%)	11,11	42,22	31,11	15,56	100,00
PUB	6,00	13,00	33,00	8,00	60,00
(%)	10,00	21,67	55,00	13,33	100,00
Total	11,00	32,00	47,00	15,00	105,00
	10,48%	30,48%	44,76%	14,29%	100,00%

A- Sim; **B** – Não; **C**- Não Sei; **N** – Respostas em branco.

Conclui-se que não existe uma associação (P>0.050) entre o tipo de instituição e o conhecimento por parte dos profissionais inquiridos da existência de algum documento institucional que regulamente a segurança ou o acesso aos dados clínicos e pessoais dos doentes. No privado, 42,22 % dos profissionais refere não existir qualquer documento, enquanto 31,11% refere não saber; no público 21,67% afirma a não existência do documento regulamentador, enquanto que mais de metade dos inquiridos deste tipo de instituição afirma não saber se tal documento existe (55%). Destaca-se apenas que 14.29% dos inquiridos, privado e público, optou por não responder a essa questão.

4.2.6 Idade e adaptação aos modelos de CA

O objetivo deste teste é verificar se existe uma associação entre a idade dos profissionais e a adaptação dos profissionais aos modelos de controlo de acesso (Tabela 6).

Tabela 6: Relação entre a idade dos profissionais e a adaptação aos modelos de CA. Resultados em percentagem e valor absoluto

	Pergunta 3.1 do questionário						
Idade	**A**	**B**	**C**	**D**	**E**	**N**	**Total**
20-35 anos	1,00	1,00	2,00	9,00	5,00	4,00	22,00
(%)	4,55	4,55	9,09	40,91	22,73	18,18	100,00
36-55 anos	1,00	1,00	7,00	36,00	10,00	6,00	61,00
(%)	1,64	1,64	11,48	59,02	16,39	9,84	100,00
56-65 anos	,00	,00	4,00	3,00	,00	,00	7,00
(%)	,00	,00	57,14	42,86	,00	,00	100,00
Mais de 65 anos	,00	,00	1,00	,00	,00	,00	1,00
(%)	,00	,00	100,00	,00	,00	,00	100,00
Total	2,00	2,00	14,00	48,00	15,00	10,00	91,00
	2,20%	2,20%	15,38%	52,75 %	16,48%	10,99%	100,00%

A – muito difícil; **B** – difícil; **C** – neutro; **D** – fácil; **E** – muito fácil; **N** – Respostas em branco

Conclui-se não existe uma associação (P>0.050) entre a idade dos profissionais de radiologia e a adaptação dos mesmos profissionais aos modelos de controlo de acesso em uso. Ou seja, a adaptação dos profissionais de radiologia aos modelos de controlo de acesso não depende da idade dos inquiridos.

4.2.7 Restrição do Acesso aos dados em papel

O objetivo deste teste é verificar se o tipo de dados dos doentes consultados em formato de papel depende da categoria profissional dos profissionais do departamento de radiologia das instituições inquiridas (Tabela 7).

Tabela 7: Relação entre a restrição do acesso aos dados em papel e a categoria profissional. Resultados em percentagem e valor absoluto

	Pergunta 1 do questionário											
Categoria Profissional	**A**	**ABCD**	**AC**	**ACD**	**AD**	**AF**	**BC**	**C**	**D**	**E**	**N**	**Total**
Médico	1,00	7,00	1,00	,00	,00	,00	,00	1,00	,00	2,00	,00	12,00
(%)	8,33	58,33	8,33	,00	,00	,00	,00	8,33	,00	16,67	,00	100,00
Enfermeiro	,00	1,00	1,00	,00	2,00	,00	,00	,00	,00	1,00	2,00	7,00
(%)	,00	14,29	14,29	,00	28,57	,00	,00	,00	,00	14,29	28,57	100,00
Técnico	24,00	11,00	3,00	1,00	1,00	,00	1,00	,00	,00	12,00	4,00	57,00
(%)	42,11	19,30	5,26	1,75	1,75	,00	1,75	,00	,00	21,05	7,02	100,00
Investigador	,00	,00	,00	,00	,00	,00	,00	,00	1,00	,00	,00	1,00
(%)	,00	,00	,00	,00	,00	,00	,00	,00	100,00	,00	,00	100,00
Auxiliar	1,00	4,00	1,00	,00	,00	,00	,00	,00	,00	6,00	,00	12,00
(%)	8,33	33,33	8,33	,00	,00	,00	,00	,00	,00	50,00	,00	100,00
Administ.	4,00	5,00	1,00	1,00	,00	1,00	,00	,00	,00	,00	3,00	15,00
(%)	26,67	33,33	6,67	6,67	,00	6,67	,00	,00	,00	,00	20,00	100,00
Outra	,00	,00	,00	,00	,00	,00	,00	,00	,00	1,00	,00	1,00
(%)	,00	,00	,00	,00	,00	,00	,00	,00	,00	100,00	,00	100,00
Total	30,00	28,00	7,00	2,00	3,00	1,00	1,00	1,00	1,00	22,00	9,00	105,00
(%)	28,57	26,67	6,67	1,90	2,86	,95	,95	,95	,95	20,95	8,57	100,00

A – Dados pessoais; **B** – Imagens MCDT; **C** – Relatórios MCDT; **D** - Análises clinicas; **E** – Nenhum; **F** – Outros; **N** – Respostas em branco.

Conclui-se que o tipo de dados dos doentes consultados em formato de papel varia significativamente (P<0.005) dependendo da categoria profissional do respondente. De notar que 58.33% dos médicos inquiridos responderam que acedem regularmente em formato de papel a dados pessoais, imagens de meios complementares de diagnóstico, relatórios de meios complementares de diagnóstico e análises clínicas dos doentes. Já 42.11% dos técnicos consultam regularmente em formato de papel dados pessoais dos doentes. De salientar que 28.57% dos enfermeiros e 20.00% dos administrativos preferiram não se pronunciar se acedem regularmente aos dados dos doentes em formato de papel.

A Tabela 8 mostra o tipo de dados dos pacientes que são mais consultados em formato de papel, e em cada tipo de instituição (Tabela 8).

Tabela 8: Relação entre a restrição do acesso aos dados em papel e o tipo de instituição. Resultados em percentagem e valor absoluto

	Pergunta 1 do questionário											
Tipo de Instituição	**A**	**ABCD**	**AC**	**ACD**	**AD**	**AF**	**BC**	**C**	**D**	**E**	**N**	**Total**
Privadas	10,00	27,00	1,00	,00	,00	,00	1,00	0,00	,00	3,00	3,00	45,00
(%)	22,22	60,00	2,22	,00	,00	,00	2,22	,00	,00	6,67	6,67	100,00
Públicas	20,00	1,00	6,00	2,00	3,00	1,00	,00	1,00	1,00	19,00	6,00	60,00
(%)	33,33	1,67	10,00	3,33	5,00	1,67	,00	1,67	1,67	31,67	10,00	100,00
Total	30,00	28,00	7,00	2,00	3,00	1,00	1,00	1,00	1,00	22,00	9,00	105,00
(%)	28,57	26,67	6,67	1,90	2,86	,95	,95	,95	,95	20,95	8,57	100,00

A – Dados pessoais; **B** – Imagens MCDT; **C** – Relatórios MCDT; **D** - Análises clinicas; **E** – Nenhum; **F** – Outros; **N** – Respostas em branco.

Conclui-se que o tipo de dados dos doentes consultados em formato de papel varia significativamente (P<0.005) dependendo do tipo de instituição. No privado 60 % dos inquiridos refere consultar em papel todo o tipo de

dados, enquanto que no público os dados mais consultados em papel são dados pessoais. De realçar, que no público 31,67% dos inquiridos diz não consultar dados em papel.

4.2.8 Restrição do acesso a dados eletrónicos

O objetivo deste teste é verificar se o tipo de dados dos doentes consultados em formato eletrónico depende da categoria profissional dos profissionais do departamento de radiologia das instituições inquiridas (Tabela 9).

Tabela 9: Relação entre a restrição do acesso aos dados eletrónicos e a categoria profissional. Resultados em percentagem e valor absoluto

	Pergunta 2 do questionário											
Categoria Profissional	**A**	**AB**	**ABC**	**ABCD**	**AD**	**B**	**BC**	**BCD**	**BD**	**E**	**N**	**Total**
Médico	,00	,00	,00	9,00	,00	3,00	,00	,00	,00	,00	,00	12,00
(%)	,00	,00	,00	75,00	,00	25,00	,00	,00	,00	,00	,00	100,00
Enfermeiro	,00	,00	1,00	2,00	2,00	,00	,00	,00	,00	,00	2,00	7,00
(%)	,00	,00	14,29	28,57	28,57	,00	,00	,00	,00	,00	28,57	100,00
Técnico	,00	1,00	16,00	29,00	,00	5,00	,00	2,00	,00	,00	4,00	57,00
(%)	,00	1,75	28,07	50,88	,00	8,77	,00	3,51	,00	,00	7,02	100,00
Investigador	,00	,00	,00	,00	,00	,00	,00	,00	,00	,00	1,00	1,00
(%)	,00	,00	,00	,00	,00	,00	,00	,00	,00	,00	100,00	100,00
Auxiliar	,00	,00	,00	1,00	,00	,00	,00	,00	,00	11,00	,00	12,00
(%)	,00	,00	,00	8,33	,00	,00	,00	,00	,00	91,67	,00	100,00
Administrativo	5,00	,00	3,00	1,00	,00	,00	1,00	,00	1,00	,00	4,00	15,00
(%)	33,33	,00	20,00	6,67	,00	,00	6,67	,00	6,67	,00	26,67	100,00
Outra	,00	,00	,00	1,00	,00	,00	,00	,00	,00	,00	,00	1,00
(%)	,00	,00	,00	100,00	,00	,00	,00	,00	,00	,00	,00	100,00
Total	5,00	1,00	20,00	43,00	2,00	8,00	1,00	2,00	1,00	11,00	11,00	105,00
(%)	4,76	,95	19,05	40,95	1,90	7,62	,95	1,90	,95	10,48	10,48	100,00

A – Dados pessoais; **B** – Imagens MCDT; **C** – Relatórios MCDT; **D** - Análises clinicas; **E** – Nenhum; **N** – Respostas em branco.

Conclui-se que o tipo de dados dos doentes consultados em formato eletrónico varia significativamente (P<0.005) dependendo da categoria profissional do profissional. De notar que 75.00% dos médicos inquiridos responderam que acedem regularmente em formato eletrónico a dados pessoais, imagens de meios complementares de diagnóstico, relatórios de meios complementares de diagnóstico e análises clínicas dos doentes, sendo que estes pertencem na sua maioria ao privado,

A Tabela 10 apresenta o tipo de dados dos doentes, em formato eletrónico, que são mais consultados em cada tipo de instituição (Tabela 10).

Tabela 10: Relação entre a restrição do acesso aos dados eletrónicos e o tipo de instituição. Resultados em percentagem e valor absoluto.

	Pergunta 2 do questionário											
Tipo de Instituição	**A**	**AB**	**ABC**	**ABCD**	**AD**	**B**	**BC**	**BCD**	**BD**	**E**	**N**	**Total**
Privadas	3,00	1,00	12,00	11,00	,00	8,00	,00	1,00	,00	4,00	5,00	45,00
(%)	6,67	2,22	26,67	24,44	,00	17,78	,00	2,22	,00	8,89	11,11	100,00
Públicas	2,00	,00	8,00	32,00	2,00	,00	1,00	1,00	1,00	7,00	6,00	60,00
(%)	3,33	,00	13,33	53,33	3,33	,00	1,67	1,67	1,67	11,67	10,00	100,00
Total	5,00	1,00	20,00	43,00	2,00	8,00	1,00	2,00	1,00	11,00	11,00	105,00
(%)	4,76	,95	19,05	40,95	1,90	7,62	,95	1,90	,95	10,48	10,48	100,00

A – Dados pessoais; **B** – Imagens MCDT; **C** – Relatórios MCDT; **D** - Análises clinicas; **E** – Nenhum; **N** – Respostas em branco.

Conclui-se que o tipo de instituição condiciona (P<0.010) o tipo de dados dos doentes em formato eletrónico, a que os profissionais de radiologia acedem eletrónico. No público mais de metade dos profissionais (53,33%) acede a todo tipo de dados dos doentes em formato eletrónico, contrastando com 24,44% no privado, que afirmam o mesmo. O tipo de dados dos doentes mais acedido/consultado em formato eletrónico pelos profissionais de radiologia dos dois tipos de instituições inquiridas é, sem dúvida, as imagens complementares de diagnóstico.

5. Discussão e Conclusões

Este estudo compara as formas de controlo de acesso a dados do departamento de radiologia de instituições de saúde privadas e públicas.

Considerando a revisão da literatura efectuada, não foram encontrados estudos semelhantes, no entanto, existe à disposição das intuições uma grande variedade de opções, quando se trata de assegurar o acesso a dados sensíveis.

O RBAC é, segundo a literatura, o modelo mais utilizado na conceção de sistemas TI, podendo ser considerado o padrão de controlo de acesso da indústria. Factor que vai de encontro aos resultados do estudo.

Este estudo demonstra que existem algumas diferenças relativas ao controlo de acesso que dependem da índole da instituição, e foram também identificados alguns fatores que devem ser melhorados quer nas instituições privadas, quer nas públicas.

5.1 Discussão de Resultados

A análise de resultados evidencia diferenças relativamente ao controlo de acesso a dados dos doentes no departamento de Radiologia, dependendo da índole da instituição.

Existem diferenças quer no que se refere ao acesso a dados em formato de papel, quer em formato electrónico.

Após a análise dos dados é inquestionável a necessidade de existir um departamento não só responsável pela área da informática, mas que incorpore especialistas na área da segurança informática, o que definitivamente não se verifica em todas as instituições.

A criação deste departamento nas instituições teria várias finalidades: desde atualizações e auditorias periódicas dos modelos , mecanismos e politicas implementadas, corrigindo falhas que possam provocar indisponibilidade das aplicações informáticas devido a atualizações, erros de funcionamento ou partilhas de dados entre várias categorias profissionais; formação e esclarecimentos dos profissionais relativamente à importância de um CA eficaz, quais os últimos avanços nesta área; gerenciamento, uniformização e teste de aplicações informáticas que servem de armazenamento aos diferentes tipos de dados; articulação com outras instituições na formulação e aplicação de medidas de controlo de acesso.

Nas instituições privadas, 71,79% dos inquiridos neste estudo afirma não ter qualquer restrição no acesso aos dados em papel dos doentes do Departamento de Radiologia, valor este que contrasta com 34,29% dos funcionários das instituições públicas. Factor que pode ser explicado por uma baixa utilização do formato em papel nas instituições privadas, uma vez que estas possuem a maioria dos registos em formato eletrónico, considerando a sua pequena dimensão, quando comparadas com as instituições públicas, a informatização mostra-se mais facilitada. Embora a informatização de dados tenha conduzido a uma diminuição da utilização dos dados em papel, estes continuam a existir e a sua proteção não deve ser descurada, podendo esta ser efectuada através da utilização de portas só acessíveis através de código, chave, cartão, entre outras, apenas por responsáveis bem definidos; o uso de câmaras de vigilância CCTV ou de seguranças que verifiquem o acesso físico podem também ser outra solução.

Relativamente aos dados em formato eletrónico, verifica-se uma semelhança entre as instituições privadas e as públicas, na escolha dos mecanismos de autenticação, pois ambas elegem o *login/password* como mecanismo preferencial, uma vez que este é de fácil implementação e utilização. No entanto, existe no privado um maior número de funcionários que indica a inexistência de qualquer mecanismo de autenticação. A mesma tendência é verificada quando falamos nos modelos de CA a dados clínicos em formato eletrónico, em que nos privados é maior a percentagem de funcionários que diz não existirem (20% versus 8,33%). O que pode acontecer é que, como as instituições privadas analisadas são instituições de menor dimensão, podem não ter um departamento responsável pelas questões informáticas, mais precisamente de segurança informática, não havendo desta forma políticas bem estruturadas de controlo de acesso. Isto é, podem por exemplo existir mecanismos de autenticação *login/ password* para algumas categorias profissionais e outras não, o que gera discórdia nas opiniões relativamente à existência destas; uma outra hipótese é: como o número de profissionais é reduzido, a instituição não vê justificação para aplicar políticas de controlo de acesso, sendo o acesso livre a todos, para todos os dados. De qualquer modo recomenda-se, que tal não aconteça, na eventualidade de existir alguma auditoria ou procedimento legal, não é possível determinar quem alterou o que, nem quando e portanto, a instituição pode ser implicada legalmente e não ter meios de se defender nem aos seus funcionários.

Nas instituições públicas inquiridas, os funcionários afirmam que os modelos de CA a dados clínicos dos doentes em formato eletrónico são baseados no grupo de utilizadores de acordo com as suas funções nas instituições (85%) ou seja, um modelo RBAC, que associa a autoridade de acesso ao papel do utilizador. Nas instituições privadas embora a maioria afirme o mesmo (57,78%), as opiniões divergem, podendo esta situação justificar-se pela acumulação de funções, que se verifica muitas vezes nas instituições de

índole privada, uma vez que possuem menor número de funcionários, não sendo possível inserir o funcionário num único grupo de utilizadores.

Perante as opiniões dos inquiridos, parece-me pertinente uma melhor adequação do modelo de controlo de acesso, e verificação do porque deste modelo não permitir uma maior flexibilidade na adição de funcionários com vários tipos de perfis, numa tentativa de colmatar este problema.

Como já referido, o mecanismo de autenticação preferencial é o login/password tanto nas instituições de cariz público como privado, no entanto após a análise de resultados, verifica-se que 88.89% dos inquiridos do público afirmam não partilhar as suas credenciais com os colegas, em contraste com apenas 37.50% dos privados. Numa primeira análise a discrepância parece grande, mas devemos considerar que no privado 15% dos inquiridos não respondeu, enquanto no público a percentagem de não respostas foi de apenas 3,70%. Uma vez mais, tal pode dever-se à acumulação de funções, que se verifica nas instituições privadas, sendo necessário a partilha de credenciais, para que os funcionários tenham acesso a todos os dados que necessitam para desempenhar as várias funções. Uma forma de ultrapassar a questão da partilha de credenciais, passa pela implementação de registo biométrico que embora represente um maior investimento financeiro, pode fazer a diferença na atribuição de responsabilidades em casos de "ataque".

A maioria dos inquiridos, independentemente da faixa etária, refere ainda que a adaptação quer aos mecanismos de autenticação, quer aos modelos de controlo de acesso é fácil. Sendo este fator preponderante e encorajador, na medida em que, se as instituições pretenderem inovar e renovar no controlo de acesso aos dados dos doentes, os profissionais, irão provavelmente colaborar sem colocar grandes entraves ou objeções. Posto isto, os profissionais devem ser parte ativa na implementação e criação de políticas, modelos e mecanismos de controlo de acesso, mantendo-os motivados para a utilização dos mesmos, e

tornando a segurança da informação mais fundamentada nos seus fluxos de trabalho e práticas diárias.

A regulamentação do controlo de acesso foi referida pela grande maioria dos inquiridos como útil. No entanto, tanto nas instituições privadas como públicas os inquiridos mostram alguma dúvida em relação à existência de um documento institucional, que regulamente a segurança ou o acesso aos dados clínicos e pessoais dos doentes, havendo mesmo uma percentagem de 14,29%, que optou por não responder, possivelmente por desconhecimento. A existência de um documento regulamentador que contemple: quais os dados disponíveis a cada categoria profissional; qual o mecanismo de autenticação em vigor, assim como o modelo de CA; quais as situações em que é possível aceder excepcionalmente a dados não anteriormente acessíveis a essa categoria; as medidas a ser aplicadas em caso de violação das normas de controlo de acesso; qual o responsável pelo controlo de acesso; periodicidade de atualização do documento regulamentador; quem faz a gestão/criação de novos utilizadores, tal como os procedimentos que inclui; como funciona o controlo de acesso a dados em papel; quais os procedimentos burocráticos para que o paciente possa ter acesso aos seus dados clínicos.

Concluindo, todas as instituições deveriam contemplar, assim como divulgar e atualizar um documento institucional, que regulamente a segurança ou o acesso aos dados clínicos e pessoais dos doentes, de forma a manter a confidencialidade dos mesmos, a limitar o acesso aos dados a pessoas não autorizadas, a uniformizar procedimentos e a salvaguardar os profissionais, a instituição e o paciente.

5.2 Limitações

A maior limitação na realização deste estudo foi sem dúvida o tempo disponível para o mesmo.

Considerando que este estudo foi desenvolvido em instituições de saúde, foi necessário despender muito tempo nos pedidos de autorização às mesmas, assim como às respetivas Comissões de Ética. Estas só reúnem na maioria dos casos mensalmente, sendo que cada documento, a ser adicionado ao processo de autorização, demorava um mês a ser avaliado.

O fator tempo, acabou também por restringir a amostra, uma vez que a recolha foi realizada presencialmente em cada instituição, em várias visitas às mesmas, não houve possibilidade desta recolha se alargar a um grande número de instituições. Para além disso, limitou-se a mesma recolha apenas aos Departamentos de Radiologia, quando idealmente deveriam ser analisados vários departamentos, para podermos ter uma visão mais abrangente acerca do controlo de acesso da instituição. Sendo que, esta limitação pode ser ultrapassada alargando a análise a outros departamentos das mesmas instituições, em trabalhos futuros.

O facto de não existir nenhum estudo idêntico também trouxe algumas dificuldades pois não havia nenhum instrumento de recolha para os dados que nós pretendíamos recolher, e sobre o qual pudéssemos basear/comparar o nosso. Desta forma, foi necessário desenhar e testar de raiz um instrumento de recolha com base na revisão da literatura efetuada. No desenho do instrumento de recolha foi também despendido muito tempo, uma vez que foram realizadas e reavaliadas várias versões do mesmo, de forma a que fosse de encontro às necessidades e objetivos do estudo, mas também que fosse de fácil interpretação para todos, sem ambiguidades e inconsistências.

Uma outra limitação, passou pela forma de recolha dos dados, na qual idealmente o levantamento dirigido aos responsáveis, deveria ser realizado sobre a forma de entrevista, o que não se verificou devido aos entraves colocados pelas Comissões de Ética. A entrevista, permitiria aos responsáveis confirmarem com outros órgãos da instituição as informações a fornecer sobre a mesma, obtendo respostas inequívocas, para numa análise posterior puder compara-las com as respostas obtidas nos questionários aos restantes profissionais de saúde. Não tendo tal sido possível, foi necessário descartar a utilização dos levantamentos na análise dos dados, pois não eram estatisticamente significativos.

Relativamente à análise, para além de algum viés que possa ter sido introduzido pela autora desta dissertação, visto ela mesma ser profissional de radiologia numa instituição de caráter privado, a maior limitação passou pela elevada taxa de respostas em branco às questões de resposta aberta, que limitou retirar conclusões sobre alguns parâmetros relevantes como: de que forma o paciente pode ter uma papel mais ativo no controlo de acesso aos seus dados clínicos de radiologia; o que poderia ser melhorado nos modelos de controlo de acesso.

5.3 Conclusões

Deste estudo pode concluir-se que existem diferenças relativas ao controlo de acesso aos dados dos doentes nos departamentos de radiologia entre instituições de saúde públicas e privadas. Mais se pode acrescentar que nas intuições públicas, e de acordo com os dados recolhidos, existem mais restrições ao acesso a dados em formato de papel; menor partilha de credenciais de acesso entre profissionais; e menor número de profissionais, que indicam inexistência de qualquer mecanismo de autenticação ou modelo de controlo de acesso, fatores estes que devem agora ser comprovado ou refutados com

estudos complementares observacionais, para verificar se a percepção do profissionais corresponde ou não à realidade da sua prática diária.

Também se conclui que existem semelhanças entre os dois tipos de instituições, pois ambas têm como mecanismo de autenticação preferencial o *login/password* e referem como modelo de controlo de acesso implementado o RBAC, embora no privado em menor escala. Em ambos os tipos de instituição e independentemente da idade, os profissionais referem fácil adaptação às formas de controlo de acesso.

Assim sendo, conclui-se que o estudo vai de acordo à hipótese inicial, de que o controlo de acesso aos dados difere em alguns aspetos, consoante a índole da instituição.

5.4 Trabalho Futuro

O trabalho futuro passa por detalhar as recomendações aos profissionais e instituições, apresentadas neste estudo, permitindo melhorar o controlo de acesso, respeitando a lei vigente. Para tal, este estudo deveria ser realizado a nível mais generalizado nas instituições, abrangendo não só o departamento de Radiologia, mas os vários departamentos, uma vez que possuem necessidades/fragilidades diferenciadas.

A criação e implementação de um modelo baseado nas recomendações obtidas por tal estudo, poderá ser um projeto mais desafiante e envolto em custos mais elevados, no entanto poderá ser mais seguro e eficiente a longo prazo para as instituições de saúde, quer públicas, quer privadas que consigam abarcar tal projeto.

5.5 Contribuições do Estudo

No âmbito da temática "Segurança Informática e Controlo de Acesso ", o estudo desenvolvido e apresentado nesta dissertação, apresenta as seguintes contribuições:

a) é um estudo pioneiro visto não haver estudos semelhantes na literatura atual;
b) disponibiliza aos investigadores interessados, um questionário elaborado de raiz, bem estruturado e detalhado focado no tema em estudo, sendo este um tema muito relevante não só em saúde mas em qualquer domínio. Este instrumento pode ser reutilizado para reproduzir o mesmo estudo ou para ser adaptado em estudos semelhantes;
c) proporciona uma visão detalhada com uma amostra razoável e equilibrada da percepção da utilização de CA em saúde pública e privada na região norte e que se pode facilmente propagar para outras regiões e instituições.
d) apresenta recomendações relativas ao controlo de acesso e à sua utilização, que podem ser auxilio de todas as instituições que usem mecanismos semelhantes, apesar de todas as limitações inerentes às características do próprio estudo;

6. Referências

Ferreira, A. ,Chadwick,D., Zao, G., Farinha,P., Correia,R., Chilro, R. L. A. (2009). How to securely break into RBAC: the BTG-RBAC model. *Proceedings from 25th Annual Computer Security Applications Conference*, pp. 23–31.

Abdulrahman Hamed Almutairi, B., Helal Alruwaili, A., Hamed Almutairi α, A., & Helal Alruwaili α, A. (2012). Security in Database Systems Security in Database Systems Security in Database Systems. *Global Journal of Computer Science and Technology Network*, *12*(17).

Almeida, A. (2009). Os Sistemas De Gestão Da Informação Arquivística Nos Hospitais Públicos Portugueses. *Biologia*, *I*, 1–94. Retrieved from http://dx.doi.org/10.1007/978-3-540-88682-2_51

Bai, Q., & Zheng, Y. (2011). Study on the Access Control Model in Information Security. *Proceedings of 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, *1*, 830–834. http://doi.org/10.1109/CSQRWC.2011.6037079

Blobel, B. (2004). Authorisation and access control for electronic health record systems. *International Journal of Medical Informatics*, *73*(3), 251–257. http://doi.org/10.1016/j.ijmedinf.2003.11.018

Bugliesi, M., Calzavara, S., Focardi, R., & Squarcina, M. (2012). Gran: Model checking grsecurity RBAC policies. *Proceedings of the Computer Security Foundations Workshop*, 126–138. http://doi.org/10.1109/CSF.2012.29

Calberson, F. L. G., Hommez, G. M., & De Moor, R. J. (2008). Fraudulent Use of Digital Radiography: Methods To Detect and Protect Digital Radiographs. *Journal of Endodontics*, *34*(5), 530–536. http://doi.org/10.1016/j.joen.2008.01.019

Computer Security Applications Conference, 2009. ACSAC'09. Annual, 23-31

Cotrini, C., Weghorn, T., Basin, D., & Clavel, M. (2015). Analyzing First-Order Role Based Access Control. *2015 IEEE 28th Computer Security Foundations Symposium*, 3–17. http://doi.org/10.1109/CSF.2015.8

Ferraiolo, D. F., & Kuhn, D. R. (1998). *Role-based access control. Advances in computers*. http://doi.org/10.1002/1521-3773(20010316)40:6<9823::AID-ANIE9823>3.3.CO;2-C

Ferrara, A. L., Fuchsbauer, G., & Warinschi, B. (2013). Cryptographically enforced RBAC. *Proceedings of the Computer Security Foundations Workshop*, 115–129. http://doi.org/10.1109/CSF.2013.15

Ferreira, A. M. (2010). Modelling Access Control for, (April).

Ferreira, A., Cruz-Correia, R., Antunes, L., & Chadwick, D. (2007). Access control: how can it improve patients' healthcare? *Studies in Health Technology and Informatics*, *127*, 65–76. http://doi.org/17901600

Guimarães, R.; Cabral, J..(1999). Estatística, Edição Revista. McGraw-hill.Lisboa.

Khan, M. F. F., & Sakamura, K. (2012). Context-aware access control for clinical information systems. *2012 International Conference on Innovations in Information Technology (IIT)*, 123–128. http://doi.org/10.1109/INNOVATIONS.2012.6207715

Lampson. (2009). Segurança: Controlo de Acesso.

Landolt, S., Hirschel, J., Schlienger, T., Businger, W., & Zbinden, A. M. (2012). Assessing and Comparing Information Security in Swiss Hospitals. *Interactive Journal of Medical Research*, *1*(2), e11. http://doi.org/10.2196/ijmr.2137

Lovis, C., Spahni, S., Cassoni, N., & Geissbuhler, A. (2007). Comprehensive management of the access to the electronic patient record: Towards trans-institutional networks. *International Journal of Medical Informatics*, *76*(5–6), 466–470. http://doi.org/10.1016/j.ijmedinf.2006.09.014

Martinho, R., & Varajão, J. (2014). Tecnologias e sistemas de informação em entidades hospitalares: dois casos de hospitais portugueses. *Por Que GESITI?* Retrieved from http://repositorium.sdum.uminho.pt/handle/1822/31098

Miller, R. H., & Sim, I. (2004). Physicians' use of electronic medical records: Barriers and solutions. *Health Affairs*, *23*(2), 116–126. http://doi.org/10.1377/hlthaff.23.2.116

Pato, J. N., Millett, L. I., & National Research Council (U.S.). Whither Biometrics Committee. (n.d.). *Biometric recognition : challenges and opportunities*.

Rodrigues, B. J. de S. (2015). *Segurança no acesso ao registo clínico eletrónico*. Universidade do Minho.

Ross, S. E., & Lin, C.-T. (2003). The Effects of Promoting Patient Access to Medical Records: A Review. *Journal of the American Medical Informatics Association : JAMIA*, *10*(2), 129–138. http://doi.org/10.1197/jamia.M1147

Segurança em Sistemas de Informação na área da Saúde. (n.d.). Retrieved September 11, 2017, from http://im.med.up.pt/seguranca/

Yeo, K., Lee, K., Kim, J.-M., Kim, T.-H., Choi, Y.-H., Jeong, W.-J., … Yoo, S. (2012). Pitfalls and Security Measures for the Mobile EMR System in Medical Facilities. *Healthcare Informatics Research*, *18*(2), 125–135. http://doi.org/10.4258/hir.2012.18.2.125

Zriqat, A. (2016). Security and Privacy Issues in Ehealthcare Systems : Towards Trusted Services, *7*(9), 229–236.

7. Anexos

Anexo I : Revisão da Literatura

De forma, a perceber que modelos, mecanismos e políticas de controlo de acesso aos dados existem, nomeadamente em instituições de saúde, e como funcionam; assim como a existência de estudos idênticos; os maiores problemas relacionados com a segurança da informação em instituições de saúde, em particular na Radiologia, foi realizada uma pesquisa em duas bases de dados: Pubmed e IEE. Os termos/ expressões utilizados na pesquisa inicial foram: "Acess Control", "access control and health<in>metadata" e "Comparing computer security between private and public hospitals". Na pesquisa inicial obtivemos 534 referências, das quais algumas foram excluídas segundo os seguintes factores de exclusão: data de publicação superior a 10 anos; artigos sem acesso livre; título não incluído na temática e interesses do estudo; tipo de artigo; e linguagem de publicação. Desta forma, selecionamos 37 referências, dos quais se analisou o *Abstract,* para percepcionar se estes se enquadravam no estudo, excluindo deste modo 9 referências. De forma a esclarecer alguns conceitos, foram analisados 8 artigos, através de pesquisa dirigida aos conceitos. Concluindo, a revisão bibliográfica baseou-se na análise de 36 referências, apresentadas na Tabela 11.

Tabela 11: Artigos Revisão Bibliográfica

Titulo	Autor	Ano	Base
Security measures in a secure computer communications architecture	Bottino, LJ	2006	IEEE
Physicians' use of electronic medical records: barriers and solutions.	Miller RH	2004	Pubmed
Authorisation and access control for electronic health record systems.	Blobel B.	2004	Pubmed
The effects of promoting patient access to medical records: a review.	Ross SE	2003	Pubmed.
Evaluating computerised health information systems: hard lessons still to be learnt	Peter Littlejohns	2003	Pubmed
Study on the access control model	Bai Qing-hai	2011	IEEE
Context-aware access control for clinical information systems	Khan, M.F.F ; Sakamura, K.	2012	IEEE
Formal Analysis of Access Control Policies for Pattern-Based Business Processes	Karimi, Vahid R.	2009	IEEE
Constructing Grounded Theory: A Practical Guide through Qualitative Analysis.	Charmaz K.	2006	IEEE
Spatio-temporal Role Based Access Control for Physical Access Control Systems	Geepalla, E.	2013	IEEE
Acess control: how can it improve patient's healthcare?	Ana Ferreira		FMUP
Grounding information security in healthcare	Ana Ferreira	2010	FMUP
Design of Fusion Classifiers for Voice-Based Access Control System of Building Security	Syazilawati et al.	2009	IEEE
Handwriting dynamics as a means of authentication	Pavel Lozhnikov; Oksana Chernikova	2011	IEEE
Role-Based Access Control	David F. Ferraiolo et al.	2007	IEEE
A framework for distributed metadata management of mineral information resources with access control	Z. Sui et al.	2013	IEEE
Enabling secure service discovery in mobile healthcare enterprise networks	A. Toninelli et al.	2009	IEEE
Pseudonymization with Metadata Encryption for Privacy-Preserving Searchable Documents	J. Heurix et al.	2012	IEEE
Design and Implementation of a Privacy Aware Framework for Sharing Electronic Health Records	Cheng-Yi Yang et al.	2015	IEEE
A decentralized access control mechanism using authorization certificate for distributed file systems	J. Arakawa et al.	2011	IEEE
Hybrid intelligent access control framework to protect data privacy and theft	J. C. Doshi; B. Trivedi	2015	IEEE

Security models for web-based applications: using traditional and emerging access control approaches to develop secure applications for the web. Communications of the ACM.	Joshi J et al.	2001	IEEE
Security in Database Systems	Abdulrahman Hamed Almutairi & Abdulrahman Helal Alruwaili	2012	IEEE
Detection and Prevention of SQL Injection Attacks	Nausheen Kanwal		Retirado de outro artigo
Tecnologias e Sistemas de Informação em entidades hospitalares – Dois casos de hospitais portugueses	Ricardo Martinho et al.		
Os Sistemas de Gestão da Informação nos Hospitais Públicos Portugueses	Andreia da Silva Almeida		
Fraudulent Use of Digital Radiography: Methods To Detect and Protect Digital Radiographs	Filip L.G. Calberson, DDS, MMS, Geert M et al.	2008	Pubmed
Comprehensive management of the access to the electronic patient record: Towards trans-institutional networks	Christian Lovis et al.	2007	Pubmed
Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services	Isra'a Ahmed Zriqat	2016	Pubmed
Segurança no acesso ao registo clínico electrónico	Bruno Jorge de Sales Gomes Rodrigues	2015	
Cryptographically Enforced RBAC	Anna Lisa Ferrara et al.	2013	IEEE
Gran: model checking grsecurity RBAC policies	Michele Bugliesi Stefano Calzavara Riccardo Focardi Marco Squarcina	2012	IEEE
Analyzing First-order Role Based Access Control	Carlos Cotrini et al.	2015	IEEE
Assessing and comparing information security in swiss hospitals.	Landolt et al.	2012	Pubmed
Comprehensive management of the access to the electronic patient record: Towards trans-institutional networks	Filip L.G et al.	2007	
Fraudulent Use of Digital Radiography: Methods To Detect and Protect Digital Radiographs		2008	

Anexo II: Questionário

Questionário

Este questionário tem como objetivo o levantamento das opiniões dos profissionais do departamento de Radiologia das instituições participantes, relativo à forma como estes profissionais utilizam mecanismos de controlo de acesso e de autenticação, no acesso aos dados dos doentes, na sua prática clínica diária.

Este estudo é realizado no âmbito da tese de Mestrado em Informática Médica, intitulada "Comparação do controlo de acesso em instituições de saúde privadas e públicas, da região Norte", pela aluna Ana Sofia Maria. O objetivo principal desta tese é sumariar os principais modelos e mecanismos de controlo de acesso e de autenticação, físicos e informáticos, utilizados na prática clínica, em particular, dos profissionais de Radiologia, e analisando de que forma estas medidas de segurança podem influenciar o seu fluxo de trabalho. Deste modo, poderão surgir recomendações de alterações para divulgação e uso dentro das instituições de saúde participantes, que podem garantir uma melhoria na proteção e integridade dos dados relativos à pessoa humana.

Todos os dados recolhidos neste questionário serão tratados de forma anónima (garantindo-se a total confidencialidade dos participantes e respetivas instituições) e usados unicamente para efeitos de investigação.

Preencha, sempre que possível, com um X.

Porto, 31 de Março de 2017

Rua Doutor Plácido da Costa | 4200-450 Porto , Portugal
Tel. +351 225 513 622 | Fax: +351 225 513 623
http://mim.med.up.pt , mim@med.up.pt

2º Ciclo de Estudos
Em Informática Médica

Dados Demográficos

Instituição: _____

Género:

Masculino ☐ ☐ Feminino

Idade:

○ 20 a 35 anos ○ 36 a 55 anos ○ 56 a 65 anos ○ Mais de 65 anos
○ Não responde

Atividade profissional: _____

Categoria profissional:

○ Médico ○ Enfermeiro ○ Técnico ○ Investigador
○ Auxiliar ○ Administrativo ○ Outra _____

Anos de experiência (**nesta instituição**):

○ Menos de 1 ano ○ 1 a 5 anos ○ 6 a 10 anos ○ Mais de 10 anos
○ Não responde

Anos de experiência (**noutras instituições**):

○ Menos de 1 ano ○ 1 a 5 anos ○ 6 a 10 anos ○ Mais de 10 anos
○ Não responde

2º Ciclo de Estudos
Em Informática Médica

2.1. Indique se utiliza **aplicações informáticas na sua atividade diária** e que tipo de dados armazenam, **apontando o nome destas se souber** (deixe em branco se não utilizar nenhuma aplicação que armazene o tipo de dados indicado):

2.1.1. Dados pessoais dos doentes

2.1.2. Imagens de Meios Complementares de Diagnóstico (MCDT)

2.1.3. Relatórios de Meios Complementares de Diagnóstico (MCDT)

2.1.4. Análises Clínicas

2.1.5. Outros dados dos doentes

2.2. No âmbito da sua atividade diária tem alguma **restrição no acesso** aos **dados informatizados dos doentes?**

- ◯ Não, tenho acesso aos dados de todos os doentes do departamento de Radiologia
- ◯ Sim, tenho apenas acesso aos dados que necessito para realizar o meu trabalho
- ◯ Sim, apenas consigo aceder a parte do que necessito para realizar o meu trabalho
- ◯ Não aplicável
- ◯ Outro _____

2.3. Que **mecanismos de autenticação** são utilizados para aceder aos dados dos doentes em **formato eletrónico** (pode assinalar mais do que uma opção):

- ◯ Login/password
- ◯ Smart-card/token (cartão de acesso ou outro dispositivo semelhante)
- ◯ Biometria (impressão digital, reconhecimento da íris, etc)
- ◯ Não existem mecanismos de autenticação
- ◯ Outros Quais?_____

2.4. Numa escala de 1 a 5 (sendo 1 muito difícil e 5 muito fácil) como classifica a sua adaptação aos **mecanismos de autenticação**, caso existam?

◯ 1 (muito difícil) ◯ 2 (difícil) ◯ 3 (neutro) ◯ 4 (fácil) ◯ 5 (muito fácil)

2.5. Considera que os **mecanismos de autenticação** que utiliza são:

◯ Barreiras ◯ Facilitadores ◯ Não Sei

2.5.1. Porquê?

2.5.2. O que considera que poderia ser melhorado?

2.6. Costuma **partilhar com os seus colegas as suas credenciais para acesso** aos dados dos doentes (e.g., login/password ou outras):

◯ SIM ◯ NÃO ◯ Não Respondo

2.6.1. Se sim, porquê?

3. Indique em que se baseiam os **modelos de controlo de acesso** a dados clínicos dos doentes **em formato eletrónico** (pode assinalar mais do que uma opção):

◯ Grupo de utilizadores de acordo com as suas funções na instituição

◯ Necessidades específicas de cada utilizador

◯ Regras obrigatórias para todos os utilizadores do sistema

◯ Não existe controlo de acesso

◯ Outros Quais?_____

3.1. Numa escala de 1 a 5 (sendo 1 muito difícil e 5 muito fácil) como classifica a sua adaptação **aos modelos de controlo de acesso**, caso existam?

◯ 1 (muito difícil) ◯ 2 (difícil) ◯ 3 (neutro) ◯ 4 (fácil) ◯ 5 (muito fácil)

2º Ciclo de Estudos
Em Informática Médica

3.2. Considera que os **modelos de controlo de acesso** aos dados dos doentes que utiliza são:

◯ Barreiras ◯ Facilitadores ◯ Não Sei

3.2.1. Porquê?

3.2.2. O que considera que poderia ser melhorado?

4. Indique com que frequência, e em que aplicações, ocorrem as seguintes falhas ou erros quando acede aos dados dos doentes (**sendo 1 nunca e 5 muito frequentes**):

Indisponibilidade das aplicações informáticas devido a atualizações:

◯ 1 (nunca) ◯ 2 (raramente) ◯ 3 (2 vezes por mês) ◯ 4 (frequente) ◯ 5 (muito frequente)

Nomeie a(s) aplicação(ões) que te(ê)m esta falha:

Indisponibilidade das aplicações informáticas devido a erros de funcionamento:

◯ 1 (nunca) ◯ 2 (raramente) ◯ 3 (2 vezes por mês) ◯ 4 (frequente) ◯ 5 (muito frequente)

Nomeie a(s) aplicação(ões) que te(ê)m esta falha :

Indisponibilidade no acesso às aplicações informáticas por parte dos utilizadores:

◯ 1 (nunca) ◯ 2 (raramente) ◯ 3 (2 vezes por mês) ◯ 4 (frequente) ◯ 5 (muito frequente)

Nomeie a(s) aplicação(ões) que te(ê)m esta falha :

Indisponibilidade de meios de partilha de dados, com os colegas:

◯ 1 (nunca) ◯ 2 (raramente) ◯ 3 (2 vezes por mês) ◯ 4 (frequente) ◯ 5 (muito frequente)

Nomeie a(s) aplicação(ões) que te(ê)m esta falha :

2º Ciclo de Estudos
Em Informática Médica

Refira outras falhas e/ou problemas frequentes e, se possível, em que aplicações estas ocorrem:

5. Um **doente** do departamento de Radiologia tem **acesso aos seus dados clínicos**?

◯ SIM ◯ NÃO ◯ NÃO SEI

5.1. Se sim, de que forma?

6. Na sua opinião, **o doente** deveria ter um papel mais ativo no controlo de acesso aos seus dados clínicos de radiologia?

◯ SIM ◯ NÃO ◯ NÃO SEI

6.1. Porquê?

6.2. Se sim, de que forma?

7. Os **familiares** de um doente do departamento de Radiologia têm **acesso aos dados** desse doente?

◯ SIM ◯ NÃO ◯ NÃO SEI

7.1. Se sim, quais os procedimentos para o conseguirem?

8. Na sua opinião, os **familiares do doente** deveriam ter um papel mais ativo no controlo de acesso aos dados desse doente?

◯ SIM ◯ NÃO ◯ NÃO SEI

8.1. Porquê?

8.2. De que forma?

2º Ciclo de Estudos
Em Informática Médica

9. Tem conhecimento da existência de algum **documento institucional** que **regulamente a segurança ou o acesso aos dados clínicos e pessoais dos doentes?**

◯ SIM ◯ NÃO ◯ NÃO SEI

9.1. Se Sim, qual o documento e onde se encontra disponível?

9.1. Considera útil a existência de um **documento que regule o acesso aos dados dos doentes**, quer em suporte de papel ou informatizado?

◯ SIM ◯ NÃO ◯ NÃO SEI

9.1.1. Porquê?

TERMINOU O PREENCHIMENTO DO INQUÉRITO.

OBRIGADA PELA COLABORAÇÃO

Anexo III: Levantamento

Levantamento de dados sobre a instituição

Este documento destina-se a efetuar o levantamento de informação que caracteriza a instituição de saúde em estudo (e.g., nº de camas, nº e tipo de profissionais, nº e tipo de aplicações informáticas, autenticação e controlo de acesso usados, etc) por parte dos profissionais que gerem a mesma instituição ou as aplicações e software que integram os dados dos seus doentes.

Este estudo é realizado no âmbito da tese de Mestrado em Informática Médica, intitulada "Comparação do controlo de acesso em instituições de saúde privadas e públicas, da região Norte", pela aluna Ana Sofia Maria. O objetivo principal desta tese é sumariar os principais modelos e mecanismos de controlo de acesso físicos e informáticos utilizados na prática clínica, em particular, dos profissionais de Radiologia, e analisando de que forma estas medidas de segurança podem influenciar o seu fluxo de trabalho. Deste modo, poderão surgir recomendações de alterações para divulgação e uso dentro das instituições de saúde participantes, que podem garantir uma melhoria na proteção e integridade dos dados relativos à pessoa humana.

Todos os dados recolhidos neste levantamento serão tratados de forma anónima (garantindo-se a total confidencialidade das instituições participantes) e usados unicamente para efeitos de investigação.

Porto, 31 de Março de 2017

Rua Doutor Plácido da Costa | 4200-450 Porto , Portugal
Tel: +351 225 513 622 | Fax: +351 225 513 623
http://mim.med.up.pt , mim@med.up.pt

2º Ciclo de Estudos
Em Informática Médica

Instituição:

1. A instituição é :

   ☐ Privada ☐ Pública ☐ Ambos

2. Qual o tipo de instituição?

   ☐ Hospital ☐ Clínica ☐ Outra _____

3. Qual o número total de profissionais que trabalham nesta instituição?

4. Qual o número total de camas que a instituição incorpora?

5. Existe alguma política de controlo de acesso aos dados dos doentes definida pela instituição?

   ◯ SIM ◯ NÃO ◯ NÃO SEI

   5.1. Se sim, este documento está atualizado?

   ◯ SIM ◯ NÃO ◯ NÃO SEI

   5.2. Quem é o responsável pela manutenção da política de controlo de acesso?

   5.3. A política de controlo de acesso é constituída por que partes?

6. A instituição contempla **departamento de informática**?

   ◯ SIM ◯ NÃO ◯ NÃO SEI

6.1. Os serviços informáticos são geridos por uma empresa externa à instituição? Se **SIM** qual?

2º Ciclo de Estudos
Em Informática Médica

Departamento de Informática

7. Quantos profissionais trabalham no **departamento de informática?**

- ◯ Nenhum
- ◯ Menos de 5 profissionais
- ◯ 5 a 10 profissionais
- ◯ 10 a 15 profissionais
- ◯ Mais de 15 profissionais

7.1. Destes, quantos são especialistas na área da **segurança informática?**

7.2. Quantos profissionais **gerem** a segurança dos dados?

- ◯ Nenhum
- ◯ Menos de 5 profissionais
- ◯ 5 a 10 profissionais
- ◯ 10 a 15 profissionais
- ◯ Mais de 15 profissionais

8. Que outras atividades regulares desenvolvem os profissionais do **departamento de informática?**

9. De que forma é assegurado o **acesso físico** aos dados dos doentes da instituição? (pode ser mais do que uma opção)

- ◯ Portas só acessíveis através de código, chave, cartão, etc, apenas pelos responsáveis
- ◯ Uso de câmaras de vigilância CCTV ou seguranças que verificam o acesso
- ◯ Não existe qualquer restrição ao acesso
- ◯ Não aplicável
- ◯ Outros Quais?_____

2º Ciclo de Estudos
Em Informática Médica

10. Que **mecanismos de autenticação** são utilizados na instituição para aceder aos dados dos doentes em formato eletrónico? (pode ser mais do que uma opção)

- ◯ Login/password
- ◯ Smart card/token (cartão de acesso ou outro dispositivo semelhante)
- ◯ Biometria (impressão digital, reconhecimento da iris, etc)
- ◯ Nenhum
- ◯ Outros Quais?_____

11. Que **mecanismos de autenticação** são usados para controlar o acesso às aplicações que armazenam os dados dos doentes do **departamento de Radiologia**?

- ◯ Login/password
- ◯ Smart card (cartão de acesso)
- ◯ Biometria (impressão digital, reconhecimento da iris, etc)
- ◯ Nenhum
- ◯ Outros Quais?_____

12. Indique em que se baseiam os **modelos de controlo de acesso** a dados clínicos dos doentes implementados na instituição (pode ser mais do que uma opção):

- ◯ Grupo de utilizadores de acordo com as suas funções na instituição
- ◯ Necessidades específicas de cada utilizador
- ◯ Regras obrigatórias para todos os utilizadores do sistema
- ◯ Nenhum
- ◯ Outros Quais?_____

Faculdade de Medicina da Universidade do Porto
Faculdade de Ciências da Universidade do Porto
2º Ciclo de Estudos
Em Informática Médica

13. Que **modelos de controlo de acesso** a dados clínicos informatizados dos doentes estão implementados no **departamento de Radiologia**? (pode ser mais do que uma opção)

- ◯ Grupo de utilizadores de acordo com as suas funções na instituição
- ◯ Necessidades específicas de cada utilizador
- ◯ Regras obrigatórias para todos os utilizadores do sistema
- ◯ Nenhum
- ◯ Outros Quais?_____

14. **A criação e registo de novos utilizadores** que acedem a dados dos doentes acarreta as seguintes alterações (pode ser mais do que uma opção):

- ◯ Criação de novo perfil de utilizador
- ◯ Definição de privilégios para o novo utilizador
- ◯ Alterações na base de dados Quais? _____
- ◯ O utilizador tem de efetuar tarefas Quais? _____
- ◯ Outros Quais? _____
- ◯ Nenhuma alteração

14.1. Quem faz a **gestão** da criação de novos utilizadores ou da alteração das permissões dos já existentes?

Rua Doutor Plácido da Costa | 4200-450 Porto , Portugal
Tel: +351 225 513 622 | Fax: +351 225 513 623
http://mim.med.up.pt , mim@med.up.pt

Faculdade de Medicina da Universidade do Porto
Faculdade de Ciências da Universidade do Porto

2º Ciclo de Estudos
Em Informática Médica

Departamento de Radiologia

15. Quantos profissionais trabalham no **departamento de Radiologia?**

- ○ Menos de 10 profissionais
- ○ 10 a 20 profissionais
- ○ 20 a 30 profissionais
- ○ Mais de 30 profissionais

16. Qual o número de **aplicações informáticas** que existe no **departamento de Radiologia,** para armazenamento de dados dos doentes?

- ○ Menos de 5 aplicações
- ○ 5 a 10 aplicações
- ○ 10 a 15 aplicações
- ○ Mais de 15 aplicações

16.1. Indique o nome das **aplicações informáticas** mais usadas no **departamento de Radiologia** para armazenamento/gestão de dados dos doentes.

16.2. Que **tipo de dados dos doentes** são armazenados nestas aplicações? (pode ser mais do que uma opção)

- ○ Dados pessoais
- ○ Imagens de MCDT
- ○ Relatórios de MCDT
- ○ Análises clínicas
- ○ Outros Quais?_____

Rua Doutor Plácido da Costa | 4200-450 Porto . Portugal
Tel. +351 225 513 622 | Fax: +351 225 513 623
http://mim.med.up.pt . mim@med.up.pt

17. Que **mecanismos de autenticação** são utilizados no **departamento de Radiologia** para aceder aos dados **informatizados** dos doentes? (pode ser mais do que uma opção)

- ◯ Login/password
- ◯ Smart card/token (cartão de acesso ou outro dispositivo semelhante)
- ◯ Biometria (impressão digital, reconhecimento da iris, etc)
- ◯ Outros Quais?_____
- ◯ Nenhum

18. Indique em que se basciam os **modelos de controlo de acesso** a dados clínicos informatizados, implementados no **departamento de Radiologia** (pode ser mais do que uma opção):

- ◯ Grupo de utilizadores de acordo com as suas funções na instituição
- ◯ Necessidades especificas de cada utilizador
- ◯ Regras obrigatórias para todos os utilizadores do sistema
- ◯ Outros Quais?_____
- ◯ Nenhum

19. A **criação e registo de novos utilizadores** que acedem a dados dos doentes no **departamento de Radiologia**, acarreta as seguintes alterações (pode ser mais do que uma opção):

- ◯ Criação de novo perfil de utilizador
- ◯ Definição de privilégios para o novo utilizador
- ◯ Alterações na base de dados Quais? _____
- ◯ O utilizador tem de efetuar tarefas Quais? _____
- ◯ Outros Quais? _____
- ◯ Nenhuma alteração

19.1. **Quem faz a gestão** da criação de novos utilizadores ou da alteração das permissões dos já existentes, no **departamento de Radiologia**?

2º Ciclo de Estudos
Em Informática Médica

20. Como é assegurado o controlo de **acesso ao espaço físico** do **departamento de Radiologia**? (pode ser mais do que uma opção)

- ◯ Portas só acessíveis através de código, chave, cartão, etc, apenas pelos responsáveis
- ◯ Uso de câmaras de vigilância CCTV ou seguranças que verificam o acesso
- ◯ Não existe qualquer restrição ao acesso
- ◯ Não aplicável
- ◯ Outros Quais?_____

21. No **departamento de Radiologia** recorre-se ao **suporte em papel** para armazenamento de dados?

◯ SIM ◯ NÃO ◯ NÃO SEI

21.1. Se sim, para armazenar que tipo de informação?

21.2. Com que objectivo?

21.3. De que forma é assegurado o acesso aos **dados em papel**, no **departamento de Radiologia**? (pode ser mais do que uma opção)

- ◯ Portas só acessíveis através de código, chave, cartão, etc, apenas pelos responsáveis
- ◯ Uso de câmaras de vigilância CCTV ou seguranças que verificam o acesso
- ◯ Não existe qualquer restrição ao acesso
- ◯ Não aplicável
- ◯ Outros Quais?_____

TERMINOU O PREENCHIMENTO DESTE INQUÉRITO.

OBRIGADO PELA COLABORAÇÃO

Anexo IV: Consentimento Informado

Consentimento Informado, Livre e Esclarecido para participação em investigação

No âmbito da tese de Mestrado em Informática Médica, intitulada "Comparação do controlo de acesso em instituições de saúde privadas e públicas, da região Norte", pretende realizar-se um inquérito, no departamento de Radiologia, que poderá ser preenchido por todos os profissionais deste departamento, que de livre vontade o pretendam fazer.

O objectivo principal do mesmo prende-se com sumariar os principais mecanismos de controlo de acesso utilizados na prática clínica, analisando de que forma podem influenciar o fluxo de trabalho das instituições. Deste modo, poderão surgir recomendações para a sua alteração, que garantam uma melhoria na proteção e integridade dos dados relativos à pessoa humana, assim como à sua utilização e divulgação. Este estudo destina-se a profissionais das áreas da saúde e da informática que fazem a gestão das aplicações e software que integram os dados dos doentes nas instituições de saúde.

Os participantes têm a possibilidade de em qualquer altura recusar participar no estudo, sem quais quaisquer consequência.

Todos os dados são recolhidos de forma anónima (garantindo-se a total confidencialidade dos participantes) sendo os mesmos posteriormente tratados estatisticamente. As respostas obtidas no âmbito do estudo serão utilizadas unicamente para efeitos de investigação.

Assinaturas:

Declaro ter lido e compreendido este documento, bem como as informações verbais que me foram fornecidas pela/s pessoa/s que acima assina/m. Foi-me garantida a possibilidade de, em qualquer altura, recusar participar neste estudo sem qualquer tipo de consequências. Desta forma, aceito participar neste estudo e permito a utilização dos dados que de forma voluntária forneço, confiando em que apenas serão utilizados para esta investigação e nas garantias de confidencialidade e anonimato que me são dadas pela investigadora.

Nome:
Assinatura:
Data:

Anexo V: Pedido ao Conselho de Administração

PEDIDO DE AUTORIZAÇÃO PARA REALIZAÇÃO DE PESQUISA CLÍNICA/ INVESTIGAÇÃO CLÍNICA

Exmº Sr Presidente do Conselho de Administração

Ana Sofia da Silva Maria, licenciada em Radiologia pela Universidade de Aveiro, residente em Vila Real, atualmente a exercer a função de Técnica de Radiologia, na Clinica JCC Diagnóstico por Imagem SA, cédula profissional nº C-046140140 , vem requerer a V/Exa. autorização para a realização da Pesquisa Clínica/Investigação Clínica subordinada ao tema "Comparação do controlo de acesso em instituições de saúde privadas e públicas, da região Norte", no âmbito do mestrado que venho a desenvolver em Informática Médica na Faculdade de Medicina da Universidade do Porto.

A recolha será realizada recorrendo a questionários em papel, entregues e recolhidos em mão na instituição, de forma a serem preenchidos pelos profissionais do departamento de Radiologia, que o pretendam fazer, sendo impreterivelmente mantido o anonimato da instituição, bem como de todos os participantes, durante o desenvolvimento de todo o projeto, assim como em qualquer divulgação ou publicação de resultados.

A tese em desenvolvimento tem como objectivo primordial sumariar os principais mecanismos de controlo de acesso utilizados na prática clínica da instituição, nomeadamente do departamento de Radiologia, analisando de que forma podem influenciar o fluxo de trabalho das instituições. Deste modo, poderão sugerir-se alterações, que garantam uma melhoria na proteção e integridade dos dados relativos à pessoa humana, assim como à sua utilização e

Rua Doutor Plácido da Costa | 4200-450 Porto . Portugal
Tel: +351 225 513 622 | Fax: +351 225 513 623
http://mim.med.up.pt . mim@med.up.pt

divulgação.

Desta forma, as instituições terão conhecimento do vasto leque de opções de modelos para implementação nas suas instituições, assim como as vantagens que estes acarretam; quais os modelos, que facilitam o fluxo de trabalho, aumentando a produtividade, diminuindo os tempos de resposta aos que procuram cuidados, levando a um aumento de receitas; podem garantir aos pacientes maior segurança e credibilidade nos cuidados prestados, conduzindo a um aumento da afluência destes, à instituição.

Contando com a autorização desta instituição, coloco-me à disposição para qualquer esclarecimento.

Contatos:
Investigadora:
Ana Maria – assm@ua.pt

Coordenadora:
Dra. Ana Ferreira – amlaf@med.up.pt

Habilitações académicas: Doutoramento

Local de trabalho: FMUP

19 de Abril de 2016

Ana Sofia da Silva Maria